

**530.1**

# Defensible Security Architecture and Engineering

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020

**SANS**

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | [sans.org](https://sans.org)

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

SANS

# Defensible Security Architecture and Engineering

© 2019 Eric Conrad, Justin Henderson, & Ismael Valenzuela | All Rights Reserved | Version E01\_02

Welcome to Defensible Security Architecture and Engineering!

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020

Table of Contents	Page
Course Overview.....	4
Defensible Security Architecture.....	22
Traditional Security Architecture Deficiencies.....	28
Winning Defensible Security Techniques.....	44
Security Models.....	60
Threat, Vulnerability, and Data Flow Analysis.....	75
<b>EXERCISE:</b> Egress Analysis.....	88
Physical Security .....	90
Wireless.....	102
Layer 2 Attacks and Mitigations .....	118
<b>EXERCISE:</b> Identifying Layer 2 Attacks .....	136
Private VLANs .....	138

### 530.1 Table of Contents

This table of contents outlines our plan for 530.1.



Table of Contents	Page
Switch and Router Best Practices.....	148
Network Flow .....	163
<b>EXERCISE:</b> Architecting for Flow Data .....	179
530.1 Summary.....	181

### 530.1 Table of Contents

This table of contents outlines our plan for 530.1.

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020

## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. **Course Overview**
2. Defensible Security Architecture
3. Traditional Security Architecture Deficiencies
4. Winning Defensible Security Techniques
5. Security Models
6. Threat, Vulnerability, and Data Flow Analysis
7. **EXERCISE: Egress Analysis**
8. Physical Security
9. Wireless
10. Layer 2 Attacks and Mitigation
11. **EXERCISE: Identifying Layer 2 Attacks**
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. **EXERCISE: Architecting for Flow Data**
16. 530.1 Summary

### Course Roadmap

Each section of this course presents a Course Roadmap slide to help you follow where we are in the course material. These “you are here” slides will also help you easily locate information for after-class review.

This first section provides an overview of the 530 course.

## Welcome to SEC530!

### Course Goals

- Help you design, build and harden networks, infrastructure and applications that are ‘defensible’
- To architect to reduce the scope and severity of the incidents you’ll have, no matter what!
- To provide you with a framework to continually improve your security stance, knowing how to best defend now and in the future
- Learn in a practical way, with tons of hands-on labs!

### Welcome to SANS Security 530!

This course is intended to help you design, build and harden networks, infrastructure and applications that are effectively defensible.

While the course authors have many years of experience in building and assessing security architectures, they have also been involved in reacting to security incidents that have caused major havoc to organizations that relied a little too much on prevention. The truth is, incidents happen and will continue to happen, no matter what. And that’s why it is imperative that we study and learn from other organizations’ incidents so we can mitigate the impact of them when they materialize in our environment.

As the proverb goes: “the wise man learns from the mistakes of others”, and we definitely want to be wise, don’t we?

It’s with this intention that we have created this class, so we can provide you with a framework to continually improve your security stance, one you can use now and for the years to come. One that will teach how to best defend now and in the future.

And of course, it wouldn’t be a SANS class, without tons on hands-on labs, filled with fun challenges and realistic scenarios.

Your participation during the course is very much encouraged. Feel free to make comments, ask questions, and relate experiences related to the concepts and issues presented during this course.

At the end of every day, we ask you to complete a brief course evaluation form. Please take the time to do so. The feedback received from attendees is used to optimize and enhance each SANS course. If there’s something that can be done in class to assure you have an excellent experience, please let us know. We’ll do our best to honor requests. If there are facility issues such as temperature, please bring this to the attention of the class facilitator or SANS staff to have it resolved.

## What Is a Security Architecture?

- Architecture is meant to communicate a future state
- Security architecture focuses on designing and building security in:
  - Networks and infrastructure
  - Applications
  - Endpoint
  - Cloud
- Typically built from the network up
- It must be built around business processes

### So what is a security architecture?

A security architecture is nothing but a communication tool, one to communicate a future state. It's an overall plan on how to implement security at every layer, using technology, processes and people.

Note that a security architecture is NOT an extra layer, something that we can put on top of existing architecture to cover its deficiencies. On the contrary, it's about focusing on designing and building security in every single layer, including:

- Networks and infrastructure
- Applications
- Endpoint
- Cloud

To do so, we will follow a bottom up approach, starting from the network up, while we take into consideration strategies and methodologies that allow us to align security to business goals and objectives.

## What Does a Security Architect Do?

Just like a homeowner works with an architect to provide an upon agreed architectural drawing of the key elements of a house, security architects design, builds and oversees the implementation of network and computer security for an organization.



### What Does a Security Architect Do?

While that sounds fantastic, in theory, the reality is that in many organizations the same person that designs the solution has also to build, oversee, operate and even monitor it, while riding a bike on fire at the same time...

Since an architecture is simply an overall plan to communicate a future state, project management is certainly an important part of what an architect does. While this class will cover the minimal aspects required for that, we will focus on the practical aspects of how to harden each of the layers we operate at.

[1] <https://www.spreadshirt.com/security+architect+women-s+t-shirt-D13506502>

## What Makes a Good Security Architect?

- Understanding of networks, infrastructure, applications, information and business architecture... and how each of those layers deal with risk
  - **Think RED**: What are the threats that are likely to cause an impact?
  - **Act BLUE**: What are the architectural designs and technologies that will help me defend against them?
- Can balance business and technical communications
- Has good project management skills
- Has a strategic and tactical vision

### What Makes a Good Security Architect?

To do so, as a security architect you must **REALIZE THAT SECURITY IS PROBABLY NOT THE CORE BUSINESS OF YOUR ORGANIZATION**. The security architect must do what it's best for the business, mitigating the impact that security risks can have on it. This adds value to the organization and makes you win the trust of those working with you.

Since **MITIGATING EVERY RISK IS IMPOSSIBLE, SOME PRIORITIZATION IS NEEDED**. Therefore, a good security architect must understand how the different layers of networks, infrastructure, applications, data and business architectures deal with risk, thinking like an attacker (red), but acting like a defender (blue).

A good security architect must also have a good understanding of:

- **Business** requirements:
- **Regulatory** landscape
- **Threat landscape**
- **IT landscape**

Since deep knowledge of these areas typically goes beyond the duties of a security architect, **YOU'LL HAVE TO WORK WITH OTHER NETWORK AND ENTERPRISE ARCHITECTS AS WELL AS ENGINEERS THAT ARE EXPERTS IN THESE FIELDS**. For this reason, you must have **good communication skills** to be able to communicate in all forms, written and verbally, and at different levels, technical and managerial.

A good security architect can also see the **big picture (strategic) and tactical**, and can **zoom out and zoom in** depending on what is required or the phase of the security architecture lifecycle she's in.

Finally, you must also understand that a good security architecture is a combination of people, process and technology.

## Different Types of Security Architects

- Security professionals (engineers, admins, analysts...) that want to understand ‘architectures’
- IT, enterprise, network and application architects that want to understand ‘security’
- Roles can include:
  - Enterprise Security Architect (strategic and program mgmt.)
  - Solution Security Architect (technology project focused)
  - Security Engineers (technology implementation focused)

### Different Types of Security Architects

There are different types of security architects, depending on their specialization and background. For the purposes of this class, we will not focus on learning architectures per se, but rather on how to design and build **security** into the organization.

However, the chances are that you’ll have to wear quite a few hats in your organization, and maybe even design, build, oversee, operate and monitor yourself! That’s never a good idea, but it’s not uncommon. The convergence of security and IT roles due to the “move to the Cloud” have this effect in many organizations.

## Our Approach to Security Architecture & Engineering

- Focused on **implementation**
  - **Blue-team** approach: not an IT, enterprise, network or application 'architecture' class
  - But we will provide the methodology and tools needed to design and build defensible security architectures at each layer
- Risk-driven, **practical, hands-on** approach
  - Mapped to best practices and standards
  - Based on authors' experience on what works and what doesn't
  - Appropriate for the reality of a wide variety of organizations

### Our Approach to Security Architecture

Our approach to security architectures is a practical approach. We will cover strategy and tactics, but our focus will not be theoretical.

While assessing risk is an important part of doing security architectures, that by itself will not stop any attacks. It would be fantastic if we could tell our attackers to wait and do not attack us until we are done with our risk assessment, but that's not how things work. One of the authors has worked in risk assessment projects that have extended way over what it's considered practical, while the organization was lacking some obvious security controls that could have been implemented with little overhead. Is that practical?

This class has been written with a practical approach in mind, mapped to best practices and standards but also based on authors' experience on what works and what doesn't. We have also prioritized the areas that are most effective to defend against modern adversaries and their tactics, along with those that are most commonly overlooked.



## Learning Through Case Studies

### Welcome to Tyrell Corporation!

- A powerful corporation that develops highly advanced technology, with a not so 'advanced' security architecture.
- We will use Tyrell Corporation to illustrate and visualize many of the contents covered in SEC530
- Don't worry, having watched the movie is not a pre-requisite 😊

**BLADE  
RUNNER**



### Learning Through Case Studies

To make things a little bit more interesting, we will frame some of our discussions using a case study based on Tyrell Corporation<sup>1</sup>.

The Tyrell Corporation is a powerful corporation from the 1982 Ridley Scott film Blade Runner. Based in Los Angeles in the year AF 19, Tyrell is named after its founder Eldon Tyrell and is a high-tech corporation primarily concerned with the production of androids known as replicants.

The company's motto is "More human than human".

[1] [http://bladerunner.wikia.com/wiki/Tyrell\\_Corporation](http://bladerunner.wikia.com/wiki/Tyrell_Corporation)

## A Common Language: The OSI Model

- We will not cover the OSI model in depth neither will follow it exactly layer by layer, but it provides us a 'common language' to discuss common features, devices, and protocols at each layer:
  - Layer 1: Physical (electricity, light, radio waves, copper, fiber, cabling, bits, hubs, etc.)
  - Layer 2: Data Link (frames and switches)
  - Layer 3: Network (IP addresses, routers, routing, etc.)
  - Layer 4: Transport (TCP and UDP, ports)
  - Layer 5: Session (NetBIOS, RPC)
  - Layer 6: Presentation (graphics, character sets)
  - Layer 7: Data (applications and data)

<b>7</b>	<b>Application</b>
<b>6</b>	<b>Presentation</b>
<b>5</b>	<b>Session</b>
<b>4</b>	<b>Transport</b>
<b>3</b>	<b>Network</b>
<b>2</b>	<b>Data Link</b>
<b>1</b>	<b>Physical</b>

### A Common Language: The OSI Model

The standard reference model for protocol stacks is the International Standards Organizations (ISO) Open Systems Interconnection (OSI) model. The OSI model divides network communications into seven layers. A layered network model allows changing one layer (such as changing from a wired to wireless Ethernet connection) without affecting others (such as your browser).

We will not be covering the OSI (Open Systems Interconnection) model in depth, but 'hitting the highlights,' focusing on the terms we will use during 530, such as 'layer 1,' 'layer 2,' etc.

The Protocol Data Units (PDUs) are also useful to know. They are how we describe the data at each layer. The PDUs are:

- Layer 1: Bits
- Layer 2: Frames
- Layer 3: Packets
- Layer 4: Segments (TCP) or Datagrams (UDP)
- Layer 5-7: Data

PDUs are a TCP/IP model concept, and the TCP/IP model is older (and simpler) than the OSI model. OSI layers 5 through 7 are considered one layer in the TCP/IP model (called the application layer), which is why the PDU is 'data' for those layers.

## Main Topics Covered in SEC530

- Defensible Security Architecture
- Network Security Architecture
- Network-Centric Application Security Architecture
- Data-Centric Application Security Architecture
- Zero-Trust Architecture
- Defend the Flag **NETWARS** Challenge

### Main Topics Covered in SEC530

Although the course will perform a deep dive into many different facets of information security, a cursory review of the main topics will give you a better sense of how the major pieces and parts will fit together.

The next several slides provide a simple overview of major topics to be covered over the next six days so that you can be mentally prepared for the material presented.

The major topics include:

- Defensible Security Architecture
- Switch and Router Security
- Application Layer Security
- Data Security Architecture
- Zero-Trust Architecture
- Defend the Flag NetWars Challenge

## How This Class Flows

### Days 1 & 2

- Traditional vs defensible security architecture
- Security models and winning techniques
- Defensible security architecture lifecycle
- Main emphasis is on network security at layers 1-4
- From VLANs and PVLANS to firewall zoning and DMZs
- Best practices to secure switches, routers and wireless
- Flow data and IPv6

### How This Class Flows

In days 1 and 2, we will introduce the fundamentals of security architectures and will start hardening our organizations from the bottom up, from the physical layer to the network.

## How This Class Flows Cont.

### Days 3 & 4

- Day 3 focuses on network-based controls for application layer security such as NGFW, NSM, network encryption, remote access, jump boxes, and DDoS protection
- Day 4 focuses on a data-centric approach to securing the application security layer, including WAF, DB controls, data encryption, file classification, DLP, MDM, Cloud security and containers.

### How This Class Flows Cont.

Many security technologies have a heavy emphasis on network security. The assumption is that good and bad traffic need to be identified and treated appropriately. Technologies such as NGFW and IDS are a critical control that should be in place. Primarily, these technologies are network-centric defenses. Their main placement use is to protect all or many assets. This will be the focus on Day 3. However, more is necessary.

An additional approach that needs to be considered is data-centric security. The difference is a data-centric approach focuses in on how to secure key data. For example, if you have a large database containing patient healthcare records, then that database needs more security controls than a database containing web server logs. Basically, a data-centric approach identifies key data and applies purpose-built technologies to help protect it. This will be the focus of Day 4.

## How This Class Flows Cont.

### Day 5

- Understanding zero trust principles, model and architectures
- Practical application of zero trust through existing infrastructure:
  - Credential rotation, securing traffic on windows networks, host-based firewalls, NAC, segmentation gateways, SIEM, log collection, audit policies, host hardening, patching and red herring defenses.

### How This Class Flows Cont.

On Day 5 we will cover the zero trust principles and model briefly while we focus practical implementations of this new philosophy.

## How This Class Flows Cont.

### Day 6

#### Capstone goals:

- Put everything we have learned this week into hands-on practice
- Learn
- Have fun while competing to win

Hints are available and can be used strategically and/or to complete each challenge

- **Anyone** can complete the entire challenge

# NETWARS



## How This Class Flows Cont.

Finally, we will wrap up the week defending the flag with a super fun Netwars competition!

## SEC530 VM

- VMware Workstation 11+, Player 7+, or Fusion 7+
- 25 GB of free disk space
- Wireless Ethernet 802.11 B/G/N/AC
- CPU: **64 bit** 2.0+ GHz or higher (Important - Please Read: a **64-bit** system processor is **mandatory**)
- BIOS/UEFI: VT-x, AMD-V, or equivalent enabled
- RAM: >=8GB RAM
- A Linux VM is provided
  - USB 3.0 Ports Highly Recommended
  - Administrative access to disable any host-based firewall

### SEC530 VM

A properly configured system is required for each student participating in this course. These are mandatory requirements.

You can use any 64-bit version of Windows, Mac OSX, or Linux as your core operating system that also can install and run VMware virtualization products. You also must have **8 GB of RAM** or higher for the VM to function properly in the class.

It is critical that your CPU and operating system **support 64-bit** so that our 64-bit guest virtual machine will run on your laptop.

In addition to having 64-bit capable hardware, AMD-V, Intel VT-x, or the equivalent must be enabled in BIOS/UEFI.

You must have downloaded and installed VMware Workstation 11, VMware Fusion 7, or VMware Workstation Player 7 or higher versions on your system prior to the beginning of the class. If you do not own a licensed copy of VMware Workstation or Fusion, you can download a free 30-day trial copy from VMware. VMware will send you a time-limited serial number if you register for the trial on its website.



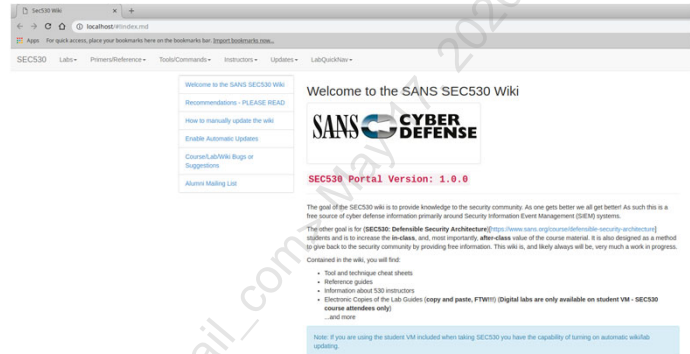
## SEC530 Wiki

Within the Linux VM you will find the SEC530 Course Portal (or wiki)

- Default homepage of your web browser

Some of what the SEC530 Portal includes:

- Electronic versions of workbook labs (copy & paste)
- Lab videos
- Course Index
- Course MP3s
- Additional resources



This page intentionally left blank.

## Authors and Instructors – Community

### Authors:

- Eric Conrad (@eric\_conrad)
- Justin Henderson (@securitymapper)
- Ismael Valenzuela (@aboutsecurity)

### Course errors/updates

- [justin@hasecuritysolutions.com](mailto:justin@hasecuritysolutions.com)
- [ivalenzuela@sans.edu](mailto:ivalenzuela@sans.edu)

### Instructors

- Josh Johnson (@jcjohnson34)
- Greg Scheidel (@greg\_scheidel)
- Ryan Nicholson (@ryan Nicholson)

### Other

- #SEC530
- SANS (@SANSInstitute)
- Cyber Defense (@SANSDefense)
- <http://sec530.com/slack>
- <https://wiki.sans.blue>

This page intentionally left blank.

## Icons

- Throughout the course material, there are icons to help to describe the different phases of the security architecture lifecycle and other elements that will help us during in-class discussion



Discover & Assess



Re-Design



Implement



Operate & Monitor



Threats

### Icons

To help us discuss the different layers and technologies covered in class, we have organized the material around a specific structure that we will cycle over. The icons used throughout the material will help us to identify these different elements and keep focus throughout the in-class discussion.

## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. Course Overview
2. **Defensible Security Architecture**
3. Traditional Security Architecture Deficiencies
4. Winning Defensible Security Techniques
5. Security Models
6. Threat, Vulnerability, and Data Flow Analysis
7. EXERCISE: Egress Analysis
8. Physical Security
9. Wireless
10. Layer 2 Attacks and Mitigation
11. EXERCISE: Identifying Layer 2 Attacks
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. EXERCISE: Architecting for Flow Data
16. 530.1 Summary

### Course Roadmap

Each section of this course presents a Course Roadmap slide to help you follow where we are in the course material. These “you are here” slides will also help you easily locate information for after-class review.

This first section provides an overview of the 530 course.

## Where We Came From

*“I know one of the guys who helped create the ARPANET, and he said security was not part of the statement of work.”*

- Michael Hayden, former NSA Director (2016)

- ARPANET was the first TCP/IP network created by the U.S. military - the precursor infrastructure for what we now refer to as the Internet.
- The massive growth of IP adoption over the ‘80s and ‘90s led to the birth of NAT, which led to perimeter defense.

### Where We Came From

Best military generals throughout history have been masters at using the terrain to gain the advantage on enemies and allow the good guys to outmaneuver their opponents in the battlefield. Unfortunately, this proven tactic has gone by the wayside when it comes to cyberspace.

[1] <https://www.forbes.com/sites/forbestechcouncil/2017/09/21/building-a-strong-foundation-how-network-architecture-dictates-it-security/#13bf7f793d5b>

## Where We Came From

- Perimeter defense is "a sort of crunchy shell around a soft, chewy center."<sup>1</sup>
  - Bill Cheswick (1990), describing the first internet gateways (proxy firewalls)
- This was a reasonable design in 1990
- We have come a long way since then, but many organizations still have this "candy bar" design
  - Hard on the outside, soft on the inside
  - Flat networks with little to no internal segmentation
  - A hardened perimeter, but with weaker/unpatched internal systems

### Where We Came From

Bill Cheswick's seminal 1990 paper, "The Design of a Secure Internet Gateway,"<sup>2</sup> described the first internet proxies (which he called gateways). Bill describes the inspiration for the first proxies:

*The design of a Corporate gateway to the Internet must deal with the classical tradeoff between security and convenience. Most institutions opt for convenience and use a simple router between their internal internets and the rest of the world. This is dangerous. Strangers on the Internet can reach and test every internal machine. With workstations sitting on many desks, system administration is often decentralized and neglected. Passwords are weak or missing. A professor or researcher often may install the operating system and forget it, leaving well-known security holes uncorrected. For example, a sweep of 1,300 machines inside Bell Labs around the time of the Internet Worm found over 300 that had at least one of several known security holes.<sup>3</sup>*

The "Internet Worm" he described was the Morris Worm, released in 1988 by William Tappan Morris Jr. Much like World War I (called the "Great War" at the time), the first major worm was called the "Internet Worm" at the time. You may learn more about the Morris Worm at:  
<http://groups.csail.mit.edu/mac/classes/6.805/articles/morris-worm.html>

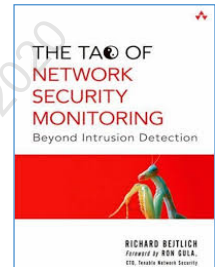
[1] <http://www.cheswick.com/ches/papers/gateway.pdf>

[2] Ibid.

[3] Ibid.

## Defensible Security Architecture

- The term "Defensible Networks" was coined by Richard Bejtlich in *The Tao of Network Security Monitoring*
  - *I use the term defensible networks to describe enterprises that encourage, rather than frustrate, digital self-defense.*<sup>1</sup>
- Bejtlich makes these points about defensible networks:
  - *Defensible networks can be watched*
  - *Defensible networks limit an intruder's freedom to maneuver*
  - *Defensible networks offer a minimum number of services*
  - *Defensible networks can be kept current*<sup>1</sup>



### Defensible Security Architecture

Richard Bejtlich is (in the course authors' opinion) one of the godfathers of the blue team, along with Clifford Stoll (famous for writing the Cuckoo's Egg<sup>3</sup>). "Blue team" refers to defenders, the "red team" describes the offense (such as penetration testers).

Bejtlich also wrote a number of other useful books for blue teamers, including:

- The Practice of Network Security Monitoring (2013)
- Extrusion Detection: Security Monitoring for Internal Intrusions (2005)

Links to these (and others) available here: <https://www.taosecurity.com/books.html>

[1] <http://www.informit.com/store/>

[2] Ibid.

[3] <http://www.simonandschuster.com/books/The-Cuckoos-Egg/Cliff-Stoll/9781416507789>

## Defensible Network Architecture 2.0

Richard Bejtlich later refined the idea of Defensible Networks, using the term Defensible Network Architecture 2.0, which he described as having the following characteristics:

- Monitored
  - Deploy IDSeS and IPSeS
- Inventoried
  - Know every host and application
- Controlled
  - Ingress and egress filtering
- Claimed
  - Identify owners of all systems
- Minimized
  - Reduce the attack surface
- Assessed
  - Conduct vulnerability assessments
- Current
  - Patched<sup>1</sup>

### Defensible Network Architecture 2.0

Richard Bejtlich later refined his idea of Defensible Networks in 2008, using the term Defensible Network Architecture 2.0.<sup>2</sup> He used the mnemonic MICCMAC ("mick-mack"): Monitored, Inventoried, Controlled, Claimed, Minimized, Assessed. And Current.<sup>3</sup>

Bejtlich explains Defensible Network Architecture 2.0:

*Four years ago when I wrote *The Tao of Network Security Monitoring* I introduced the term defensible network architecture. I expanded on the concept in my second book, *Extrusion Detection*. When I first presented the idea, I said that a defensible network is an information architecture that is monitored, controlled, minimized, and current. In my opinion, a defensible network architecture gives you the best chance to resist intrusion, since perfect intrusion prevention is impossible.*

*I'd like to expand on that idea with *Defensible Network Architecture 2.0*. I believe these themes would be suitable for a strategic, multi-year program at any organization that commits itself to better security. You may notice the contrast with the *Self-Defeating Network* and the similarities to my *Security Operations Fundamentals*. I roughly order the elements in a series from least likely to encounter resistance from stakeholders to most likely to encounter resistance from stakeholders.<sup>4</sup>*

[1] <https://taosecurity.blogspot.com/2008/01/defensible-network-architecture-20.html>

[2] Ibid.

[3] Ibid.

[4] Ibid.



## The Mindset of Defensible Security Architecture

- Defensible security architecture is entirely complementary to traditional network architecture approaches that focus primarily on operations
  - Often at the expense of security
- The mindset is "build it once, build it right"
  - All networks must perform their operational functions effectively
  - Security can be complementary to this goal
  - It is (much) more efficient to bake security in at the outset, rather than retrofitting it later
- For example: your team configures robust logging using a secure template as part of their new router deployment process
  - This logging later helps detect an operational issue that is impacting performance
  - The problem is solved before users are aware of any issue

### The Mindset of Defensible Security Architecture

Security is not in opposition to operations: when performed properly, security enhances operations.

A course author encountered high amounts of IP fragmentation while diagnosing an IDS (Intrusion Detection System) performance issue, which was caused by an IPsec tunnel that created packets larger than 1500 bytes. Many encrypted tunnels (including GRE and IPsec) can create packets that are larger than 1500 bytes, which typically requires fragmenting one packet into two. This lowers performance and causes applications to run slowly, time out, or fail.

Cisco describes the issue. "The 1500-byte packet is encrypted by IPsec and 52 bytes of overhead are added (IPsec header, trailer, and additional IP header). Now IPsec needs to send a 1552-byte packet. Since the outbound MTU is 1500, this packet will have to be fragmented."<sup>1</sup> The solution is simple (and also described in Cisco's "Resolve IP Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPsec"<sup>2</sup>

The author opened a ticket, asking the client's server engineering team to adjust the MSS (Maximum Segment Size) of the sending systems, lowering it to account for the extra 52 bytes of data. The ticket was initially closed with no action; the rationale was, "Not a security problem." It took some arm wrestling to convince the engineers it was both a security and an operational issue. They finally made the change, and client sites (connected via point-to-point VPN connections) reported a significant boost in application speeds.

[1] <https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html>

## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. Course Overview
2. Defensible Security Architecture
3. **Traditional Security Architecture Deficiencies**
4. Winning Defensible Security Techniques
5. Security Models
6. Threat, Vulnerability, and Data Flow Analysis
7. EXERCISE: Egress Analysis
8. Physical Security
9. Wireless
10. Layer 2 Attacks and Mitigation
11. EXERCISE: Identifying Layer 2 Attacks
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. EXERCISE: Architecting for Flow Data
16. 530.1 Summary

### Course Roadmap

We will next discuss traditional security architecture deficiencies.

## Traditional Security Architecture Deficiencies

- Traditional deficiencies in security architecture include:
  - Emphasis on perimeter
    - Lack of true perimeter (de-perimeterization via cloud/mobile/IoT)
  - Most (and sometimes virtually all) controls emphasize exploitation prevention
  - The Internet of Things (IoT)
  - Predominantly network-centric
  - Compliance-driven security
  - Resistance to change
  - Introducing technology without analysis

### Traditional Security Architecture Deficiencies

Traditional deficiencies in security architecture include:

- Emphasis on perimeter
- Lack of true perimeter (de-perimeterization via cloud/mobile/IoT)
- Most (and sometimes virtually all) controls emphasize exploitation prevention
- The Internet of Things (IoT)
- Predominantly network-centric
- Compliance-driven security

Let's discuss each...

## Why Firewalls Were Created

- The firewall (and modern information security industry) gained steam in the wake of the Morris worm (released in 1988)
- Lesson learned: a globally flat ARPANET (the precursor to the internet) was a bad idea
  - The worm is estimated to have infected 10% of the ARPANET's 60,000 computers
- How many corporate WANs have more than 60,000 hosts today, and are also internally flat?
  - "Those who cannot remember the past are condemned to repeat it."<sup>1</sup> - George Santayana

### Why Firewalls Were Created

Robert Tappan Morris, Jr. released the worm (originally called "the Internet Worm") on November 2<sup>nd</sup>, 1988.

*On November 2, 1988, Robert Morris, Jr., a graduate student in Computer Science at Cornell, wrote an experimental, self-replicating, self-propagating program called a worm and injected it into the Internet. He chose to release it from MIT, to disguise the fact that the worm came from Cornell. Morris soon discovered that the program was replicating and reinfesting machines at a much faster rate than he had anticipated---there was a bug. Ultimately, many machines at locations around the country either crashed or became "catatonic." When Morris realized what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent reinfection. However, because the network route was clogged, this message did not get through until it was too late. Computers were affected at many sites, including universities, military sites, and medical research facilities. The estimated cost of dealing with the worm at each installation ranged from \$200 to more than \$53,000.<sup>2</sup>*

The United States also formed a national CERT (Computer Emergency Response Team) as a lesson learned, it is now called US-CERT.

How many corporate WANs approach the size of the 1988 ARPANET (or exceed it)? How many of those are fully flat internally (or nearly so)?

[1] <https://www.iep.utm.edu/santayan/>

[2] [https://www.cs.indiana.edu/docproject/zen/zen-1.0\\_10.html#SEC91](https://www.cs.indiana.edu/docproject/zen/zen-1.0_10.html#SEC91)

## Flat Networks Fail Catastrophically

- A 'flat' network offers little or no internal **filtering** at OSI layers 2 (Data Link), 3 (Network) and 4 (Transport)
  - Simply separating systems on VLANs (Virtual LANs, discussed later in 530.1) does not address this issue
  - There must also be ACLs (Access Control Lists) firewall rules, etc.
  - Note that VLANs are certainly a good idea, but filtering must also take place
- A flat network allows an intruder to reach a large number of other systems
  - For example: if an intruder can compromise one system, and then scan TCP port 445 (SMB) on hundreds or thousands of others: that network is too flat
- These networks fail catastrophically because one compromised system can endanger many others
- Internal network segmentation is required to address this risk

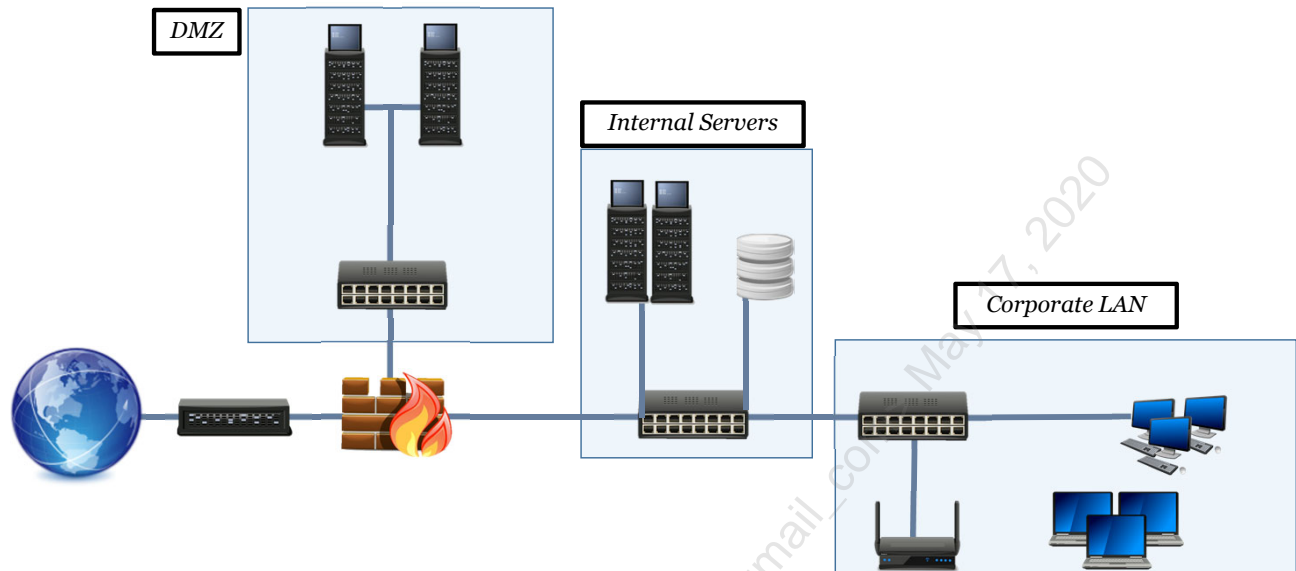
### Flat Networks Fail Catastrophically

The course authors use the term "magic VLAN solution:" place different systems on different VLANs, and all your problems magically melt away. While segmenting traffic at layer 2 is certainly a good idea (which we will discuss later in 530.1), VLANs do not automatically filter traffic. Additional steps must be taken, such as VLANs ACLs, filtering IP addresses at layer 3 and or ports at layer 4, etc.

Organizations like flat networks because they are quite easy to manage: for example, any two internal systems will be able to connect, with no firewall rules to manage.

The problem: if it's easy for any two internal systems to connect, that also makes it easy for an intruder to pivot from one compromised system to another. While most companies are diligent in patching and hardening internet-facing systems, the same is not always true internally.

## Case Study: Tyrell Corporation



### Case Study: Tyrell Corporation

As discussed, we are going to use Tyrell Corp. to illustrate some of the issues and solutions proposed throughout this class, and to frame some of the discussions we will have during the week. This is what Tyrell's network looks like today.

Like many organizations, they have very little segmentation in place, with only 3 zones defined: INTERNET, DMZ and LAN.

Notice how the internal servers and the corporate LAN are effectively on the same segment, only connected to 2 different switches. The internal servers include domain controllers and databases that may contain confidential information, and that may be critical to Tyrell's business.

Can anything go wrong with this approach?

## Case Study: NotPetya

- NotPetya is part of a family of malware based on the leaked (alleged) NSA hacking tools, including ETERNALBLUE
  - This exploit targeted Windows Server Message Block (SMB, TCP port 445) and was patched by MS17-010<sup>1</sup>
- This malware would typically enter an environment via SMB
  - It would then use Mimikatz to attempt to steal credentials and move laterally through a network via Microsoft PSEXEC and WMIC (Windows Management Instrumentation Console)
  - Automated malware is now behaving like human penetration testers
- If an organization had one unpatched system and 999 patched: all 1,000 could become compromised
  - This is dependent on internet network segmentation, trust models, etc.

### Case Study: NotPetya

In the old days: worms were dumb, often called 'breeders not warriors.' For example, if an organization had 1,000 systems, and one was missing the patch MS08-067<sup>2</sup>, then the Conficker<sup>3</sup> worm could compromise that one system. It would then attempt to pivot (move laterally) and attack the other 999 systems. These attacks would fail because the systems were patched.

That is now changing: NotPetya could compromise that one system, steal Windows credentials from it, and then attempt to spread via Microsoft PSEXEC or WMIC (this is exactly what a human penetration tester would do). In the end: all 1,000 systems could become compromised, despite virtually all being patched.

According to The Register:

*Crucially, NotPetya seeks to gain administrator access on a machine and then leverages that power to commandeer other computers on the network: it takes advantage of the fact that far too many organizations employ flat networks in which an administrator on one endpoint can control other machines, or sniff domain admin credentials present in memory, until total control over the Windows network is achieved.<sup>4</sup>*

[1] <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>

[2] <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067>

[3] <http://malware.wikia.com/wiki/Conficker>

[4] [https://www.theregister.co.uk/2017/06/28/petya\\_notpetya\\_ransomware/](https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/)

## Case Study: Petya Victims

- Shipping company Maersk reported a \$200 - \$300 million (US) dollar loss<sup>1</sup>
- FedEx TNT Reported a \$300 million dollar loss<sup>1</sup>
- Pharmaceutical company Merck also reported a \$300 million dollar loss
- Mondelez International (the world's 2nd-largest confectionary company and makes of Cadbury) reported a 5% drop in quarterly sales<sup>4</sup>
- Additional victims include British consumer goods company Reckitt Benckiser (\$115 million) and Beiersdorf AG (make of Nivea skin cream) and French construction company Saint-Gobain (\$387 million)<sup>5</sup>

### Case Study: Petya Victims

While financial losses are staggering (over a billion \$USD was noted in the slide above), NotPetya also introduced potential risk to human life and safety due to potential slowdowns in prescription drugs. Reuters reported:

*The impact on Merck was particularly troubling because it affected the firm's ability to produce medicines, said Joshua Corman, director of the Cyber Statecraft Initiative at the Atlantic Council.*

*"This is serious. It affects human lives," Corman said. "Imagine if the supply of something like H5N1 influenza vaccine was affected when we needed them."<sup>4</sup>*

[1] <https://threatpost.com/maersk-shipping-reports-300m-loss-stemming-from-notpetya-attack/127477/>

[2] [https://www.theregister.co.uk/2017/09/20/fedex\\_notpetya\\_damages/](https://www.theregister.co.uk/2017/09/20/fedex_notpetya_damages/)

[3] <https://threatpost.com/pharmaceutical-giant-still-feeling-notpetyas-sting/127130/>

[4] <https://www.reuters.com/article/cyber-results/cyber-worm-attack-hits-global-corporate-earnings-idUSL1N1KO0VB>

[5] <http://www.ansbachblog.com/2017/08/the-true-costs-of-recent-ransomware-attacks-mass-business-disruption-hundreds-of-millions-lost/>



## Failed Mindset: The LAN Is Secure

- Most layer 2, 3, and 4 protocols have little or no built-in security
  - These include ARP, CDP (and many others), as we will discuss later in SEC530
- The course authors have witnessed organizations that ignore layer 2 hardening advice based on this flawed mindset:
  - "An ARP cache poisoning attack requires local subnet access, and since the black hat is not on the local LAN, we have no risk..."
  - This presumes that no system will ever become compromised in the future
  - Past compromise history usually indicates this is a flawed assumption

### Failed Mindset: The LAN Is Secure

Many organizations ignore basic layer 2 hardening best practices on the flawed assumption that the black hat requires local access to launch them. Since the black hats are on the outside: there is little to no risk.

This assumes no internal system will ever become compromised. Assume a black hat compromises a local system via a phishing campaign and installs an agent (such as Metasploit's Meterpreter) on that system. The black hat now has layer 2 access to that local subnet and will be able to launch a wide variety of layer 2 attacks, including ARP cache poisoning, MAC address spoofing, DHCP (Dynamic Host Configuration Protocol) attacks, and many others.

We will discuss ARP, CDP (Cisco Discovery Protocol), DHCP (Dynamic Host Configuration Protocol), and many other protocols in detail later in 530.1.

## Failed Mindset: Perimeter-Based Security Model

- "The WAN is trusted, so..."
  - Many bad things have occurred due to this mindset
- The "inside == trusted", "outside == untrusted" leads to risky assumptions and decisions
  - Do you encrypt internal network traffic?
  - If you could do so trivially (for example: via tunnels on core routers): why not?
- Admittedly, \*some\* organizations maintain an actual perimeter
  - These tend to be more common in government/military organizations
  - And even these can fail

### Failed Mindset: Perimeter-Based Security Model

A course author had a client who was concerned about the ease of sniffing VoIP (Voice over IP) traffic. There are a number of ways to mitigate this risk; the easiest for this network (which had older VoIP equipment) was to tunnel the traffic between the routers. Newer environments could use SRTP and SIP via TLS.<sup>1</sup>

All of the VoIP devices were already placed on separate VLANs (Virtual LANs, which we will discuss later in 530.1) and subnets (this is often true, due to the multicast groups typically created for VoIP systems). The Cisco routers had plenty of CPU and RAM to handle the task, and the network had more than enough capacity to handle the additional bandwidth requirements. A small test showed performance was fine.

The head of network engineering pushed back, saying "The WAN is trusted! We don't encrypt traffic on the WAN..."

The hardest part of the project was changing this mindset.

[1] <https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/tips-ip-phone-security.html>

## De-Perimeterization

- De-Perimeterization describes the destruction of the classic network perimeter via the cloud, mobile devices, and the Internet of Things (IoT)
- Typical perimeter controls (such as firewalls) struggle to secure these devices and services
  - If you allow services such as Gmail...
  - You probably allow Google Docs
- Many of these devices and services escape the scrutiny that classic network devices such as desktops and servers receive
  - Existing controls for these devices and services are often quite immature

### De-Perimeterization

Classic firewall/perimeter design is often described using a castle analogy: the walls are the firewall, protecting devices on the inside.

The rise of cloud, mobile devices and the Internet of Things (IoT) makes this model (and analogy) far less effective.

Below are the options for sharing data via Google Docs. These are selectable by the owner (usually the creator or uploader). The first option openly shares data on the web (and Google will typically find and index the link). Allowing users to choose one of these settings creates a significant risk of accidentally exposing data.

Link sharing

- On - Public on the web**  
Anyone on the Internet can find and access. No sign-in required.
- On - Anyone with the link**  
Anyone who has the link can access. No sign-in required.
- On - Backshore Communications**  
Anyone at Backshore Communications can find and access.
- On - Anyone at Backshore Communications with the link**  
Anyone at Backshore Communications who has the link can access.
- Off - Specific people**  
Shared with specific people.

Access: Anyone (no sign-in required) [Can view](#) ▾

Note: Items with any link sharing option can still be published to the web. [Learn more](#)

[Save](#) [Cancel](#) [Learn more about link sharing](#)

## Failed Mindset: The All-Prevent Defense

- Firewalls, antivirus, patching, host and network-based IPSes (HIPS and NIPS) are primarily preventive controls
  - These are fine controls
- The "All-Prevent Defense" refers to an over-reliance on purely preventive controls, at the expense of defensive controls
  - Note that prevention is a critical, and required, layer of defense in depth
  - Many organizations possess little effective detective capabilities
  - Detection is often outsourced, sometimes driven by compliance needs
  - Compliance != security

### Failed Mindset: The All-Prevent Defense

Any good defender knows that you may also detect with a firewall (by inspecting the logs), but there is little argument that a firewall is primarily a preventive control.

Preventive controls are great: they offer low Total Cost of Ownership (TCO) and, **when they are successful**, automatically mitigate risk. The catch is 'when they are successful', because all prevention will fail. Firewalls fail, antivirus fails, patching may fail, etc.

The question is: what then? What effective detective controls does the organization possess when prevention ultimately fails? The answer is often little to none. Outsourcing detection is common via MSSPs (Managed Security Service Providers). This can serve as a good control for compliance, but how effective are they for actual security? Remember: compliance does not equal security: compliance is a (critical) subcomponent of security.

A recent Verizon Data Breach Investigation Report (DBIR) reported that outsourced "Monitor Services" were 1% effective at detecting the breaches they investigated. See: <https://enterprise.verizon.com/resources/reports/dbir/>

## The Internet of Things (IoT)

- The Internet of Things (IoT) describes low-cost Internet-enabled devices
  - Video cameras, kitchen appliances, DVRs, televisions, children's toys, etc., etc.
  - These devices are often very inexpensive, leaving little to no revenue to support patches, firmware updates, etc.
- "Hypponen's law: Whenever an appliance is described as being "smart", it's vulnerable."<sup>1</sup>



**The Internet of Things (IoT)** is currently undergoing an explosion, expanding rapidly. Anyone who has bought a television lately can attest to this fact: try to buy one **without** internet connectivity. They are quite hard to find!

Quoting Hypponen, "The core of the problem is that when you go and buy an appliance, security isn't a selling point. You go and buy a toaster or washing machine ... clearly price is number one. Number two: colour. Security doesn't even enter the discussion, which means the vendor making these things will invest the minimum amount of money possible into security,"<sup>2</sup>

In other words: The Internet of Things is an area where the (typical) buyer \*and\* seller of a product doesn't care about security. The devices usually have low margins, leaving little room for additional features (such as patches or firmware updates). This makes addressing the challenge quite difficult.

[1] <https://twitter.com/mikko/status/808291670072717312>

[2] <https://www.businessinsider.com/dyn-hack-calls-grow-regulation-internet-of-things-security-mikko-hypponen-f-secure-interview-2016-10>

## Network-Centric Architecture

- Security architecture comes in a variety of flavors
  - Network-based, host-based, application-based, product-based, etc.
- The term "security architect" is often applied too narrowly to network architecture
  - This is a critical component, but the others are also important
  - "Network security architect" is a well-known job title, but there are less "Host-based security architects" (etc.)
- The recent generation of attacks have moved to the host itself, via layer 7, and often leveraging encryption
  - This makes taking a broader view of architecture critical

### Network-Centric Architecture

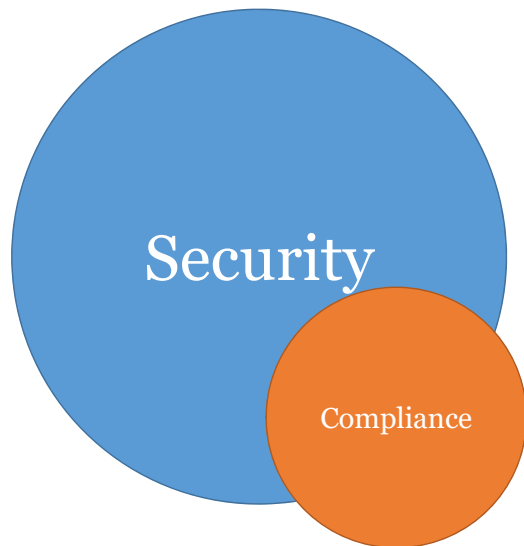
In the slide above, "layer 7" describes the application and its data. We won't stop to describe the OSI model in depth, Microsoft has a nice description<sup>1</sup> if you'd like to research it a bit more.

Traditional controls such as firewalls perform a poor job of mitigating layer 7 attacks. Next generation firewalls attempt to fill part of this gap, and while they are fine controls, they can also fail. "Malware detonation devices" (automated sandboxes) exist for this reason: they can take an email attachment, drop it into a virtual machine, simulate a user clicking, and then detect changes to the filesystem, changes to the registry, DNS requests, outbound network connections, etc. The fact that these devices exist speaks to the fact that other components may fail here.

A layer 7 attack could include a phishing email containing a 'poison PDF' (meaning a PDF containing malware). Most corporate firewalls and mail servers will allow incoming mail containing PDF attachments. This means the PDF will likely reach the user's inbox, assuming it passes whatever antimalware checks are in place, such as antivirus, reputation services, etc. Should these fail to detect the malware, host-based controls (and user awareness) are the next layers of defense in depth.

[1] <https://docs.microsoft.com/en-us/windows-hardware/drivers/network/windows-network-architecture-and-the-osi-model>

## Failed Mindset: Compliance-Driven Security



A common failing of information security teams: compliance-driven security

- Meeting compliance requirements becomes the goal, often divorced from (larger) security needs

Compliance-driven security tends to fail in the face of a persistent adversary

Assessing without remediating is common in these organizations

### Failed Mindset: Compliance-Driven Security

Compliance-driven security can be harmful towards overall information security when it is viewed as the primary security end-goal. The goal of compliance is valid, and compliance controls are helpful when part of a larger security process.

Think about all of the credit card breaches companies have suffered. Bryan Krebs reported on the following breaches in 2017 and 2018 (note that this is a partial list):

- Arby's, B&B Theaters, Buckle Stores, Equifax, Gamestop.com, Hyatt Hotels, InterContinental Hotels Group, Jason's Deli, K-Mart, Shoney's, Sonic Drive-In, and Trump Hotels

All of these organizations were presumably PCI DSS (Payment Card Industry Data Security Standard, a mandated industry compliance standard for organizations that accept credit cards) compliant and passed their most recent PCI audit. Note that being PCI compliant is undoubtedly a good thing, but the point is: it's not enough. Organizations must go beyond complying with the letter of the compliance standard.

[1] <https://krebsonsecurity.com/>

## Failed Mindset: We Always Did It This Way

- Some IT folks build entire careers by delaying or rejecting necessary change
- They often populate change management boards, advising 'caution', and 'prudence'
- The screenshot on the right is from the OSS (precursor to the United States CIA) Simple Sabotage Field Manual<sup>1</sup>
  - "This classified booklet described ways to sabotage the US' World War II enemies."<sup>2</sup>

(11) *General Interference with Organizations and Production*

(a) *Organizations and Conferences*

(1) Insist on doing everything through "channels." Never permit short-cuts to be taken in order to expedite decisions.

(2) Make "speeches." Talk as frequently as possible and at great length. Illustrate your "points" by long anecdotes and accounts of personal experiences. Never hesitate to make a few appropriate "patriotic" comments.

(3) When possible, refer all matters to committees, for "further study and consideration." Attempt to make the committees as large as possible — never less than five.

(4) Bring up irrelevant issues as frequently as possible.

(5) Haggle over precise wordings of communications, minutes, resolutions.

(6) Refer back to matters decided upon at the last meeting and attempt to re-open the question of the advisability of that decision.

(7) Advocate "caution." Be "reasonable" and urge your fellow-conferrees to be "reasonable" and avoid haste which might result in embarrassments or difficulties later on.

### Failed Mindset: We Always Did It This Way

The OSS (Office of Strategic Services) was the precursor of the United States Central Intelligence Agency (CIA). The Simple Sabotage Field Manual was released in 1944.

The course authors have been on seemingly countless change management meetings where other participants attempt to delay or stop many meaningful changes. They seem to think they are trying to help, by advocating caution, more testing, delaying until after the current IT project is complete (only to be followed by another one), etc. They often seem well intended, but their effect can be disastrous.

Home Depot had a famous breach in 2014. IT folks were aware of security issues in their infrastructure and approached management many times seeking funding to address them.

*Several former Home Depot employees said they were not surprised the company had been hacked. They said that over the years when they sought new software and training, managers came back with the same response: "We sell hammers."<sup>3</sup>*

[1] <https://www.cia.gov/news-information/featured-story-archive/2012-featured-story-archive/simple-sabotage.html>

[2] Ibid.

[3] [https://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html?\\_r=0](https://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html?_r=0)



### Failed Mindset: Introducing Technology without Analysis

Introducing new technology into the organization driven by the so called ‘shiny object syndrome’, often dictated by:

- Analysts or media
- Vendors
- Your latest incident response report

Without considering:

- Alignment to business strategy
- How it ties to your overall architecture
- How effectively it mitigates risk for the organization

#### Failed Mindset: Introducing Technology without Analysis

Likewise, introducing new technology into the organization driven by the so called ‘shiny object syndrome’, often dictated by other parties that know little about your own organization, is a common failure.

Tools are important and necessary elements of a solid security architecture but without careful planning and consideration they might be not only of little help but can also give you a false sense of security.

## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

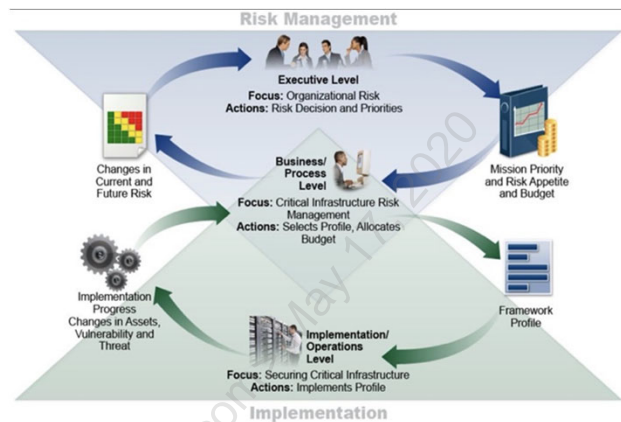
1. Course Overview
2. Defensible Security Architecture
3. Traditional Security Architecture Deficiencies
4. **Winning Defensible Security Techniques**
5. Security Models
6. Threat, Vulnerability, and Data Flow Analysis
7. EXERCISE: Egress Analysis
8. Physical Security
9. Wireless
10. Layer 2 Attacks and Mitigation
11. EXERCISE: Identifying Layer 2 Attacks
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. EXERCISE: Architecting for Flow Data
16. 530.1 Summary

### Course Roadmap

We will next discuss winning defensible security techniques.

## Risk-Driven and Business Outcome-Focused Architecture

- Effective and valuable security architectures require measuring the risk, costs, and benefits of cybersecurity strategies and steps
- To do so, we will provide mappings to NIST CSF core functions (**Identify, Protect, Detect, Respond & Recover**) through our Wiki



NIST CyberSecurity Framework v1.1, April, 2018

### Risk-Driven and Business Outcome-Focused Architecture

Lack of context against threat profiles and attack methods often lead to ineffective architectures. At the same time, security management must provide ongoing reporting to key stakeholders to prioritize investments and ultimately manage risk.

To address that need, the NIST Cybersecurity Framework<sup>1</sup> provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk.

NIST CSF provides mappings to CSC, COBIT, ISO 27001 and NIST SP 800-53, among others, so it's a good document to use to navigate and cross-reference all these different standards and best practices that map to the domains we will use in this class. This will allow you to define architectures and implement controls that provide operational and cyber resilience while using a common language across your organization.

The Figure depicted on the slide describes a common flow of information and decisions at the following levels within an organization:

- Executive
- Business/Process
- Implementation/Operations

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process and to the implementation/operations level for awareness of business impact.

While we will not follow this process in class, it's important to understand that our security architectures design and implementation must be able to fit within this or similar risk management frameworks to ensure it provides ongoing value to the organization.

[1] <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

Licensed To: Martin Brown <hermespaul56@gmail\_com> May 17, 2020

## The Presumption of Compromise

- Network defenders should always operate under the presumption of compromise
  - Assume something on the network is already compromised
  - Then conduct threat hunting to discover intrusions that evaded prevention and initial detection
- Preventive controls **will** fail in the face of a persistent adversary
  - "Three words sum up my attitude toward stopping intruders: *prevention eventually fails.*"<sup>1</sup> – Richard Bejtlich, the *Tao of Network Security Monitoring*

### The Presumption of Compromise

Bejtlich Discusses the fact the prevention will fail in the preface of the *Tao of Network Security Monitoring*:

*Welcome to The Tao of Network Security Monitoring: Beyond Intrusion Detection. The goal of this book is to help you better prepare your enterprise for the intrusions it will suffer. Notice the term "will." Once you accept that your organization will be compromised, you begin to look at your situation differently.*<sup>2</sup>

Jake Williams discusses the Presumption of Compromise in his SANS Analyst Whitepaper "Server Security: A Reality Check":

*Server security is paramount to any organization. All too often, network defenses focus entirely on the perimeter, leaving networks looking like pieces of candy—having a hard outer shell and a soft gooey inside. In today's threat landscape, defenders must operate under the presumption of compromise. Attacks involving spearphishing, social engineering, weak bring your own device (BYOD) security, poor physical security of end-user equipment (for example, traveling laptops) and user carelessness contribute to the initial compromise of user endpoints. Once user endpoints are compromised, attackers typically use these as stepping off points to compromise other network assets.*<sup>3</sup>

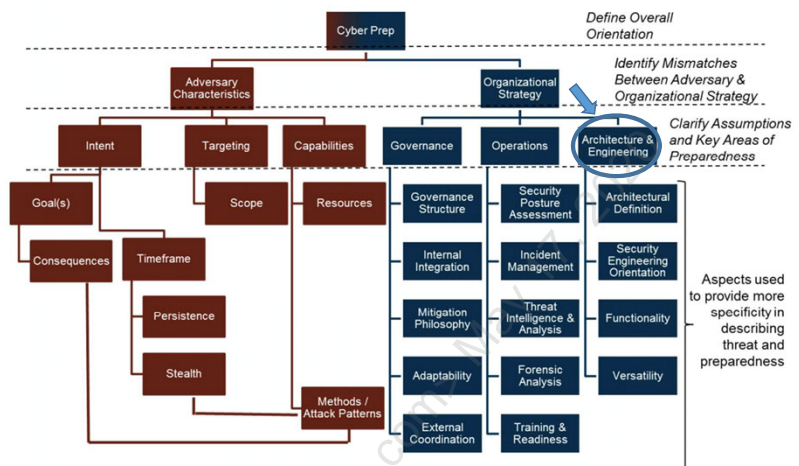
[1] <http://www.informit.com/store/tao-of-network-security-monitoring-beyondintrusion-9780321246776>

[2] Ibid.

[3] <https://www.sans.org/reading-room/whitepapers/analyst/membership/34725>

## Practical Threat Modeling: Purple Teaming

- We need to determine the characteristics of the adversaries which could be expected to target our systems so we can define and implement effective architectures and controls
- Purple teaming (**red** + **blue**) facilitate this by **working together** through simulation of specific threat scenarios



MITRE Cyber Prep 2.0, May 2017

### Practical Threat Modeling: Purple Teaming

From MITRE Cyber Prep 2.0<sup>1</sup>, May 2017:

Cyber Prep is a threat-oriented approach that allows an organization to define and articulate its threat assumptions, and to develop organization-appropriate, tailored aspects of a preparedness strategy. Cyber Prep focuses on advanced threats, but also includes material related to conventional cyber threats. Cyber Prep can be used in standalone fashion, or it can be used to complement and extend the use of other, more detailed frameworks (e.g., the NIST Cybersecurity Framework) and threat models.

An organization that seeks to improve its overall cybersecurity posture starts by acquiring cybersecurity products and tools and then abandoning them because it lacks the expertise or sufficient staff to use them effectively, or because it failed to clearly plan or resource the products and tools to make them operational. Cyber Prep helps an organization consider such interdependent aspects of preparedness as:

**Governance:** What is the organization’s overall approach to defending against cyber threats? How strongly integrated is cyber risk management with other aspects of organizational risk management? Is the focus on compliance or pushing state of the art to engage the APT better?

**Operations:** Is the organization simply reacting to incidents as they become evident, or are cyber defenders proactively engaging early and across the cyber attack life cycle? How much does the organization use threat intelligence in its operations? How integrated (or isolated) is the organization’s cyber security staff with other key players such as cyber defenders, malware analysts, and tool developers?

**Architecture & Engineering:** How well defined, and integrated with mission operations, is the organization’s security architecture? Are the organization’s security capabilities focused on some or all of the CSF core functions; do they go beyond the CSF and address aspects of cyber resiliency? What is the organization’s security engineering orientation?

[1] <https://www.mitre.org/sites/default/files/publications/16-0939-motivating-organizational-cyber-strategies.pdf>

## Look for Blue/Red Asymmetries

- Network architects and systems engineers should always seek to deploy defensive controls that are easy for the blue team (defenders) but make the red team's job (attackers) **much** more difficult
- For example: private VLANs
  - As we will discuss later in 530: private VLANs can be used to prevent clients from connecting to other clients
  - For organizations with good client/server network segmentation: this is often an easy win (users and IT staff usually fail to notice the change)
  - It prevents the client-client pivot: attackers can only pivot against servers

### Look for Blue/Red Asymmetries

Blue/red asymmetries offer great 'bang for the buck' to defenders. Another example is switch and router hardening, as we will discuss shortly. If performed properly: no end users will notice. But hardening switches and routers mitigate entire classes of attacks.

We will discuss all of the terms used above during 530. In the meantime: here's a quick primer.

A VLAN is a virtual LAN, a way to segment systems at OSI layer 2 (the data link layer, where switches live). A private VLAN means members of the same private VLAN cannot send traffic to each other. For client VLANs: it means the clients can send data to the switch, default gateway, DHCP and other servers, but not to other clients.

A pivot is an attack from one compromised system to another. It often occurs after one client is compromised (for example, during a phishing attack), and then the attacker uses that infected system to attack other internal systems (often behind the same firewall).

## Know Thy Network

- The 'prime directive' of both network engineering and network security architecture (NSM) is: know thy network
- This means knowing:
  - All of the systems that are on a network
  - All of the network services and protocols
  - The type and nature of the data on the network
    - Where that data may exist (such as PII) and where it may not
    - And where it must be encrypted

### Know Thy Network

Fortune 500 organizations have lost billions of dollars by refusing to heed the advice shown on the slide above. There is no "know thy network as a service": there is no shiny box, appliance, or outsourced option that can adequately replace a network engineer knowing his or her network.

This means servers and clients, ports and protocols, and expected data flow. It means knowing where the system's and network's sensitive data is allowed to reside on, and those where it is not. It means knowing where sensitive data must be encrypted, and where it does not. It also means understanding the business need for the data.

That understanding allows the engineer to design systems and networks properly, in accordance with what is already in place, as well as in harmony with that the business needs. A lack of understanding leads to poor solutions that do not mesh well with existing architecture, and sometimes at odds with what the business needs.



## Disrupting Nation State Hackers

Rob Joyce, former head of NSA's (National Security Agency) TAO (Tailored Access Operations) group:

- *If you really want to protect your network, you really have to know your network*<sup>1</sup>
- *"We put the time in ...to know [that network] better than the people who designed it and the people who are securing it," he said. "You know the technologies you intended to use in that network. We know the technologies that are actually in use in that network. Subtle difference. You'd be surprised about the things that are running on a network vs. the things that you think are supposed to be there."*<sup>2</sup>

### Disrupting Nation State Hackers

Rob Joyce, former head of the NSA's TAO group, gave a great talk on Disrupting Nation State Hackers at USENIX Security Enigma 2016 conference. The video is available here and is well worth 35 minutes of your time: <https://www.youtube.com/watch?v=bDJb8WOJYdA>

More quotes from Rob Joyce's talk:

- *If you really want to protect your network, you really have to know your network*
- *Our key to our success is knowing that network better than the people who set it up*
- *Reduce the attack surface*
- *A lot of people think the nation states, they're running on the engine of zero days... Take these big corporate networks, any large network: I will tell you that persistence and focus will get you in, not the zero day*
- *You really need to invest in continuous defensive work*
- *Enable those logs, but also look at those logs. You'd be amazed at incident response teams go in, there's been some tremendous breach, and 'yup there it is, right there in the logs'*<sup>3</sup>

[1] <https://www.youtube.com/watch?v=bDJb8WOJYdA>

[2] <https://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/>

[3] <https://www.youtube.com/watch?v=bDJb8WOJYdA>

## Identify and Prioritize Critical Assets

- The answer to: “*what are you trying to protect?*” can’t be *everything*
- A security architect needs to understand the mission(s) of the organization and work with business owners to identify the associated critical assets needed to support them
- Create a list of defensible assets and classify them from most critical to least critical
  - If your organization has a BCP, start there
- Consider different network zones and user tiers
- Align different security levels to zones & tiers



### Identify and Prioritize Critical Assets

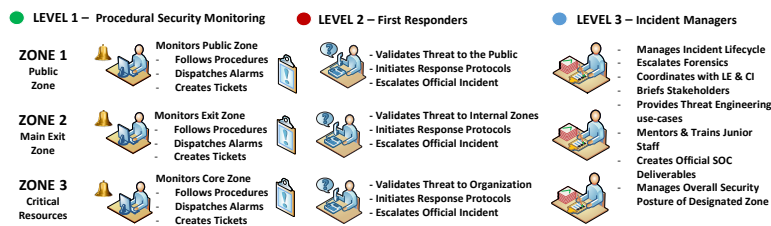
A course author liked to ask this question when meeting with new customers that wanted to establish new security operations or re-design and build security architectures: what are you trying to protect? If you don't know the answer to this question, you probably need to understand your business better. As a security architect, you need to understand the mission(s) of the organization and work with business owners to identify the associated critical assets needed to support them.

Therefore, identifying critical assets is an important part of that. If your organization has a Governance, Risk and Compliance (GRC) team or has a Business Continuity Plan (BCP) in place, it's likely that some of this information is already available to you.

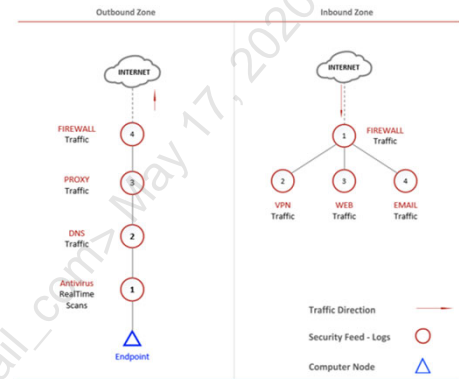
This information will be critical to be able to establish different security levels, zones and tiers, as we will see later on day 2, when we discuss segmentation.

## Architecting with Security Operations Monitoring in Mind

- Architecting using the concept of “zones” to defend your organization allows for both IT and business context to simplify building effective monitoring Use-Cases (more on Day 2)



Source: @TTP0 [https://github.com/TTP0/tp0\\_community\\_templates](https://github.com/TTP0/tp0_community_templates)



### Architecting with Security Operations Monitoring in Mind

Traditional architectures were built with a focus on protection, not detection. That’s why it’s important that we architect with security operations, and specially monitoring, in mind.

Using the concept of SOC Zones to defend your organization allows for both IT and business context to simplify building effective Use-Cases, as well as setting the stage to build efficient processes around Zones, Categories, Severity, Sensitivity, and Tiers for response process. Zoning should be implemented in a way that reflects the business-critical capability.

Other examples of zones include:

- OT/ICS
- Manufacturing
- R&D
- PCI Zones
- business-critical application
- Cloud critical hosting
- DMZ

[1] [https://github.com/TTP0/tp0\\_community\\_templates](https://github.com/TTP0/tp0_community_templates)

[2] <https://github.com/TTP0/info>

[3] <https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1533057129.pdf>

## The Broken Windows Theory of Network Engineering

- The broken windows theory states, "that a broken window left unrepaired will make a building look uncared for or abandoned and soon attract vandals to break all the other windows."<sup>1</sup>
- This theory, when applied to network engineering, states: fix the small stuff, and maintaining security becomes easier
- Reconfigure any systems that have the following issues:
  - Bad DNS settings, misconfigured netmask or gateway, fragmentation caused by MTU issues often associated with IPsec tunnels, misconfigured benign systems blocked by the outbound firewall, etc.

### The Broken Windows Theory of Network Engineering

The Broken Windows Theory was described by Criminologist James Q. Wilson and George Kelling. They tested two abandoned cars ("an automobile without license plates parked with its hood up on the street"<sup>2</sup>), one parked in a poorer neighborhood, the other in a richer neighborhood.

The car in the poorer neighborhood was robbed very quickly, while the one in the richer neighborhood was left alone for a week. "Then Zimbardo smashed part of it with a sledgehammer. Within a few hours, the car had been turned upside down and utterly destroyed."<sup>3</sup> The idea: crack down on petty crime, including graffiti, panhandling, and broken windows. It is less likely to escalate to serious crimes.

This theory has been controversial when applied to policing, as it can lead to issues such as racial profiling.

The theory is solid when applied to networks: small problems are less likely to become large problems if they are dealt with quickly. Network Security Monitoring can become very difficult if hundreds of systems are hammering an outbound firewall with denied traffic (which can mask worm propagation behavior).

[1] [http://sociologyindex.com/broken\\_window\\_theory.htm](http://sociologyindex.com/broken_window_theory.htm)

[2] Ibid.

[3] Ibid.

## Change Management Meeting Rules of Engagement

- Let's assume an organization holds a weekly change management meeting
- Rules of Engagement:
  - The default answer is: yes
  - The default change implementation speed is: soon
  - Representatives from all relevant lines of business must attend
  - Silence or non-attendance equals yes
  - "Go/no go" decisions are made during the meeting
  - No one is allowed to quote from the Simple Sabotage Field Manual
- Encourage those advocating "no" or "not yet" to offer specific methods to get to "yes" and "soon"

### Change Management Meeting Rules of Engagement

Issues that delay or stop change include testing, as well as single points of failure that could lead to (or risk to) outages. We will discuss those issues next.

One line often quoted by the course authors, when faced with change-adverse clients: status quo isn't working anymore. Those advocating for less, slow, or no change are advocating for the status quo. If a company has suffered a major breach (or perhaps multiple), repeating the same processes of the past is likely to lead to similar outcomes in the future.

The bottom line is change must occur frequently and quickly. Some changes can be scheduled on a routine basis, such as Microsoft 'patch Tuesday', which occurs on the second Tuesday of every month.<sup>1</sup> Other changes may need to occur on a rapid and/or unscheduled basis. 2017's macOS "I am Root" flaw is a case study illustrating this point, as we will discuss shortly.

Many organizations allow a self-submitted change management ticket for low-risk changes. This is done so that all changes can be audited while avoiding slowing down low-risk changes due to extra process.

[1] <https://docs.microsoft.com/en-us/security-updates/>

## "But We Have to Test"

- Yes, testing is required
- Change is often stopped or delayed due to deficient processes and/or infrastructure
- For most organizations (mean non-critical infrastructure, etc.): if testing takes weeks:
  - Fix your testing process
- If patching a system results in an outage of a critical single-point-of-failure system:
  - Improve your redundancy

### "But We Have to Test"

For those quoting from the OSS Simple Sabotage Field Manual, they often cling to this part:

Advocate "caution." Be "reasonable" and urge your fellow-conferrees to be "reasonable" and avoid haste which might result in embarrassments or difficulties later on.<sup>1</sup>

This is often backed by past changes that caused operational issues. For example, a course author worked for a large healthcare provider with a firewall and VPN concentrator that were single-points of failure. Every major firewall or VPN concentrator change (including patching) was vigorously attacked by multiple members of the change management board. The team finally received funding to replace the single point of failure with an active-passive HA (highly available) firewall/VPN cluster.

The team announced a planned change to replace the old firewall/VPN concentrator with the new HA cluster: and that change was vigorously attacked, with attempts to stall, delay, etc. Persistence is the key to a long-term and successful information security career, and the team lead patiently advocated the HA change, which occurred a week later than desired. After that: firewall/VPN changes happened quickly, with little or no pushback from the change management board.

[1] <https://www.cia.gov/news-information/featured-story-archive/2012-featured-story-archive/simple-sabotage.html>

## Emergency Change Management

- All change management policies must include an 'emergency' clause
  - This is designed to mitigate fast-moving risks
  - It sometimes means patching the same day (or faster) as vulnerability disclosure and discovery
- Some change management policies effectively prohibit same-day changes by not addressing emergency changes
- Changes triggered via the emergency change clause require rapid management approval (perhaps from the CIO), rapid testing, and rapid user notification (when necessary)

**Emergency Change Management** is sometimes called an 'exigent circumstances clause'.

Evergreen Systems released an excellent sample change management policy, presented at the SANS Process Control & SCADA Security Summit 2009 (February 2009) that addresses emergency change management:

*The Change Management system has been designed to default to a routine priority for the end user community. The Change Coordinator will have the authority to adjust the priority level as required to meet the business needs. There are four levels of Change priorities which include:*

- *Emergency – A change that, if not implemented immediately, will leave the organization open to significant risk (for example, applying a security patch).*
- *High – A change that is important for the organization and must be implemented soon to prevent a significant negative impact on the ability to conduct business.*
- *Routine – A change that will be implemented to gain benefit from the changed service.*
- *Low – A change that is not pressing but would be advantageous.*<sup>1</sup>

[1] <https://www.sans.org/summit-archives/file/summit-archive-1493830822.pdf>



## Case Study: Emergency Change Management

- Some changes require same-day patching or mitigation
  - Recent examples include ShellShock and Heartbleed
- In 2017 the macOS "I am Root" flaw was widely exploited within hours of vulnerability disclosure
  - High Sierra systems were affected
- The attack is triggered by attempting to log in as 'root'
- If no root user account exists:
  - First attempt to log in creates the account
  - The second attempt sets the root password
  - The third attempt logs in as root



### Case Study: Emergency Change Management

The macOS High Sierra "I am root" flaw was widely exploited within hours of vulnerability notification. The most common remote vector was Apple Remote Desktop, which uses VNC (Virtual Network Computer) to allow remote GUI access to macOS systems

Ironically, some security researchers made the problem worse by scanning for remote systems running Apple Remote Desktop, accidentally creating root accounts with blank passwords (or whatever password the scanner was configured to use):

In fact, researchers who have been scanning the internet might have accidentally created a wider attack surface and left users exposed... "You are setting the root password to every machine you authenticate to, as a blank password or whatever you choose to put into the password field," security researcher Tom Ervin explains.<sup>2</sup>

The immediate workaround was to create a root account and assign a strong password. Apple released a patch the following day. Organizations that had remote exposure (such as those that used Apple Remote Desktop) and didn't apply the workaround the same day were at high risk. They were at even higher risk if they didn't patch or apply the workaround the following day.

Many organizations didn't (or couldn't) implement changes that quickly.

[1] <https://imgur.com/gallery/MV9Az>

[1] <https://www.csoonline.com/article/3238890/security/apples-high-sierra-allows-root-with-no-password-theres-a-workaround-to-help.html>



## Automatic Change Notification of Critical Devices

- Another winning technique: configuring automatic change notification of critical devices such as routers and firewalls
- This becomes straightforward once an organization develops a robust change management process
- For example: configure Cisco's Configuration Change Notification and Logging<sup>1</sup> on all supported Cisco devices
- Then have your SOC follow this procedure
  - If a change is detected to a critical device: look up the matching change management ticket
  - Escalate if no change management ticket is found

### Automatic Change Notification of Critical Devices

Cisco's Configuration Change Notification and Logging feature were added to Cisco IOS in 2003. It reports any changes made to a device, independently of the syslog server settings. This is important because previously attackers could disable syslog on a Cisco IOS device, and the final command used to disable syslog (for example, "`no logging 192.168.1.1`") would not be logged.

Cisco describes this feature:

*The Configuration Change Notification and Logging (Config Log Archive) feature allows the tracking of configuration changes entered on a per-session and per-user basis by implementing an archive function. This archive saves configuration logs that track each configuration command that is applied, who applied the command, the parser return code (PRC) for the command, and the time the command was applied. This feature also adds a notification mechanism that sends asynchronous notifications to registered applications whenever the configuration log changes.*

*Before the introduction of the Configuration Change Notification and Logging feature, the only way to determine if the Cisco software configuration had changed was to save a copy of the running and startup configurations to a local computer and make a line-by-line comparison. This comparison method can identify changes that occurred but does not specify the sequence in which the changes occurred, or the person responsible for the changes.<sup>2</sup>*

[1] <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/x3s/config-mgmt-x3s-book/cm-config-logger.html>

[2] Ibid.

## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. Course Overview
2. Defensible Security Architecture
3. Traditional Security Architecture Deficiencies
4. Winning Defensible Security Techniques
5. **Security Models**
6. Threat, Vulnerability, and Data Flow Analysis
7. **EXERCISE: Egress Analysis**
8. Physical Security
9. Wireless
10. Layer 2 Attacks and Mitigation
11. **EXERCISE: Identifying Layer 2 Attacks**
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. **EXERCISE: Architecting for Flow Data**
16. 530.1 Summary

### Course Roadmap

We will next discuss security models.

## Security Models, Standards, Frameworks, and Best Practices

- Following references like models, standards, frameworks and best practices minimize the possibility of missing or forgetting a component in a security architecture
- They also provide a common language that helps to explain your decisions
- What security architecture framework should I follow?
- Let's consider some of the existing ones, strengths and weaknesses, including the new zero trust model.

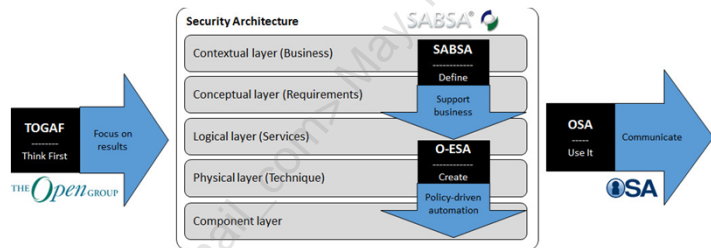


This page intentionally left blank.

Licensed To: Martin Brown <hermespaul56@gmail.com>

## Security Architecture Frameworks

- TOGAF, SABSA, O-ESA and OSA (see notes)
- Most of these references focus on the *WHAT* vs the *HOW*
- Our approach is based on ‘hands-on’, real-world security
- Use these standards ‘as needed’ to align with business needs and communicate to upper management as well as Governance, Risk and Compliance (GRC)



### Security Architecture Frameworks

While several frameworks focused on security architectures exist, they are mostly focused on what needs to be done, versus how to do it. While you can use these references to align with the business needs and communicate to upper management or GRC, our class will focus on how to design, build and implement practical security architectures.

[1] <https://www.linkedin.com/pulse/best-framework-security-architecture-pascal-de-koning/>

## Models Focused on Security Threats

- Other IT Security & Risk Standards
  - ISO/IEC 27001:2013, NIST Cyber Security Framework (CSF), COBIT, Critical Security Controls
  - O-ISM3
- We will focus on threat-driven security models that can be mapped to any of the previous ones
  - Time Based Security
  - Intrusion Kill Chain and MITRE ATT&CK
  - Diamond Model of Intrusion Analysis
  - Zero Trust Model (Forrester)

### Models Focused on Security Threats

We will next discuss the following security models:

- Time Based Security
- Intrusion Kill Chain and MITRE ATT&CK
- Diamond Model of Intrusion Analysis
- Zero Trust Model (Forrester)

Let's begin!

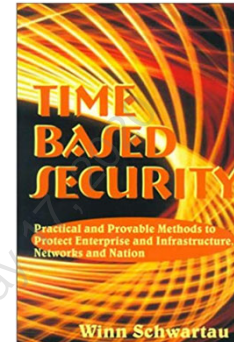
## Time-Based Security

- Reproducible method to understand how much 'security' a product or technology provides
  - How long are systems exposed?
  - How long before we detect a compromise?
  - How long before we respond?

**P** – how long our **protection** works

**D** – how long it takes us to **detect**

**R** – how long it takes us to **react**



$$P > D + R$$

### Time-Based Security

Usually applied to auditing, time based security can be a very practical model to assess and design security architectures too.

*"We've been looking at security the wrong way," says 'security maven' Winn Schwartau. "Fortress Mentality insists that building tall electronic walls is how to keep the bad guys out. That method hasn't worked for 5000 years of warfare, so why should it work for computer security? It can't and it doesn't." Written in Schwartau's highly popular and entertaining style, Time Based Security is a not - too - technical paradigm shift which gives you new tools to handle network security completely differently: - A simple method to measure your security efforts more efficiently, - A framework so management can make informed decisions as to where to smartly invest their security budget dollars. Within minutes, you will be able to judge how secure or insecure your network is! Time Based Security provides you with the tools you need to make your systems more secure than ever before. "Required reading for infosecurity professionals! Practical advice regarding fundamental security needs-- protection, detection, and reaction." Peter Harrison, Director of Marketing, MEMCO Software.*

[1] <https://www.amazon.com/Time-Based-Security-Winn-Schwartau/dp/0962870048>

## The Cyber Kill Chain®

- The Cyber Kill Chain® (also known as the Intrusion Kill Chain) is a model designed by Lockheed Martin
  - The metaphor: if you break the chain before the end: the attacker fails
- The Kill Chain is (often) applied in the context of malware, and perimeter defenses
  - Many criticize it for this reason
- However, it can also be applied to other contexts, and the metaphor is quite useful
- The steps are:
  - Reconnaissance
  - Weaponization
  - Delivery
  - Exploitation
  - Installation
  - Command and Control
  - Actions on Objectives<sup>1</sup>

### The Cyber Kill Chain®

The term "kill chain" comes from the military, predating computers. One example is "find, fix, track, target, engage, and assess"<sup>2</sup>

Lockheed Martin describes the Kill Chain:

*The phrase "kill chain" describes the structure of the intrusion, and the corresponding model guides analysis to inform actionable security intelligence. Through this model, defenders can develop resilient mitigations against intruders and intelligently prioritize investments in new technology or processes. Kill chain analysis illustrates that the adversary must progress successfully through each stage of the chain before it can achieve its desired objective; just one mitigation disrupts the chain and the adversary. Through intelligence-driven response, the defender can achieve an advantage over the aggressor for APT caliber adversaries.<sup>2</sup>*

[1] <https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>

[2] <http://www.dtic.mil/dtic/tr/fulltext/u2/a435726.pdf>

[3] <https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>

## Kill Chain Countermeasures

- Lockheed Martin also describes countermeasures that may perform the following actions:

- Detect
- Deny
- Disrupt
- Degrade
- Deceive<sup>1</sup>

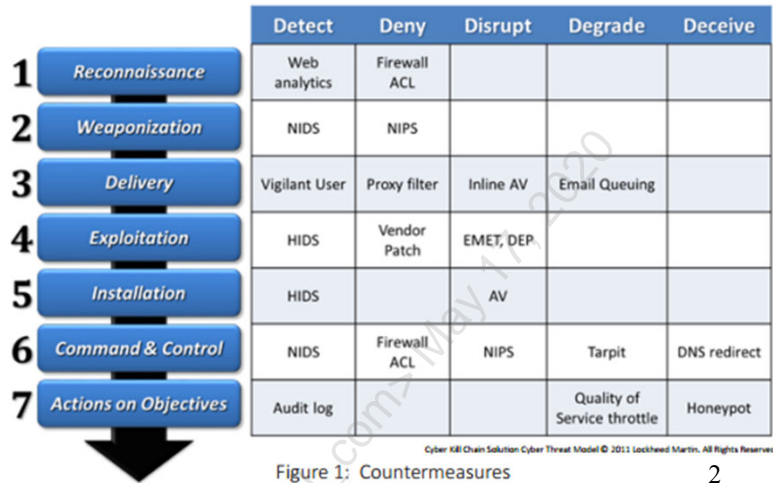


Figure 1: Countermeasures

2

### Kill Chain Countermeasures

Lockheed Martin's countermeasures are largely infrastructure-centric. We will discuss all of the devices and technologies are shown in the graphic above. Most companies have already made significant investments in the "Deny" and "Disrupt" technologies, since they are largely prevention-based, and have comparatively low Total Cost of Ownership (especially when compared with the detective controls). Detective controls are often lacking.

The "Degrade" and "Deceive" controls are often missing from many less mature organizations, which is understandable. It makes little sense to focus on deceptive technologies when other fundamental controls (such as patching) may be lacking.

This course will focus on the most effective controls and take special care to highlight controls that organizations possess, but are not yet leveraging. Examples include reconfiguring existing routers and switches to secure the environment better.

[1] [https://github.com/TTP0/ttp0\\_community\\_templates](https://github.com/TTP0/ttp0_community_templates)

[2] Ibid.



### MITRE ATT&CK Matrix

- Provides a common language to describe adversarial tactics and techniques
- Applicable to real environments, allow mapping the attacker’s behaviors to defenses
- Go-to model to plan & verify purple teaming exercises



Adversarial Action	Technique	Platform	Platform Execution	Platform Execution	Platform Execution	Platform Execution	Platform Execution	Platform Execution	Platform Execution	Platform Execution	Platform Execution	Platform Execution	Platform Execution
Account Access	Account Access	Account Access	Account Access	Account Access	Account Access	Account Access	Account Access	Account Access	Account Access	Account Access	Account Access	Account Access	Account Access

<https://attack.mitre.org/>

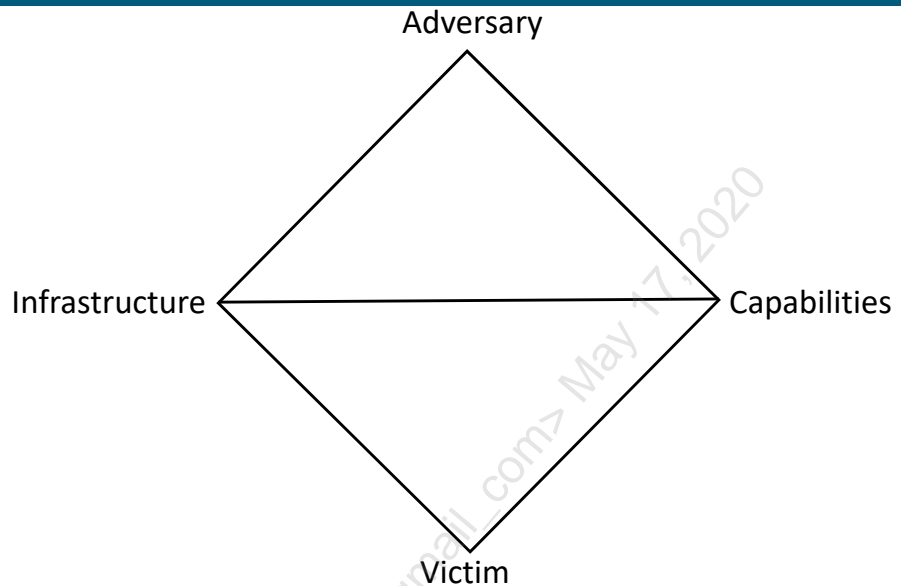
### MITRE ATT&CK Matrix

ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge. MITRE started this project in 2013 to document common tactics, techniques, and procedures (TTPs) that advanced persistent threats use against Windows enterprise networks. ATT&CK was created out of a need to document adversary behaviors for use within a MITRE research project called FMX. FMX’s objective was to investigate the use of endpoint telemetry data and analytics to improve post-compromise detection of adversaries operating within enterprise networks.

<https://medium.com/mitre-attack/att-ck-101-17074d3bc62>

## The Diamond Model of Intrusion Analysis

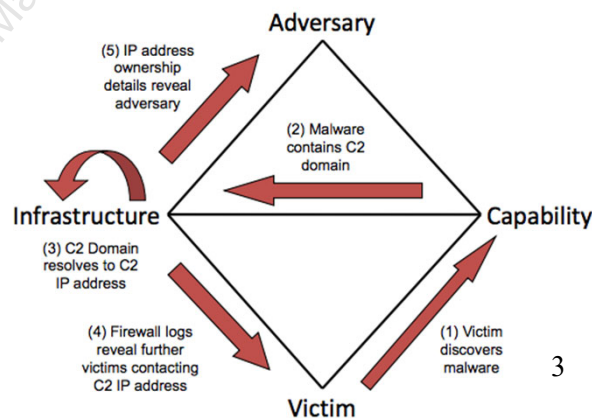
- *In its simplest form, the model describes that an adversary deploys a capability over some infrastructure against a victim.*
- *These activities are called events and are the atomic features.<sup>1</sup>*



### The Diamond Model of Intrusion Analysis

In the diagram above: the adversary is the person (often called the "actor") attempting to compromise a network or system. Infrastructure is represented by clients, servers, networks, switches, routers, firewalls, etc. Capabilities are tools and techniques, including ping sweeps, port scans, malware, exploits, hacker toolkits, etc. Finally, the victim is the organization or person targeted by the adversary.

The following diagram illustrates analytic pivoting, "One of the most powerful features of the Diamond, pivoting allows an analyst to exploit the fundamental relationship between features (highlighted by edges between the features) to discover new knowledge of the malicious activity."<sup>3</sup>



[1] [https://cdn2.hubspot.net/hubfs/454298/The\\_Diamond\\_Model\\_of\\_Intrusion\\_Analysis.pdf](https://cdn2.hubspot.net/hubfs/454298/The_Diamond_Model_of_Intrusion_Analysis.pdf)

[2] Ibid.

[3] Ibid.

## Zero Trust Model

- Forrester's Zero Trust Model removes the concept of "internal is trusted, external is not"
- It requires an organization to:
  - *...go through a state of transformation by eliminating the idea of a trusted network regardless of whether it is an internal or external network, and redesigning networks from the inside out. In the Zero Trust Model of information security, we assume that all traffic is untrusted. This approach demands that you build security into the DNA of your IT architecture by investing in situational awareness, and developing robust vulnerability and incident management capabilities.<sup>1</sup>*

**Zero Trust Model** eliminates the "inside == trusted, outside == untrusted) mindset that has dominated security design since the late 1980s.

Forrester described the Zero Trust Model in response to NIST (the United States National Institute of Science and Technology) request for feedback to "Developing a Framework to Improve Critical Infrastructure Cybersecurity.

Forrester echoes Bill Cheswick by saying,

*There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft, chewy center." This philosophy is widespread today, accompanied by the mantra "trust but verify." This mantra and M&M philosophy of information security are based on trust and the assumption that malicious individuals cannot pass the "hard crunchy outside." The thought process around this philosophy was that additional internal security measures were unnecessary because it was unlikely that an intruder would be able to get sustained access to a network, and it was also unlikely that they would be able to move from area to area once in an organization. In today's new threat landscape, this M&M and "trust but verify" model of information security is no longer an effective way of enforcing security.<sup>2</sup>*

[1] <https://www.nist.gov/file/369501>

[2] Ibid.

## The Three Concepts of Zero Trust

- Forrester describes the three concepts of Zero Trust:
  - *Ensure all resources are accessed securely regardless of location*
  - *Adopt a least privilege strategy and strictly enforce access control*
  - *Inspect and log all traffic<sup>1</sup>*
- This can seem intimidating for companies that still use the "candy bar" design, here is one way to start
  - New projects/technologies: use Zero Trust
  - Look for 'easy wins' to convert existing technologies to Zero Trust
  - Then chip away at the rest
- Software Defined Networking and Network Virtualization are key network components of Zero Trust

### The Three Concepts of Zero Trust

NAC (Network Access/Admission Control, which we will discuss later in 530.5) offers one way to begin deploying a Zero Trust architecture.

Many NAC deployments treat all systems as untrusted: whether local or remote. The system begins on an untrusted VLAN (or otherwise unconnected from the corporate network). A user logs into the supplicant (NAC client software), and once authenticated: they join the local access network at layer 3. Additional checks are also often built into NAC, such as verifying that the local system is patched, has current antivirus, and has an active firewall.

These systems can be complex (and expensive), but they solve series of problems quite well: treating the user (and their system) in the coffee shop the same way as an unauthenticated user at their desk.

[1] [https://www.nist.gov/sites/default/files/documents/2017/06/05/040813\\_forrester\\_research.pdf](https://www.nist.gov/sites/default/files/documents/2017/06/05/040813_forrester_research.pdf)

## Software-Defined Networking

Software Defined Networking (SDN) separates a router's control plane from the data (forwarding) plane

- Control plane: control data sent to/from a router, such as routing protocol updates (OSPF, BGP, etc.)
- Data plane: data sent through a router, such as routed packets

Routing decisions are made remotely, instead of on the router

- The open source OpenFlow protocol is used for remote management of the data plane in Software Defined Networks
- OpenFlow is a TCP protocol that uses TLS encryption

### Software-Defined Networking

The Open Network Foundation describes SDN in their paper "Software-Defined Networking: The New Norm for Networks":

*Network intelligence is (logically) centralized in software-based SDN controllers, which maintain a global view of the network. As a result, the network appears to the applications and policy engines as a single, logical switch. With SDN, enterprises and carriers gain vendor-independent control over the entire network from a single logical point, which greatly simplifies the network design and operation. SDN also greatly simplifies the network devices themselves, since they no longer need to understand and process thousands of protocol standards but merely accept instructions from the SDN controllers.<sup>1</sup>*

OpenFlow is managed by the Open Networking Foundation. The foundation describes OpenFlow:

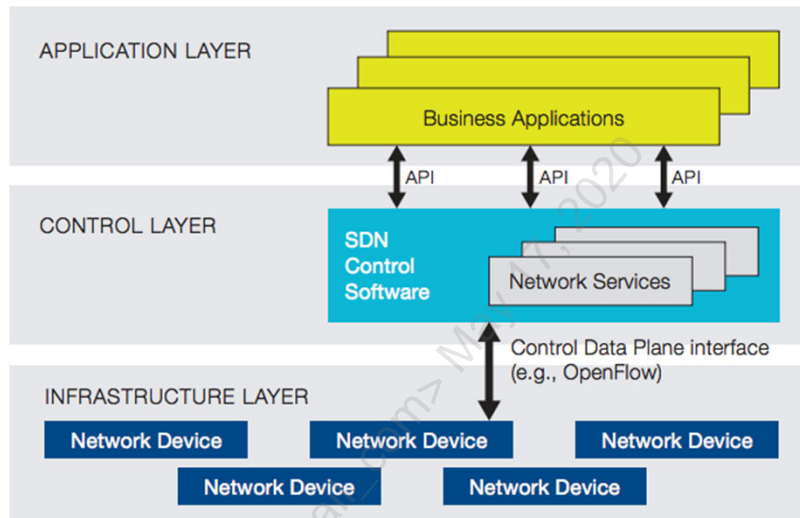
*In a classical router or switch, the fast packet forwarding (data path) and the high level routing decisions (control path) occur on the same device. An OpenFlow Switch separates these two functions. The data path portion still resides on the switch, while high-level routing decisions are moved to a separate controller, typically a standard server. The OpenFlow Switch and Controller communicate via the OpenFlow protocol, which defines messages, such as packet-received, send-packet-out, modify-forwarding-table, and get-stats.<sup>2</sup>*

[1] <http://archive.openflow.org/wp/learnmore/>

[2] <https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf>

## Software-Defined Network Architecture<sup>1</sup>

- SDN views a network in three layers
  - Application Layer
  - SDN Control Layer
  - Infrastructure Layer (switches, routers, firewalls, etc.)



### Software-Defined Network Architecture<sup>1</sup>

SDN creates three layers (layers are sometimes called "planes"):

*SDN architectures generally have three components or groups of functionality:*

- *SDN Applications: SDN Applications are programs that communicate behaviors and needed resources with the SDN Controller via an application programming interface (APIs). In addition, the applications can build an abstracted view of the network by collecting information from the controller for decision-making purposes. These applications could include networking management, analytics, or business applications used to run large data centers. For example, an analytics application might be built to recognize suspicious network activity for security purposes.*
- *SDN Controller: The SDN Controller is a logical entity that receives instructions or requirements from the SDN Application layer and relays them to the networking components. The controller also extracts information about the network from the hardware devices and communicates back to the SDN Applications with an abstract view of the network, including statistics and events about what is happening.*
- *SDN Networking Devices: The SDN networking devices control the forwarding and data processing capabilities for the network. This includes forwarding and processing of the data path.<sup>1</sup>*

[1] <https://www.sdxcentral.com/sdn/definitions/inside-sdn-architecture/>

## SDN vs. Network Virtualization

- Software-Defined Networking can be thought of as an evolutionary step beyond individually-managed switches (and VLANs), routers and firewalls
- Network Virtualization takes SDN a step further
  - *Software-defined networking allows you to control network switches and routers through software. It doesn't virtualize all networking functions and components.*
  - *Network virtualization replicates all networking components and functions in software. It allows you to run the entire network in software.<sup>1</sup>*

### SDN vs. Network Virtualization

Vendors have introduced a fair amount of confusion regarding Software-Defined Networking and Network Virtualization. This is common with many hot new security technologies: vendors elbow for the position, trying to become the go-to solution to solve the problem at hand. While there is industry disagreement on the specific differences and features, Mora Gozani offers a good summary in *Network Virtualization For Dummies*:

*Though the term software-defined networking means different things to different people, this much is clear: SDN allows software to control the network and its physical devices. SDN is all about software talking to hardware — you can essentially call it a next-generation network management solution. Though it centralizes management and allows you to control network switches and routers through software, SDN doesn't virtualize all networking functions and components. In other words, SDN doesn't allow you to run the entire network in software. Hardware remains the driving force for the network.*

*In contrast to SDN, network virtualization completely decouples network resources from the underlying hardware... With your networking resources decoupled from the physical infrastructure, you basically don't have to touch the underlying hardware. Virtual machines can move from one logical domain to another without anyone having to reconfigure the network or wire up domain connections. You implement network virtualization in the hypervisor layer on x86 servers rather than on network switches.<sup>2</sup>*

[1] <https://blogs.vmware.com/networkvirtualization/2016/04/network-virtualization-for-dummies.html/>

[2] Ibid.



## Micro-Segmentation

- Micro-Segmentation provides filtering between every interface on every system on a network
  - This is considered an end-goal of the Zero Trust Model
- Historically: this was prohibitively expensive, in both CAPEX (capital expenditures) and OPEX (operational expenditures)
  - Organizations usually lack physical and logical filtering capabilities between every interface
  - Even if such functionality was in place: configuring this would normally be extremely time consuming
- SDN and Virtual Networking make micro-segmentation possible

### Micro-Segmentation

"North-south" and "east-west" movement are terms commonly used to describe firewalls and trust zones. Firewalls were historical "north-south" devices, stopping untrusted traffic (north, on the untrusted interface) from flowing south (to the WAN, or the trusted interface). Historically, firewalls were not commonly used to filter "east-west" traffic (WAN -> WAN, behind the trusted interface).

Lawrence Miller and Joshua Soto describe the historical challenges of micro-segmentation in *Micro-segmentation For Dummies*:

*The primary issue is that once an attack gets past the data center perimeter, there are few lateral controls to prevent threats from traversing inside the network. The best way to solve this is to adopt a stricter, micro-granular security model with the ability to tie security to individual workloads and the agility to provision policies automatically. Forrester Research calls this the "Zero Trust" model, and micro-segmentation embodies this approach.*

*With micro-segmentation, fine-grained network controls enable unit-level trust, and flexible security policies can be applied all the way down to a network interface. In a physical network, this would require deploying a physical firewall for every workload in the data center, so up until now, micro-segmentation has been cost-prohibitive and operationally unfeasible. However, with network virtualization technology, micro-segmentation is now a reality.<sup>1</sup>*

[1] [http://learn.vmware.com/41021\\_REG?touch=1&int\\_cid=70134000001SjWc](http://learn.vmware.com/41021_REG?touch=1&int_cid=70134000001SjWc)



## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. Course Overview
2. Defensible Security Architecture
3. Traditional Security Architecture Deficiencies
4. Winning Defensible Security Techniques
5. Security Models
- 6. Threat, Vulnerability, and Data Flow Analysis**
7. EXERCISE: Egress Analysis
8. Physical Security
9. Wireless
10. Layer 2 Attacks and Mitigation
11. EXERCISE: Identifying Layer 2 Attacks
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. EXERCISE: Architecting for Flow Data
16. 530.1 Summary

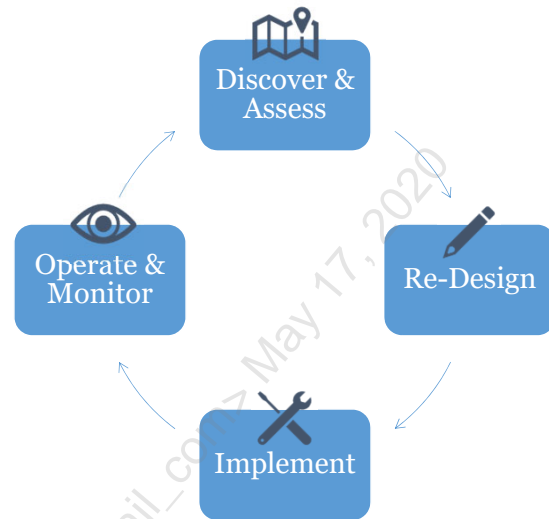
### Course Roadmap

We will next discuss threat, vulnerability, and data flow analysis.

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020

## Defensible Security Architecture Lifecycle

- Based on practical models
- Focused on implementing 'real security' mitigations vs architecture design
- Allows to secure already existing infrastructure (re-design)
- Aligned to modern security operations practices
- Risk driven: focused on mitigating impact for threats you are facing already (or will soon)



### Defensible Security Architecture Lifecycle

Developing, implementing and maintaining sound security architectures requires a sound methodology. For this class, we have opted to use a simple yet effective method that's based on other common lifecycles, including the SABSA SECURITY ARCHITECTURE lifecycle: Strategy & Planning -> Design -> Implement -> Manage & Measure.

[1] <https://sabsa.org/sabsa-executive-summary/>

## Discover & Assess



- Identify requirements, business & regulatory
  - i.e. HIPAA, PCI, SOX, GDPR, etc. Leverage BCP & GRC documentation
- Identify assets in scope and crown jewels
- Understand business and risk appetite
- Identify resources available: tools, budget, personnel, skills, time
- Practical threat modeling and risk analysis
  - Attack surface analysis, network attack surface, data egress analysis, network visibility analysis and protocol visibility analysis
  - **Red teaming**: impact analysis (think offensive), realistic scenarios based on attacker's TTP's

### Discover & Assess

In the first phase, we need to be able to discover and assess what assets are in scope, what threats are applicable, what resources we have and new security requirements arising from:

- A new statutory or regulatory mandate
- A new threat realized or experienced
- A new IT architecture initiative discovers new stakeholders and/or new requirements

In this phase, we will perform tasks like

- Document Collection
- Interviews
- Vulnerability Analysis / Pentests
- Risk Analysis
- Asset Identification & Classification
- Threat Identification & Classification
- Risk Analysis

A practical example of doing this is Threat, Vulnerability, and Data Flow Analysis

We will next discuss:

- Attack Surface Analysis
- Network Attack Surface
- Data Egress Analysis
- Network Visibility Analysis
- Protocol Visibility Analysis

Let's discuss each!

## Goal: Identifying the Unknown Unknowns

Former United States Secretary of Defense Donald Rumsfeld addressing NATO in 2002:

- *There are things we know that we know. There are known unknowns. That is to say there are things that we now know we don't know. But there are also unknown unknowns. There are things we don't know we don't know.*<sup>1</sup>

Examples that apply to network monitoring:

- Known: we know that we can see malware via HTTP
- Known unknown: we know that we can't easily identify malware via HTTPS
- Unknown unknown: we don't know that we are using protocols such as IPv6 and QUIC right now and are completely unaware of these malware vectors

### Goal: Identifying the Unknown Unknowns

Donald Rumsfeld's 2002 speech to NATO is famous. A lot of people mocked it because they didn't understand it. As we begin to discuss analyzing visibility, we must strive to identify the 'unknown unknowns:' things we don't know that we don't know.

Two examples mentioned above are IPv6 and QUIC. As we will discuss during 530.2: IPv6 is enabled by default (and automatically used) by all Microsoft Windows systems since Windows Vista (as well as all recent versions of Linux, macOS, etc.). IPv6 accounts for over 22% of internet backbone traffic as of February 2018.<sup>2</sup>

QUIC is essentially HTTP/2 over UDP port 443:

*QUIC is a new transport which reduces latency compared to that of TCP. On the surface, QUIC is very similar to TCP+TLS+HTTP/2 implemented on UDP. Because TCP is implemented in operating system kernels, and middlebox firmware, making significant changes to TCP is next to impossible. However, since QUIC is built on top of UDP, it suffers from no such limitations.*<sup>2</sup>

QUIC is used by default when using the Chrome browser (or Opera 16+) to connect to Google sites. Tool and proxy support for analyzing QUIC is currently limited to non-existent.

[1] <https://www.nato.int/docu/speech/2002/s020606g.htm>

[2] <https://www.google.com/intl/en/ipv6/statistics.html>

[3] <https://www.chromium.org/quic>

## Attack Surface Analysis

- Attack surface describes all of the vectors for exploitation
  - Attack surface of a house (risk of theft of belongings): the doors, windows, vents, chimney, etc.
  - Attack surface of a network: internet connections, extranet connections, mobile devices, physical access, etc.
- Organizations should conduct a formal attack surface analysis, and document the results
  - Then seek to lower the attack surface where possible

### Attack Surface Analysis

Stephen Northcutt describes examples of attack surface:

- *Open ports on outward facing web and other servers, code listening on those ports*
- *Services available on the inside of the firewall*
- *Code that processes incoming data, email, XML, office documents, industry-specific custom data exchange formats (EDI)*
- *Interfaces, SQL, web forms*
- *An employee with access to sensitive information is socially engineered<sup>1</sup>*

*When considering an attack surface to develop a defense-in-depth architecture, there are three basic interrelated considerations that develop from our examples:*

- *Network Attack Surface, the attack will often be delivered via a network*
- *Software Attack Surface, with a primary focus on web applications*
- *Human Attack Surface, social engineering, errors, trusted insider, death and disease<sup>1</sup>*

[1] <https://www.sans.edu/cyber-research/security-laboratory/article/did-attack-surface>

## Network Attack Surface Analysis

- The following vectors allowing network access should be carefully studied and cataloged:
  - Internet connections
  - Mobile devices and BYOD (Bring Your Own Device)
  - Internet of Things (IoT) connectivity
  - Cloud
  - VPN, tunnels, and Extranet connections (including leased lines)
  - All forms of remote access including vendor remote access
  - Modems
  - Wireless access
  - Industrial Control System (ICS) access including 'smart' building automation

### Network Attack Surface Analysis

Organizations need to catalog all of the (often) myriad ways software and people are able to connect to a network. This includes the list of options shown above and many more. It often helps to physically explore an office, and ask yourself, "how does this connect?", or, "how is this managed?"

Lots of technologies use TCP/IP: building automation, video cameras, card swipe sensors for physical access, burglar alarms, HVAC, soda machines, etc., etc.

In the case of the theft of 40,000,000 credit cards from Target, "Sources close to the investigation said the attackers first broke into the retailer's network on Nov. 15, 2013, using network credentials stolen from Fazio Mechanical Services, a Sharpsburg, Penn.-based provider of refrigeration and HVAC systems."<sup>1</sup>

Newer 'smart' buildings often have HVAC and other physical controls connected to the Internet, often via a DSL connection that is not under tenant control.

[1] <https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>

## OWASP on Attack Surface Analysis

*Attack Surface Analysis is about mapping out what parts of a system need to be reviewed and tested for security vulnerabilities. The point of Attack Surface Analysis is to understand the risk areas in an application, to make developers and security specialists aware of what parts of the application are open to attack, to find ways of minimizing this, and to notice when and how the Attack Surface changes and what this means from a risk perspective.*

*Attack Surface Analysis is usually done by security architects and pen testers. But developers should understand and monitor the Attack Surface as they design and build and change a system.<sup>1</sup>*

### OWASP on Attack Surface Analysis

OWASP (The Open Web Application Security Project) is specifically discussing application attack surface in the quote above, but it applies directly to network/system attack surface analysis as well.

OWASP goes on to say:

*The Attack Surface of an application is:*

- *The sum of all paths for data/commands into and out of the application, and*
- *The code that protects these paths (including resource connection and authentication, authorization, activity logging, data validation and encoding), and*
- *All valuable data used in the application, including secrets and keys, intellectual property, critical business data, personal data and PII, and*
- *The code that protects these data (including encryption and checksums, access auditing, and data integrity and operational security controls).<sup>2</sup>*

Replace "application" with "network" and "code" with "system" in the quote above and you have a good description of network/system attack surface analysis. The applications themselves should also be analyzed, as OWASP describes.

[1] [https://www.owasp.org/index.php/Attack\\_Surface\\_Analysis\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet)

[2] Ibid.

## Egress Analysis

- Most organizations have spent time performing ingress analysis
  - Designing systems that prevent and/or detect unauthorized/malicious person/software from getting into a system or network
  - A required part of the network attack surface analysis process
- How many have performed egress analysis?
  - Designing systems that prevent and/or detect unauthorized/malicious person/software moving data **out** of a system/network
  - Presumption of compromise: if the network is already owned, we should analyze the available vectors to push data **out**
  - Also known as 'exfiltration analysis' or 'extrusion analysis'

### Egress Analysis

Many folks at your organization have probably studied ingress analysis: preventing and/or detecting unauthorized users and/or software such as malware from getting into a network or system. It is far less common, however, to study the reverse: preventing and/or detecting unauthorized users and/or software such as malware moving data out of a network or system.

We'll discuss how to do this next. In the meantime, as a mental exercise, think about how many times your organization has tested unauthorized ingress. That's what happens during penetration tests, which many organizations perform or purchase annually (or more often).

How many times has your organization formally tested unauthorized egress? Some penetration testers will also test this vector, but that's normally an additional part of an ingress test. Ever considered tasking someone with simply pushing sensitive data out? Walk them into the data center, give them console access to a sensitive server, and push a text file (containing fake sensitive data)? Then see how long that process took, and what preventive or detecting controls that could have mitigated it?

We often discuss dwell time in our industry (how long a system or network is compromised before detection). Another critical metric is egress time: once on a system, how long does it take to push sensitive data to the internet?



## Network Visibility Analysis

- Network visibility analysis involves identifying any network 'blind spots' for NIDS, NIPS, full packet capture, NetFlow, etc.
  - Key question: can malware pivot from one system to another without being seen by any of the above controls?
- Client access networks are common examples
  - Malware pivots from one endpoint to another, with no sensor nearby to detect it
  - Note that a combination of network and host-based controls can also mitigate this risk, as we will discuss later in Security 530
  - The endpoints themselves can also provide additional visibility via logging

### Network Visibility Analysis

Network visibility analysis involves determining where the 'blind spots' (much like the blind spot in a car's rear-view mirror): places where malware can pivot without being seen by an IDS, IPS, full packet capture, NetFlow, etc.

Client access networks are common examples of network blind spots: if one client pivots into another on the same LAN: many organizations are blind from a network monitoring perspective. Note that network client-based controls can be used to mitigate this risk: for example, private VLANs (discussed later in 530.1) can be used to prohibit client-<->client traffic at layer 2. Host-based firewalls can be used to achieve the same goal. Logging, such as Windows event logging can also provide additional visibility.

For systems that are located in network blind spots: architects should add additional network visibility (through sniffers or IDSes attached to SPAN ports or network taps) or ensure that other mitigations address the risk.

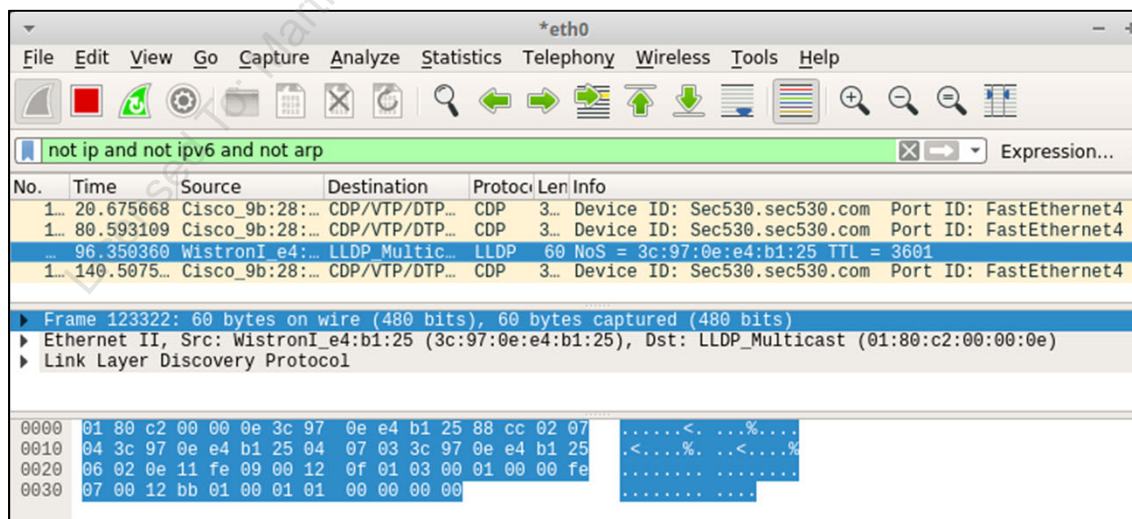
## Protocol Visibility Analysis

- A goal of protocol visibility analysis: become aware of all of the protocols being used on a network, and describe their business purpose
  - "My challenge to students is: collect 5 minutes of network traffic from your home network and try to explain every packet"<sup>1</sup> – Dr. Johannes Ullrich
- Process: capture traffic at various network locations
  - Then analyze with Wireshark and find the outliers by applying lots of "not" display filters
  - "not http and not ftp and not smb" ...
  - Fun filter: "not ip"

### Protocol Visibility Analysis

The process discussed above was used on an office LAN (client access network), using the following Wireshark display filter: not ip and not ipv6 and not arp

Note that "ip" matches IPv4 only. We discovered CDP (Cisco Discovery Protocol), a plaintext broadcast protocol used to share information between Cisco devices and leaks a lot of information. CDP should not be on a client access network). There is also an unknown Wistron device sending LLDP (Link Layer Discovery Protocol).



[1] <https://cybersecurityinterviews.com/037-johannes-ullrich-solving-puzzle-network/>

## Re-Design



- Identify desired state, determine the gap (current vs. desired) and roadmap
- Architectural decisions
  - Threat focused, covering protection, detection and reaction
- Risk mitigation
  - People
  - Processes
  - Technology
- Documentation

### Re-Design

Most of the time, security architects work on existing infrastructure, needing to secure what they already have.

Some of the documentation needed here is:

- Business rules regarding the handling of data/information assets
- Written and published security policy
- Codified data/information asset ownership and custody
- Risk analysis documentation
- Data classification policy documentation

[1] <http://pubs.opengroup.org/architecture/togaf91-doc/m/chap21.html>

## Implement



- Implement based on security architecture design
- Harden at each layer
  - Network-centric
  - Data-centric
- Enable logging for monitoring
- Determine baseline
  - Device configurations and traffic flows
- Validate implementation

### Implement

This is where we will spend most of the time this week, discussing how to implement secure architectures at each of the OSI layers, using a network as well as a data centric approach, including the zero trust model.

## Operate & Monitor



- Continuous security monitoring
  - Data at rest: registry keys, windows event logs, DNS, etc.
- Network Security Monitoring
  - Data in motion: NetFlow, transactional, pcaps
- Continue creating awareness, maintaining threat focused operations and augmenting visibility based on threat intel and IR lessons learned
- SANS student alumni report a high degree of success in implementing and automating these tasks 😊

This page intentionally left blank.

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020

## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. Course Overview
2. Defensible Security Architecture
3. Traditional Security Architecture Deficiencies
4. Winning Defensible Security Techniques
5. Security Models
6. Threat, Vulnerability, and Data Flow Analysis
7. **EXERCISE: Egress Analysis**
8. Physical Security
9. Wireless
10. Layer 2 Attacks and Mitigation
11. **EXERCISE: Identifying Layer 2 Attacks**
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. **EXERCISE: Architecting for Flow Data**
16. 530.1 Summary

### Course Roadmap

We will next conduct an exercise on egress analysis.



## Exercise 1.1: Egress Analysis

- Exercise 1.1 is in the digital wiki found in your student VM (recommended)
- Alternatively, you may use your Workbook

### SEC530 Exercise: Egress Analysis

We will now dive into a lab on egress analysis. This lab focuses on how data can be exfiltrated from a network and what defenders can do to prevent and detect exfiltration. Please go to lab workbook section 1.1.

## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. Course Overview
2. Defensible Security Architecture
3. Traditional Security Architecture Deficiencies
4. Winning Defensible Security Techniques
5. Security Models
6. Threat, Vulnerability, and Data Flow Analysis
7. EXERCISE: Egress Analysis
8. **Physical Security**
9. Wireless
10. Layer 2 Attacks and Mitigation
11. EXERCISE: Identifying Layer 2 Attacks
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. EXERCISE: Architecting for Flow Data
16. 530.1 Summary

### Course Roadmap

We will next discuss physical security.



## Network Security Architecture, Beginning at Layer 1

- We'll begin building from the ground up: **physical security**
- Before we begin, let's consider a winning defensible security architecture mindset:
  - Build security at every layer
  - Build it once, build it right
  - If there is a simple, low-risk solution to a potential security risk: deploy it
  - Employ the broken windows theory of network engineering
  - Use our **DA-R-I-OM** method

### Network Security Architecture, Beginning at Layer 1

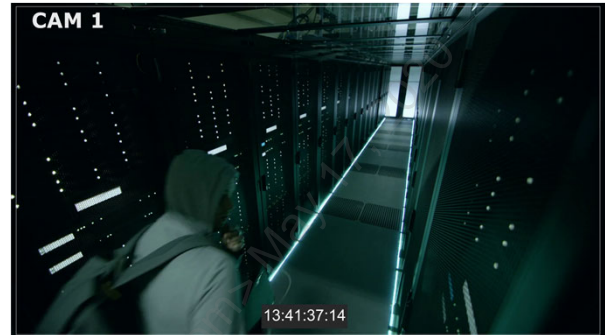
The risks we are about to begin mitigating through improved network security architecture range from high likelihood and high impact (malware pivoting from one internal host to another) to the low likelihood (an attacker abusing the PAD service (Packet Assembler/Disassembler service used by X.25 links).

We will show how to mitigate both risks. For PAD, it's as simple as putting 'no service pad' in your Cisco IOS configuration. The risk is essentially zero for environments that do not use X.25 networks. Clients will sometimes ask, *why do this if the likelihood is low?* The answer is security at every layer. If a one-line low-risk configuration addition mitigates that risk, then we do it. That is especially true when the change can be added to a secure baseline that's easily applied to a large number of systems.

Discover & Assess on 530.1 – Physical



- Physical inspection
  - Annual assessment
  - Can you get a badge issued from an email?
  - What could a janitor with a laptop do?
  - How far in can a person wearing a FedEx outfit get to?
  - Obtain written permission!



Discover & Assess on 530.1 – Physical

[1] <https://www.videoblocks.com/video/security-camera-footage-of-hacker-in-a-hoodie-infiltrating-data-center-with-his-laptop-he-connects-to-one-of-the-rack-servers-shot-on-red-epic-w-8k-helium-cinema-camera-ranjbf7hej0od324y>

## Red Team Scenario – Replicants vs. Tyrell Corporation

After finding that there is no hope for them and that their death is imminent, a group of replicants led by Roy Batty, seek to infiltrate Tyrell Corporation's network to disrupt their operations and prevent them from creating more human-like androids...

To achieve their goal, they'll use a wide variety of tactics.



### Red Team Scenario – Replicants vs. Tyrell Corporation

**Roy Batty** is the main antagonist of the science fiction novel *Do Androids Dream Of Electric Sheep?* and Ridley Scott's 1982 dark sci-fi thriller film *Blade Runner* which was based on the novel. He is a replicant (androids identical to human beings made by Tyrell Corporation to work on off-world colonies as slave labor and soldiers) from the recently made Nexus 6 generation.

Nevertheless, if you want to watch Bladerunner in 5 minutes, check this out:

[1] <https://www.youtube.com/watch?v=HJI6GRctGtY>

## Red Team Scenario – Rogue Pi

In their 1<sup>st</sup> attempt, a Nexus 6 android will attempt to drop a Rogue Pi, a pen testing Dropbox, to remotely access Tyrell Corporation's network, taking advantage of weak physical security controls.

<https://hackaday.com/2013/03/24/rogue-pi-a-rpi-pentesting-dropbox/>



### Red Team Scenario – Rogue Pi

Let's discuss what we could have done at Layer 1 to mitigate this kind of attack.

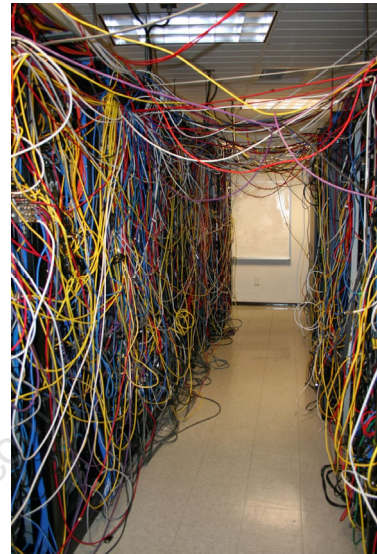
Check out a video demonstration of the Dropbox after the break. The device will create a reverse SSH tunnel to get around the firewall for remote control. We will consider how to mitigate that later on tomorrow during the layer 3/4 discussion.

[1] <https://hackaday.com/2013/03/24/rogue-pi-a-rpi-pentesting-dropbox/>

## Threats on 530.1 – Physical



- Physical access violation
  - Network cabinets
  - Backup tapes
  - Server rooms
  - Inserting weaponized USB keyboards
  - Inserting Pen testing Drop Boxes
  - Rogue Devices



### Threats on 530.1 – Physical

Spaghetti cabling...

Have you been in an environment where just by touching a cable you can knock stuff down?

## Network Closets

- Beyond cabling considerations, the security of network closets is paramount
  - The confidentiality, integrity, and availability (CIA) of network traffic is potentially at risk
- Organization's network closets should employ robust physical security measures
- Beyond authenticating users, accountability should be enforced and auditable
  - Authentication: allowing authorized users to enter (only)
  - Accountability: knowing who entered and when
- Shared demarcs (network demarcation points) can be problematic

### Network Closets

A physical key offers poor access control: they can be shared, lost, copied, etc. An expert can look at a key and memorize the 'bitting code' (pattern of cuts) and make a copy based on that memory (or a photograph). Combination locks are also poor: combinations can be shared, the most frequently used buttons can show signs of wear, etc.

Ultimately: electronic locks are best, whether a smart card, mag stripe, or using technologies such as RFID. These allow enforcing authentication (who gets in), and well as accountability (knowing who got in after the fact). Access can also be revoked on a per-user basis.

Building with shared tenancy usually has one demarc: the network demarcation point, which describes where the ISPs' responsibilities end and the customers begin. The demarc is crossed by a (shared) cable between ISP equipment and customers.

Unauthorized access to shared demarc puts all of the tenants' network data at risk as it crosses in and out of the building. It also enlarges the scope of mistakes (layer 8) from one organization to many. This means a mistake by an employee of another organization can threaten a different organization's data.

Some security-minded organizations would refuse tenancy in a multi-tenant building for this reason (and other related physical risks). Other build the 2<sup>nd</sup> demarc to control their demarc directly and exclusively.

## Layer 1: Physical Access

- Securing layer 1 requires securing physical access to the network, systems, and facilities
- Most commercial office buildings offer weak physical security
- Office personnel can also be tricked into allowing black hats to enter via social engineering attacks
- One common targeted physical attack: gain temporary access to an office, and deploy a penetration testing drop box



### Layer 1: Physical Access

Most commercial office buildings can be accessed via skilled social engineers. John Strand described this attack in his DerbyCon 2017 Keynote, "I had my Mom break into prison then we had pie"<sup>1</sup>

John's company (Black Hills Information Security) was hired to break into a prison and compromise computer systems physically. John's mother Rita had experience conducting kitchen inspections, checking for temperature, cleanliness, etc. She walked into the prison carrying a clipboard and announced she was there to conduct a routine kitchen inspection. She was immediately ushered into prison and given free rein to conduct her inspection. John's team supplied her with Rubber Duckies, which are weaponized USB keyboards we will discuss next. She inserted the Rubber Duckies into the USB ports she could find, and they immediately downloaded payloads and phoned home back to the Black Hills listening agents.

A penetration testing drop box is an inexpensive system designed to be physically deployed inside a building after gaining temporary physical access. They can be built for less than \$100 US, cheap enough to be deployed and lost. Pictured above is a Raspberry Pi with "WarBerryPi" installed:

*WarBerryPi was built to be used as a hardware implant during red teaming scenarios where we want to obtain as much information as possible in a short period of time with being as stealth as possible. Just find a network port and plug it in. The scripts have been designed in a way that the approach is targeted to avoid noise in the network that could lead to detection and to be as efficient as possible. The WarBerry script is a collection of scanning tools put together to provide that functionality.<sup>2</sup>*

[1] <https://www.youtube.com/watch?v=Upa6lEwnTTo>

[2] <https://github.com/secgroundzero/warberry>



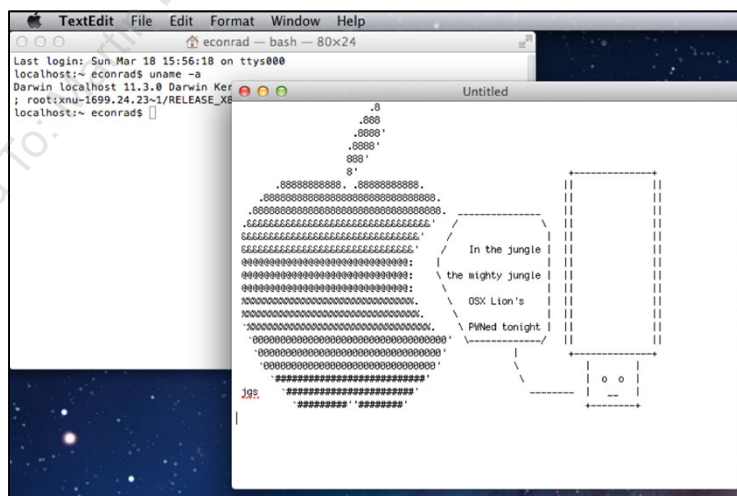
## Weaponized USB Keyboards

- The image to the right<sup>1</sup> is a Rubber Ducky, which is a USB keyboard in the size/shape of USB 'thumb drive"
- These can be loaded with payloads that are able to type commands on a logged-in computer
- Commands may include:
  - Disable the firewall and antivirus
  - Surf to a website, download a malicious payload, and execute it
- The following operating systems allowed an unknown USB keyboard to be plugged into a system with a logged-in user and send keystrokes with no user interaction:
  - Windows 7, Ubuntu Linux server and Desktop, macOS, FreeBSD and OpenBSD



### Weaponized USB Keyboards

A course author performed a lightning talk on USB keyboards called "USB Reloaded: the Teensy Attack."<sup>2</sup> The risk of USB keyboards are not mitigated by controls such as autorun, which mitigate USB disks. The keyboards require a logged-in user, and once inserted: are able to run any command the logged-in user has permission to run. The typical approach is to download a Metasploit Meterpreter payload and run it. The payload would connect outbound to a listening agent running on a black hat's system, proving inbound access to the compromised system. The author used a USB keyboard to perform the actions shown below on a macOS system.<sup>3</sup>



[1] <https://hakshop.com/products/usb-rubber-ducky-deluxe>

[2] <https://www.ericconrad.com/2012/03/im-posting-this-information-in-advance.html>

[3] Ibid.



## USB Keyboard Mitigations Are Limited

- USB devices have PIDs (Product IDs) and VIDs (Vendor IDs)
  - In theory: devices could be restricted to using approved PIDs and VIDs
  - Unfortunately, these can also be spoofed by the USB devices
  - This is still a reasonable mitigation, since the attacker would need to know the approved PIDs and VIDs in use
- For very secure sites: USB devices are designed to have a unique serial number
  - Unfortunately (again): the serial number is usually left blank on most USB keyboards.
- For sites requiring high security: mitigations include facility security, and physically blocking USB devices
  - These sites may also purchase USB keyboards with populated serial numbers, and then lock down systems to allow those serial numbers only

### USB Keyboard Mitigations Are Limited

The screenshot below shows the Vendor ID 046d (Logitech) and product ID c52e (MK260 Wireless Combo Receiver)<sup>1</sup> The serial number is blank, which is quite common.



The screenshot above is from NirSoft's USBDeview, available at:  
[http://www.nirsoft.net/utils/usb\\_devices\\_view.html](http://www.nirsoft.net/utils/usb_devices_view.html)

[1] <http://www.linux-usb.org/usb.ids>

## Layer One Mitigations

- Pen testing drop boxes require (temporary) physical access
  - Wired Ethernet versions also require finding (or reusing) an open network port, ideally in a hidden area such as a closet
- Strong layer 1 and layer 2 defenses are the best mitigations for layer one attacks including penetration testing drop boxes, Rubber Ducky attacks, etc.
  - Maintain physical security of the facility
  - Disable unused switch ports, and place them on a disabled VLAN
  - Use MAC address filtering, 802.1X or NAC
  - We will discuss the layer 2 mitigation options later in 530.1

### Layer One Mitigations

Solid layer 1 and layer 2 security is the best way to mitigate the risk of many layer one attacks, including wired penetration testing drop boxes. This begins with facility security. The next step is disabling all unused switch ports and placing them on an unused VLAN (this provides defense in depth, should the wrong port be accidentally re-enabled. Then use either MAC address filtering (MACsec), 802.1X, and/or NAC to mitigate further the risk of unknown devices being plugged into the network. We will discuss these layer 2 mitigations in detail later during 530.1.

Note that all-wireless versions of penetration testing drop boxes also exist: they typically 'phone home' to the penetration tester via a cellular connection and attempt to hack the local Wi-Fi connection via 802.11. One option is installing Metasploit on an Android cellphone<sup>1</sup>, which has both a cellular and 802.11 adapter built-in. Cheap used Android phones may be bought off sites such as eBay.com for under \$100. This vector is more difficult to mitigate: one of these phones could be mailed into the building, for example. Ultimately, solid Wi-Fi and Bluetooth security are the best mitigations.

[1] <https://android.gadgethacks.com/how-to/install-metasploit-android-0178726/>

## Re-Design & Implement on 530.I – Physical



- Robust physical security
- Color-coding and good quality cables
- Tracking of all staff, visitors and contractors with access to IT equipment
- Secure doors, badge plus code or bio-metric for restricted areas (no visitors)
- Processes including background checks for all staff with access to those areas, including janitors and contractors
- SANS paper on *Physical Security and Why It Is Important*<sup>1</sup>
  - <https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120>



Interested in learning more about cyber security training?

### SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

#### Physical Security and Why It Is Important

Physical security is often a second thought when it comes to information security. Since physical security has technical and administrative elements, it is often overlooked because most organizations focus on technology-oriented security countermeasures. (Harris, 2013) to prevent, tracking attacks.

Copyright SANS Institute  
Author Retains Full Rights

DEEPAARMOR

### Re-Design & Implement on 530.I – Physical

CommScope has made available on its website, free of charge, a 212-page document titled *Enterprise Design Guide: Physical Layer Handbook for Designers and Installers*<sup>2</sup>. According to CommScope, "This guide offers a one-source solution for virtually all the cabling needs of an enterprise system that transmits data, video, voice, and other selected applications. The guide leads installers, contractors and consultants through the process of [designing and implementing](#) an enterprise network."

Adequate controls are not present to control the physical environment without a plan in place. The company must create a team that is responsible for designing a physical security program when planning for security. The physical security team should continually improve the program using the defense in depth method. Defense in depth is a concept used to secure assets and protect life through multiple layers of security. If an attacker compromises one layer, he will still have to penetrate the additional layers to obtain an asset.

[1] <https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120>

[2] [http://nsi-usa.net/images/2009\\_Enterprise\\_Design\\_Guide.pdf](http://nsi-usa.net/images/2009_Enterprise_Design_Guide.pdf)

## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. Course Overview
2. Defensible Security Architecture
3. Traditional Security Architecture Deficiencies
4. Winning Defensible Security Techniques
5. Security Models
6. Threat, Vulnerability, and Data Flow Analysis
7. EXERCISE: Egress Analysis
8. Physical Security
9. **Wireless**
10. Layer 2 Attacks and Mitigation
11. EXERCISE: Identifying Layer 2 Attacks
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. EXERCISE: Architecting for Flow Data
16. 530.1 Summary

### Course Roadmap

We will next discuss wireless security.

## Wireless

### Multiple forms of wireless network communication

- **802.11** - Wireless standards and Wi-Fi technologies
- **Bluetooth** - Low-bandwidth, short-range
- **Zigbee** - Low-power, low-bandwidth, short-range
- **Z-Wave** - Low-power, low-bandwidth, short-range
- **Cellular** - Mobile networking over a wide area
- **Infrared** - Short-range communication (cannot penetrate walls)
- **Radio-frequency identification (RFID)** - Active or passive short-range communication often used for inventory or badges

### Wireless

When thinking of layer-1 access, organizations need to remember that it is more than just communication over a cable. Multiple wireless technologies exist, and new ones are constantly being introduced. The most common is 802.11. 802.11 comes in many editions such as 802.11a, 802.11g, 802.11n and 802.11ac. Each version varies in distance and throughput supported.

Other wireless technologies exist such as Bluetooth. Bluetooth is designed for short-range device-to-device communication. Bluetooth is commonly found on mobile devices and is used for things like hands-free headsets, credit card readers, portable speakers, and Bluetooth enabled smart home devices. Smart home devices and industrial control systems often are standardized with either Zigbee or Z-Wave wireless. Zigbee and Z-Wave are low-power, low-bandwidth, short-range communication technologies that are designed to work in mesh networking. Supporting a mesh network allows communication to hop from one device to another to extend the range without requiring more power consumption. Zigbee supports up to 65K nodes. Z-wave supports up to 232 nodes.

Other network types include cellular networks, which allows mobile devices to connect through cellular towers to have a mobile long-range network, and radio-frequency identification (RFID), which allows for extremely short range communication. RFID is commonly used for digital inventory and security badges. RFID devices can be passive, which means they have no power, or active, which means they have a power source such as a battery. Passive RFID devices are powered by an RFID reader.

<https://www.electronicdesign.com/communications/what-s-difference-between-zigbee-and-z-wave>

<https://www.lifewire.com/definition-of-infrared-817726>

<https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm>

## Wireless Risk

What is the real risk?

- **Logic:** Hacker must be physically present
- **Truth:** Physical access is not required



Consider the internet of things

- Security cameras (802.11, infrared, and wired)
  - Neighbors wired internet facing camera is compromised
  - Wireless interface can be used to find additional victims
- Mobile phones (cellular, 802.11, Bluetooth, and infrared)
  - Employees will bring infected phones within range of corporate wireless

### Wireless Risk

An attack against a wireless device requires proximity to the device. However, proximity to a device does not require an adversary to be present. For example, malware can spread by taking over internet facing devices such as security cameras, wireless routers, and mobile phones. Once infected, the wireless communication protocols on these devices can be used to target other systems. All of this is possible without human intervention or presence.

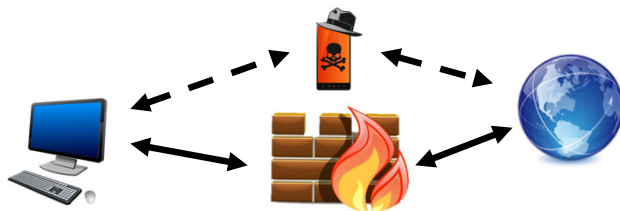
The truth is social engineering, and client-side attacks are so successful that wireless attacks may not be necessary. However, that does not mean that an automated attack cannot occur over wireless or that an adversary may attempt to find and compromise nearby wireless devices in an effort to attack your organization via wireless. In some organizations, internal controls are tight, yet wireless security is not.

## Dual-Homed Devices

A dual-homed device has more than one network interface

- Such as a corporate desktop with cellular USB connection
  - Bypasses network security controls for a low monthly fee
- Or a corporate laptop using both wireless and wired networking
  - Not a default capability, but easy enough to override and enable

Detection requires looking for multiple active routes



ifIndex	DestinationPrefix	NextHop
30	0.0.0.0/0	192.168.2.1
18	0.0.0.0/0	10.0.1.1

### Dual-Homed Devices

One of the challenges with wireless is that it bypasses an organization's architecture. An organization may spend thousands or millions of dollars to implement a web proxy, next-generation firewall, intrusion prevention, and malware sandboxing only to have all of those technologies bypassed by an employee tethering their cell phone to a workstation. This employee may not be malicious when he or she wishes to access their Facebook or another site, but the end result will be the same: an infected machine.

Detecting a dual-homed device is fairly easy using PowerShell or Python. A simple PowerShell script can find desktops or servers with more than one active route using Get-NetRoute<sup>1</sup>. This cmdlet exists on Windows 8.1 and Server 2012 R2 and later. Older operating systems can use the native route print and capture and manipulate its output. Laptops can be a little more difficult, but the same script can be modified to look for active routes to authorized VPNs or wireless networks.

[1] [https://docs.microsoft.com/en-us/previous-versions/windows/powershell-scripting/dn372890\(v=wps.630\)](https://docs.microsoft.com/en-us/previous-versions/windows/powershell-scripting/dn372890(v=wps.630))



## BYOAP - Bring Your Own Access Point

Large organizations suffer from a BYOAP problem

- Employees purchase and plugin unauthorized access points

Organization's need to find and deal with these devices

- Easy win - Look for odd User-agent strings
  - Consumer devices often check for updates or time using vendor with User-agent strings such as Belkin or Netgear
- Look for NAT traffic
  - Multiple browser User-agent strings from same IP address
  - DNS domain requests to common wireless vendor sites
  - Monitor DHCP or CAM table for wireless MAC OUI prefixes



### BYOAP - Bring Your Own Access Point

Based on one of the course author's experience, organizations are likely to find five to ten unauthorized access points per 10,000 employees on an annual basis. This number is based on service engagements with multiple large organizations. Oddly enough, many organizations are not looking for unauthorized access points unless they utilized some form of Wireless Intrusion Prevention System (WIPS). However, in many cases, the WIPS observed the unauthorized access point, but the finding is ignored.

There are multiple ways to identify unauthorized access points. Two of the easier methods are looking for blatantly obvious User-agent strings such as Belkin and Netgear and finding MAC address Organizationally unique identifier (OUI) prefixes related to unauthorized wireless vendors. Another alternative is to look for multiple User-agent strings from the same source IP address. A typical User-agent string is specific down to the patch level of a browser. This means that if an unauthorized access point has two systems using it that are using different browsers or browsers with different software versions the source IP address reaching out will reflect two different User-agent strings.



## Wireless Intrusion Prevention System (WIPS)

An "evil twin" is a rogue access point masquerading as a legitimate access point (AP)

- Possible by spoofing the BSSID of legitimate AP
  - May include denial-of-service against legitimate AP
- Often combined with man-in-the-middle attacks and phishing



WIPS offers the ability to detect and protect against rogue access points

- One or more radios scan for nearby wireless devices
  - May require a scheduled scan on older devices or continuous mode on new devices
  - May combine wireless scan information with wired scan information
- Report and alert on rogue devices
- May de-authenticate clients or rogue APs (beware legal ramifications)

### Wireless Intrusion Prevention System (WIPS)

Adversaries may introduce rogue access points nearby an organization to trick authorized devices to connect to them. In the simplest form, a rogue access point may start using a service set identifier (SSID) your organization uses. A more sophisticated attack may attempt to denial-of-service a nearby authorized access point and then broadcast with the SSID and basic service set identifier (BSSID) of the legitimate access point. The BSSID is the MAC address of the access point. This may result in authorized clients associating with an unauthorized access point.

If an attacker can trick an authorized asset into connecting to a rogue access point, then they have completed a highly effective man-in-the-middle attack whereby they can control DNS requests, HTTP requests, and more. Such an attack may include service authorized client's fake captive portal pages asking for credentials before providing access. Unfortunately, employees easily fall prey to such an attack.

To combat rogue access points, organizations should consider deploying commercial wireless intrusion prevention systems (WIPS) such as Meraki's Air Marshal<sup>2</sup> or a homegrown solution using open source wireless detection capabilities. Many next-generation firewalls that have wireless radios onboard support continuous wireless scanning and de-authentication capabilities. These capabilities allow quick detection and potential response capabilities in shutting down rogue access points. Older WIPS devices may require scheduled scans as the radio that is needed to perform the scan is the same radio devices connect to for wireless networking. Therefore, when a wireless scan is started, clients cannot connect to or use the radio.

[1] <https://shop.hak5.org/collections/wifi-pineapple-kits>

[2] <https://meraki.cisco.com/blog/2017/10/the-evil-twin/>

## 802.11 Wireless Standards

802.11 is a group of wireless standards

- **802.11n / Wireless N** - Dual-band Wi-Fi supporting multiple wireless signals and antennas
  - Up to 300 Mbps on 2.4 GHz or 5 GHz
- **802.11ac / Wireless AC** - Dual-band Wi-Fi supporting simultaneous connections across bands
  - Up to 1300 Mbps on 5 GHz
  - Up to 450 Mbps on 2.4 GHz
- **802.11w / Protected Management Frames** - Security implementation that adds cryptography to management frames

### 802.11 Wireless Standards

802.11 is commonly associated with Wi-Fi communication. However, 802.11 is actually a compilation of wireless standards. Some of these refer to a standard for wireless communication such as 802.11a, 802.11b, 802.11g, 802.11ag, 802.11n, and 802.11ac. Other 802.11 standards, however, refer to specific capabilities or implementations.

For instance, 802.11w is not a type of 802.11 communication that a wireless network interface card would support. Instead, it is a standard used in wireless communication that adds protection to management frames. Knowledge of 802.11 security standards is important so that you may implement them as they are adopted by vendors.

[1] <https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553>

[2] <https://wirelessccie.blogspot.com/2016/01/80211w-aka-pmf.html>

## Obsolete Wireless Communication

### Wired Equivalent Privacy (WEP) - Uses RC4 for encryption

- Vulnerable to bit flipping which allows changing the content of the packet
  - By flipping bits within an encrypted frame
- Integrity check (IC) field uses a linear CRC-32 checksum to prevent changes
  - But RC4 is a stream cipher that uses XOR and bit flipping carries through XOR
- An Initialization vector is used to change stream
  - But it is a 24-bit field and is cleartext making it easy to cause a collision (brute force)

### Wi-Fi Protected Setup (WPS) - Easy button wireless configuration

- Eight digit PIN (which is effectively seven digits due to having a check digit)
- Four digits checked then next three (10,000 and 1,000 max possibilities)

### Obsolete Wireless Communication

The Wired Equivalent Privacy (WEP) is an early security measure for Wi-fi. However, it has multiple weaknesses and is not considered secure. WEP utilizes the RC4 encryption algorithm which is a stream cipher. This stream cipher operates by XORing plaintext data with a symmetric key to produce ciphertext. The resulting ciphertext can be XORed against the same key to produce plaintext. To secure communication, WEP uses a combination of RC4 with an initialization vector to augment the secret key so that each packet produces a different RC4 key. The initialization vector is 24-bits. The problem is that 24-bits is computationally small and can be brute forced or passively collected and analyzed. On top of the weaknesses in WEP's encryption, WEP also uses a CRC-32 checksum to calculate the integrity of a packet. However, the implementation is faulty as it is linear meaning it is possible to change the packet and flip bits to calculate a matching checksum even though the packet has been modified. The process of bit flipping factors into RC4 encryption because of how the stream cipher functions.

Wi-Fi Protected Setup (WPS) is the easy button method of connecting to wireless. Instead of having to enter a long pre-shared key, users can push a physical button on a wireless access point and then attempt to connect from a wireless client. The WPS system will then push the pre-shared key to the wireless client. WPS is only supported when WPA or WPA2 is in use. Alternatively, clients may be required to provide an eight-digit PIN. The eight-digit PIN is either hard coded or generated by the wireless access point. If the wireless client enters the PIN correctly, then the wireless access point will provide the pre-shared key to connect. The problem with WPS implementations is the eight-digit PIN uses a check digit, so it computationally is only seven digits. Even worse, the PIN is broken in have as the first four-digits are verified separately from the last three. This means an attacker can brute force the first 10,000 possible combinations in the first four digits. After correctly guessing the four-digit PIN, the attacker can brute force the remaining 1,000 possibilities in the three-digit PIN left over. With today's hacking tools this is a simple and automated task.

The moral of the story is that both WEP and WPS are obsolete and broken security technologies. If you still have them, then you should kick off a project to remove them or add compensating controls to systems that are stuck using them.

[1] <https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng-0147340/>

[2] <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

[3] <https://nakedsecurity.sophos.com/2015/04/13/we-told-you-not-to-use-wps-on-your-wi-fi-router-we-told-you-not-to-knit-your-own-crypto/>

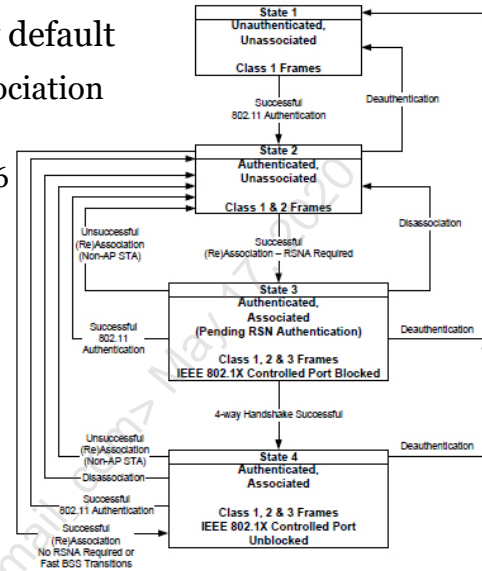
## Protected Management Frames (PMF)

Management frames do not use cryptography by default

- 802.11w adds cryptography support after the association to an access point (AP)
  - Upgrades key management from SHA1 to SHA256
  - Broadcast/multicast frames use cryptography for verifying source addresses
  - Unicast frames use cryptography for integrity checks and encryption

802.11w blocks spoofing attacks such as:

- De-authentication of clients
- Disassociation of clients from APs
- Replay attacks



### Protected Management Frames (PMF)

Because wireless operates as a hub network, all wireless devices are capable of listening and sending wireless frames. Combine the fact that anyone can send or receive wireless frames with spoofing attacks and an adversary can easily perform denial-of-service attacks or combine denial-of-service attacks with other attacks such as attempting to force a client to associate with an unauthorized access point. Spoofing on a wireless network is easy.

802.11w, or protected management frames (PMF), addresses the concern of spoofing attacks by adding cryptography support to specific management frames and actions. In wireless, there are three classes of management frames<sup>1</sup>.

Class 1 - Management frames received before authentication and association such as beacon, probe responses, authentication request and response, and 802.11h spectrum management frames. Because these frames occur before the association, they cannot be protected with encryption or integrity mechanisms<sup>2</sup>

Class 2 - Management frames that cannot be received by non-authentication wireless clients but that are not yet associated with an access point. These frames handle association request and response, re-association request and response, and disassociation frames<sup>3</sup>

Class 3 - Management frames that require being authenticated and associated with an access point. The frames are for disassociation and de-authentication frames, as well as most unicast frames. These frames use cryptography to provide integrity checks and encryption. Integrity checks verify the source address has not been spoofed, and encryption is used to mask the payload of the frame from unauthorized parties<sup>4</sup>

[1] <https://wirelessccie.blogspot.com/2016/01/80211w-aka-pmf.html>

[2] Ibid.

[3] Ibid.

[4] Ibid.

## Guest Management

Guest access could require no authentication and the internet only

- But likely need a terms and conditions page to limit liability

"Special guests" such as vendors may need internal access

- A common practice to use WPA2 with PSK for vendor SSID
  - This often is not secure enough. PSK's tend to be shared with the world
- An alternative is to create temporary accounts per guest user
- Most wireless solutions also support custom registration pages
  - A form asks about who is requesting access and for what purpose
  - Details of the form and approval grant dynamic access

**Remember to disable management services on guest interfaces!**

### Guest Management

Wireless guest access needs to be controlled properly. Often times this means the creation of multiple SSIDs with varying purpose. For example, one SSID may be for internet access only. This may offer internet access to anyone who connects to it and agrees to a terms and conditions page. The terms and conditions page is useful to lower potential legal liabilities such as a guest getting a virus while on your wireless network. This level of guest internet access should never be wide open. Basic controls such as blocking known malicious sites, pornography, drug sites, and more should be blocked to prevent infections or the risk of being sued for allowing inappropriate access.

One or more SSIDs may also be required to handle special guests such as vendors. Many organizations have professional services provided on-site requiring network access. An easy way to provide this access is to create an SSID using WPA2 and a pre-shared key (PSK). However, WPA2 with a PSK grants the same level of access to all devices that connect to it. A better alternative would be to implement WPA2 with user-based authentication or forms-based authentication. By doing so, access controls can be implemented per user, a group of users, or a category selected within a form. The most secure way of doing this is gathering requirements ahead of time and pre-creating a user or group that only has access to what is necessary.

A custom form allows guests to provide information about themselves and why they are requesting access. At the same time, the form can collect information about their machine and in some cases, with the approval of the guest user, scan their machine for malware or the security state of their device. A workflow like this can help automate some of the more tedious components of granting access while decreasing the risk to an organization. The workflow could even be fully automated. For example, if an organization had a service management ticket that a specific person was coming on site to deliver professional services an automated email, text, or phone call could provide the individual with a generated security token or username and password to use when on-site. The user or token could also be created with an expiration date based on the service ticket.

## Station Isolation

- Many corporate wireless solutions offer 'station isolation': a client on a wireless access point may speak to the AP (which is also a switch and a router) only
  - Clients may not access other clients on the same AP
  - Station isolation is also called client isolation

### Default behavior between vendors varies

- Guest networks should have station isolation enabled
  - Prevents infections from spreading from guest to guest
- Highly recommend enabled for all wireless access

### Station Isolation

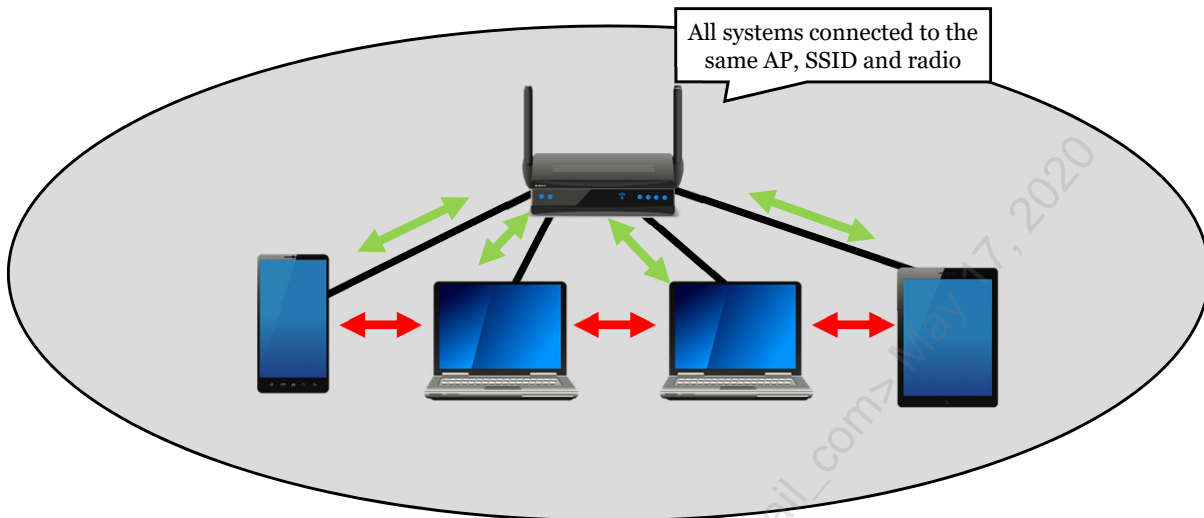
WatchGuard describes station isolation:

*When you configure an SSID for your AP device, you can optionally enable station isolation. The station isolation setting enables you to control whether wireless clients can communicate directly to each other through the AP device. Station isolation prevents direct traffic between wireless clients that connect to the same SSID on the same radio. Station isolation does not prevent direct traffic between wireless clients that connect to the SSID on different AP devices, or between wireless clients that connect to different radios...<sup>1</sup>*

Some wireless solutions also offer a pure guest mode: clients may not access any other devices, wireless or wired, and can simply reach the AP (which is also a switch and a router), and route to the Internet. This mode is great for pure Internet access (and we wish more hotels and coffee shops used this feature) but is not appropriate for the enterprise (which will normally require local access to other servers).

[1] [https://www.watchguard.com/help/docs/wsm/xtm\\_11/en-us/content/en-us/wireless/ap\\_station\\_isolation\\_c.html](https://www.watchguard.com/help/docs/wsm/xtm_11/en-us/content/en-us/wireless/ap_station_isolation_c.html)

## Station Isolation Diagram



### Station Isolation Diagram

Station isolation prevents direct traffic between wireless clients that connect to the same SSID on the same radio. Station isolation does not prevent direct traffic between wireless clients that connect to the SSID on different AP devices.



## Potential Issues with Station Isolation

- Station isolation may create problems in some environments where wireless clients send traffic to each other on the same layer 2 LAN
  - Station isolation on a home network would mean a wireless laptop would not be able to connect to other wireless devices
  - Smart TVs, AppleTV, Roku, Amazon FireTV, Chromecast, etc.
  - This is (usually) an issue unique to homes and small/simple wireless networks, which is why most do not employ station isolation
- This form of wireless/wireless client access is less common in well-designed corporate networks
  - We'll discuss corporate networks shortly

### Potential Issues with Station Isolation

Wireless station isolation works well for 'pure' internet access, such as guest access. It protects (potentially) infected systems from attacking others. The course authors wish all public Wi-Fi used this option.

Station isolation is not normally enabled on home and SOHO (small office/home office) networks, which are more informal than their corporate counterparts.

It's more common to manage wireless devices via a wireless device on informal networks, such as home networks. This largely describes the Internet of Things (IoT): managing your Roku, AppleTV, etc., etc., from a laptop.

Wireless/wireless access is much less common on well-designed corporate networks. Those are normally managed from wired networks, usually from 'trusted' network blocks, such as IT subnets.

Private VLANs, which are the wired equivalent of wireless station isolation, can cause issues in some cases, which we will discuss next.



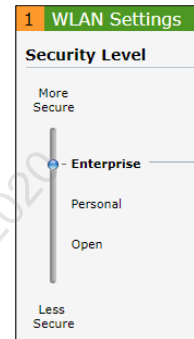
## WPA2 Personal versus WPA2 Enterprise

WPA2 Personal is intended for home or small business use

- The encryption key is a pre-shared key (PSK)

WPA2 Enterprise is intended for businesses

- The encryption key is unique to each client after logging in
- Uses 802.1X authentication and RADIUS servers which allow:
  - Active Directory/LDAP authentication
  - Digital certification authentication
  - Dynamic VLAN placement
  - Centralized key management
  - Fine-grained access control
  - Server <-> Client validation



Unique encryption keys mean less vulnerable to cracking or snooping

Certificate validation helps prevent man-in-the-middle attacks

### WPA2 Personal versus WPA2 Enterprise

Which sounds more secure, personal or enterprise? The answer is clearly enterprise, and there is a lot of truth to that statement when picking WPA2 enterprise over WPA2 personal for wireless. The main difference between the two is how authentication is handled. For WPA2 personal, a pre-shared key is shared with anyone who wishes to connect to wireless. If the key is compromised or pulled off a machine, then the pre-shared key must be changed and all devices need to be updated to use the new key.

WPA2 enterprise handles authentication by using 802.1X port authentication. 802.1X uses a RADIUS server to process authentication attempts. Digital certificates or Active Directory are two common methods of authenticating against a RADIUS server although there are many more ways to authentication. When a RADIUS server is authenticating a wireless client, it has the added advantage of being able to use attributes from a user in Active Directory or within the digital certificate. The attributes can be used to decide what VLAN access is provided to if a login expiration should be applied, or other logical access conditions. Digital certificates also provide server validation and optionally client validation. Implementing bidirectional validation prevents man-in-the-middle attacks as a rogue access point is highly unlikely to spoof or obtain a valid certificate.

While authentication is the main difference between WPA2 personal and enterprise, the way encryption keys are also established is different. With WPA2 personal, the encryption key is the pre-shared key. With WPA2 enterprise, the encryption key is generated per client after successful authentication. Because the key is unique per client session, there is a huge benefit to securing wireless traffic. Now an adversary would have to crack a password per each session, and even if they were able to, they would not be able to use the same key to decrypt the contents of a different client's network traffic.

[1] <https://www.esecurityplanet.com/views/article.php/3907721/15-Reasons-to-Use-Enterprise-WLAN-Security.htm>

## Securing Zigbee

Zigbee operates in one of three modes:

- **Unsecured Mode** - No security enabled
- **Access Control List (ACL) Mode** - MAC-based access control
- **Secured Mode** - Uses a combination of:
  - Access Control - Uses MAC address
  - Frame Encryption - Encrypts frame using AES symmetric key
  - Frame Integrity - Prevents frame from being altered in transit
  - Sequential Freshness - Countermeasure against replay attacks



Low-level security is part of **IEEE 802.15.4**

High-level security is part of the **ZigBee standard**

### Securing Zigbee

Zigbee is a common wireless communication technology used in industrial control systems as well as in other short-range wireless devices. It operates by allowing wireless communication to hop from one device to another until it reaches its expected destination. Security in Zigbee is divided into categories: low-level security and high-level security. Low-level security is defined within the IEEE 802.15.4 standard and consists of MAC address whitelisting. MAC address filtering, a form of whitelisting, is used only to allow communication from authorized nodes based on their MAC address. High-level security is maintained as part of the Zigbee standard. High-level security operates at a higher level of the OSI layer and uses AES cryptography to provide encryption, authentication, and integrity. This includes things such as a 32-bit frame counter maintained for every node a Zigbee device communicates with. This frame counter increments as each packet are received. If a frame is received that does not contain the correct frame counter, then that frame is dropped.

One critical aspect of Zigbee security is the effect cryptography has on the battery life of a device. Zigbee devices must last at least two years to pass Zigbee certification. Yet turning on integrity or encryption controls can significantly impact the batteries lifespan. For example, a battery that lasts five years may decrease to one year if all security is enabled and the most secure crypto algorithms are enabled. The impact of cryptography on batteries varies from vendor to vendor. Therefore, the impact of security settings on batter lifespan needs to be evaluated when selecting devices to purchase or before turning on security settings that were previously disabled.

[1]

[https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Securing\\_ZigBee\\_Wireless\\_Networks.pdf](https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Securing_ZigBee_Wireless_Networks.pdf)

[2] [http://processors.wiki.ti.com/images/7/7b/10\\_-\\_ZigBee\\_Security.pdf](http://processors.wiki.ti.com/images/7/7b/10_-_ZigBee_Security.pdf)

[3] <https://research.kudelskisecurity.com/2017/11/08/zigbee-security-basics-part-2/>

## Securing RFID Badges

Best method: Purchase the right card up front. You want:

- Cards that support rolling codes (code changes on each use)
  - RFID badge and badge service synchronize an initial code
  - The algorithm determines what code will be after each use
  - Often calculates the next 255 possible codes per badge
- Or cards with challenge-response
  - The process is similar to a typical Diffie-Helman key exchange
  - Secret key never is sent in cleartext



If stuck with old RFID cards consider a protective sleeve

### Securing RFID Badges

While security badges are physical in nature, they most commonly use radio frequency identification (RFID), which is a short-range wireless communication method. The badge is often a passive device that has no power, but the badge is powered by a badge reader when it is held close enough to the reader. Unfortunately, many RFID security badge systems today use outdated technology or have key security features disabled. Basically, many RFID badge systems have limited security. As an example, communication between the RFID badge and reader use the Wiegand<sup>1</sup> protocol which was developed in the 1980s. Also, communication from the card to the reader to a centralized control server usually is unencrypted with weak authentication.

When implementing or upgrading an RFID badge system consider purchasing cards that support either rolling codes or challenge-response verification. Rolling codes are not perfect and can be defeated by jammers<sup>1</sup>. For example, it is possible to use a jammer to prevent code from being received while at the same time using another device to capture the code being transmitted. Then the captured code can be replayed. In this example, the code could only be replayed once. However, other forms of attacking rolling codes exist. Yet, rolling codes are significantly better than an RFID badge that does not support rolling codes or challenge-response verification.

A more secure implementation is to purchase cards and card readers that support a challenge-response mechanism such as one-time passwords (OTP). OTP will be covered later in this course. Outside of having more secure cards and card readers, many RFID badge systems have issues detecting physical access to the card reader. For example, if someone were to open or tamper with the reader physically, it should be detected, yet it is not. The lack of detection is from a combination of either not supporting the ability to detect physical tampering or because the ability to detect this is disabled by default in many systems.

[1] <https://www.getkisi.com/blog/hid-keycard-readers-hacked-using-wiegand-protocol-vulnerability>

[2] <https://andrewmohawk.com/2016/02/05/bypassing-rolling-code-systems/>

## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. Course Overview
2. Defensible Security Architecture
3. Traditional Security Architecture Deficiencies
4. Winning Defensible Security Techniques
5. Security Models
6. Threat, Vulnerability, and Data Flow Analysis
7. EXERCISE: Egress Analysis
8. Physical Security
9. Wireless
- 10. Layer 2 Attacks and Mitigation**
11. EXERCISE: Identifying Layer 2 Attacks
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. EXERCISE: Architecting for Flow Data
16. 530.1 Summary

### Course Roadmap

We will next discuss layer 2 attacks and mitigation.

## Discover & Assess on 530.1 – Switches



- Common basic issues related to switches (routers too):
  - Secure administration
  - Services offered
  - Vulnerabilities
  - ACLs
  - Banners
  - Logging
  - Authentication, Authorization and Accounting

### Discover & Assess on 530.1 – Switches

Layer 2 issues are usually ignored. These are similar issues as we will find with routers and that we will discuss later in class. Tools like Nipper, RAT and Yersinia can be used to assess these. More on Nipper tomorrow!

## Threats on 530.1 – Switches

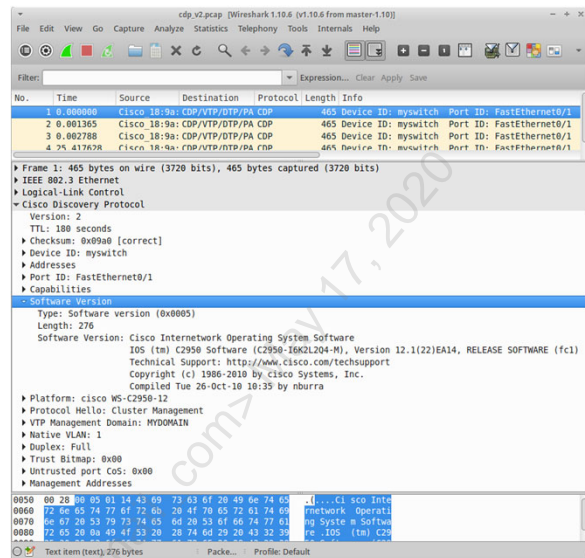


- MAC Flooding Attacks
- 802.1Q and ISL Tagging Attack
- Double-Encapsulated 802.1Q/VLAN Hopping
- ARP Attacks
- Private VLAN Attack
- VLAN Trunking Protocol Attack
- Multicast Brute Force Attack
- Spanning-Tree Attack
- Random Frame Stress Attack

This page intentionally left blank.

## Hardening Against Layer 2 Attacks: CDP

- Cisco Discovery Protocol (CDP) is a layer 2 plaintext broadcast protocol designed for troubleshooting
  - It allows Cisco devices to 'see' each other
- CDP leaks a lot of critical information to every system on the subnet
- CDP should be disabled unless expressly required
- Cisco IOS command to disable CDP globally:
  - Router(config)# **no cdp run**
- CDP may also be disabled per interface:
  - Router(config)# **no cdp enable**



### Hardening Against Layer 2 Attacks: CDP

Cisco Discovery Protocol (CDP) is:

*...a Cisco proprietary Layer 2 protocol designed to facilitate the administration and troubleshooting of network devices by providing information on neighboring equipment. With CDP enabled, network administrators can execute CDP commands that provide them with the platform, model, software version, and even the IP addresses of adjacent equipment.*

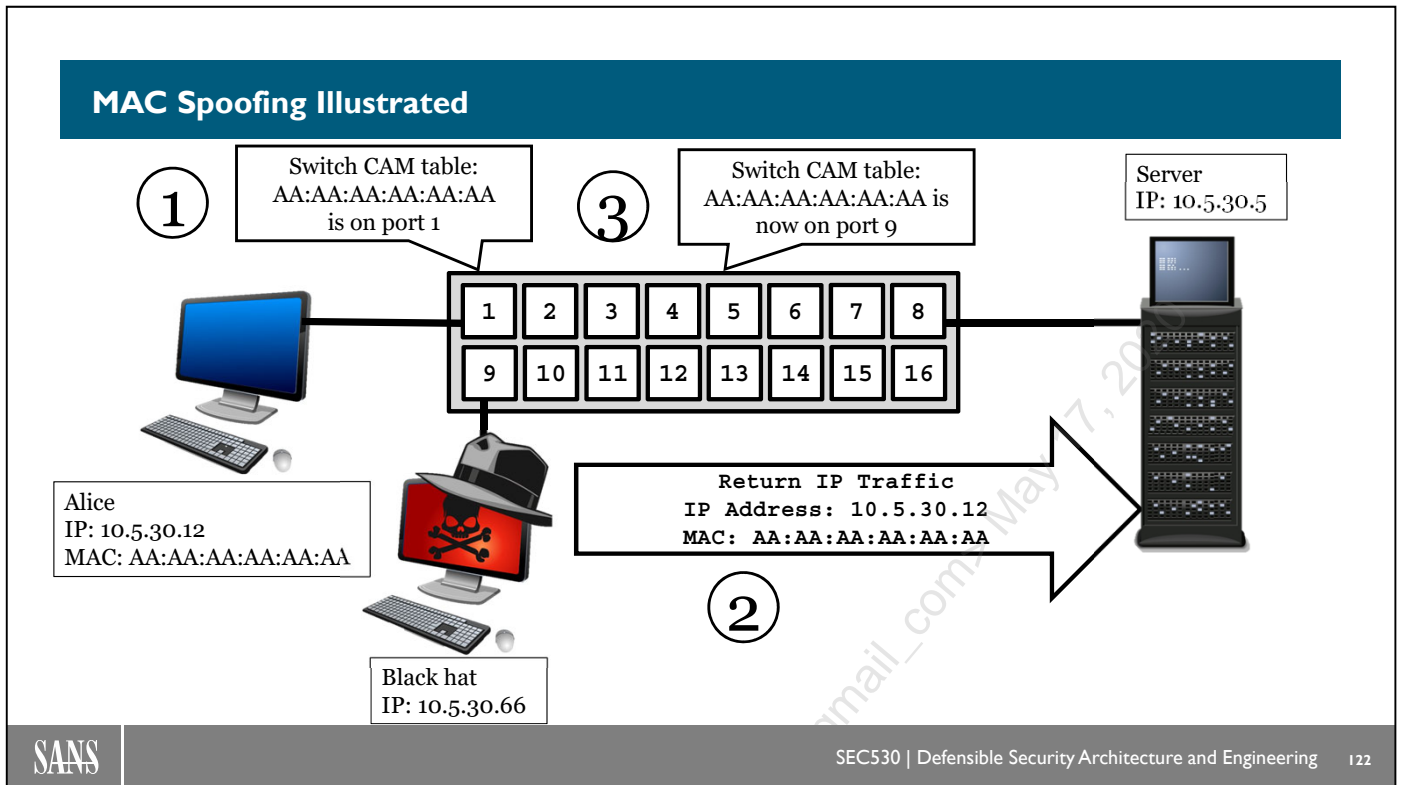
*CDP is a useful protocol but potentially could reveal important information to an attacker. CDP is enabled by default and can be disabled globally or for each interface. The best practice is to disable CDP globally when the service is not used, or per interface when CDP is still required. In cases where CDP is used for troubleshooting or security operations, CDP should be left enabled globally and should be disabled only on those interfaces on which the service may represent a risk, for example, interfaces connecting to the Internet.<sup>1</sup>*

As you can see in the screenshot above, CDP is quite chatty, sending layer 2 broadcast messages including a wealth of information, including:

- The Cisco IOS version: **IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA14, RELEASE SOFTWARE (fc1)**
- Compile date: **Compiled Tue 26-Oct-10 10:35 by nburra**

[1]

[https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline\\_Security/securebasebook/sec\\_chap4.html#wp1056446](https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook/sec_chap4.html#wp1056446)



### MAC Spoofing Illustrated

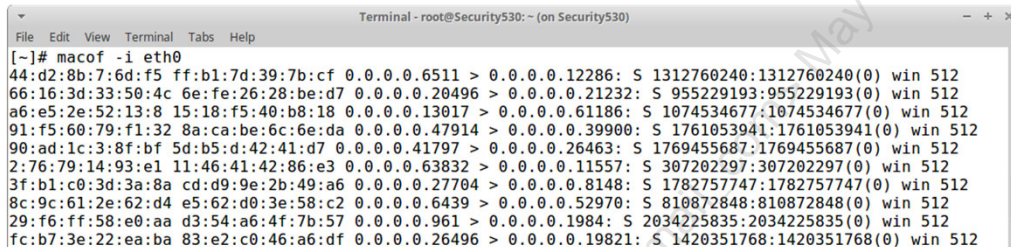
The illustration above shows the **black hat** conducting **MAC spoofing** attack vs the switch. The goal is to have the switch update its CAM table, associating Alice's MAC address with the attacker's port. If successful: frames sent to AA:AA:AA:AA:AA:AA will then be sent to the black hat. This will continue until Alice sends legitimate traffic, at which point the switch would update its CAM table again.

The attack can see-saw back and forth, with the black hat repeating step 1. Or the black hat can attempt to launch a Denial of Service (Dos) attack vs. Alice, attempting to render her system mute (and no longer send traffic)



## CAM Overflow

- The Switch CAM (Content Addressable Memory) maintains a mapping of MAC/Port pairs
- Tools such as macof (part of dsniff) can flood a network with randomly-generated MAC addresses, potentially filling the CAM table
- Once the CAM table is full: some switches will fall back to 'hub mode': sending all frames to all ports



```

Terminal - root@Security530: ~ (on Security530)
File Edit View Terminal Tabs Help
[~]# macof -i eth0
44:d2:8b:7:6d:f5 ff:b1:7d:39:7b:cf 0.0.0.0.6511 > 0.0.0.0.12286: S 1312760240:1312760240(0) win 512
66:16:3d:33:50:4c 6e:fe:26:28:be:d7 0.0.0.0.20496 > 0.0.0.0.21232: S 955229193:955229193(0) win 512
a6:e5:2e:52:13:8 15:18:f5:40:b8:18 0.0.0.0.13017 > 0.0.0.0.61186: S 1074534677:1074534677(0) win 512
91:f5:60:79:f1:32 8a:ca:be:6c:6e:da 0.0.0.0.47914 > 0.0.0.0.39900: S 1761053941:1761053941(0) win 512
90:ad:1c:3:8f:bf 5d:b5:d:42:41:d7 0.0.0.0.41797 > 0.0.0.0.26463: S 1769455687:1769455687(0) win 512
2:76:79:14:93:e1 11:46:41:42:86:e3 0.0.0.0.63832 > 0.0.0.0.11557: S 307202297:307202297(0) win 512
3f:b1:c0:3d:3a:8a cd:d9:9e:2b:49:a6 0.0.0.0.27704 > 0.0.0.0.8148: S 1782757747:1782757747(0) win 512
8c:9c:61:2e:62:d4 e5:62:d0:3e:58:c2 0.0.0.0.6439 > 0.0.0.0.52970: S 810872848:810872848(0) win 512
29:f6:ff:58:e0:aa d3:54:a6:4f:7b:57 0.0.0.0.961 > 0.0.0.0.1984: S 2034225835:2034225835(0) win 512
fc:b7:3e:22:ea:ba 83:e2:c0:46:a6:df 0.0.0.0.26496 > 0.0.0.0.19821: S 1420351768:1420351768(0) win 512

```

## CAM Overflow

Tournas Dimitrios describes macof:

*Macof is a member of the Dsniff suit toolset and mainly used to flood the switch on a local network with MAC addresses. The reason for this is that the switch regulates the flow of data between its ports. It actively monitors (cache) the MAC address on each port, which helps it pass data only to its intended target. This is the main difference between a switch and a passive hub. A passive hub has no mapping, and thus broadcasts line data to every port on the device. The data is typically rejected by all network cards, except the one it was intended for. However, in a hubbed network, sniffing data is very easy to accomplish by placing a network card into promiscuous mode. This allows that device to collect all the data passing through a hubbed network simply. While this is nice for a hacker, most networks use switches, which inherently restrict this activity.*

*Dsniff's "macof" generates random MAC addresses exhausting the switch's memory. It is capable of generating 155,000 MAC entries on a switch per minute. Some switches then revert to acting like a hub.*<sup>1</sup>

Typical Cisco switches such as the 3750 support 6,000 entries in the CAM table by default.<sup>1</sup> Macof can send 155,000 per minute, which will flood the table in seconds.

[1] <https://tournasdimitrios1.wordpress.com/2011/03/04/flood-network-with-random-mac-addresses-with-macof-tool/>

[2] <https://community.cisco.com/t5/switching/mac-address-limit/td-p/1962392>

## Port Security

- Layer 2 port security can be used to mitigate the risk of MAC spoofing and CAM overflow
- Additionally: port security can mitigate the risk of rogue devices
  - Many incidents begin when a pre-infected device such as a laptop is plugged into a switch
  - It then normally requests and receives a DHCP address
  - ...and then begins attempting to infect every machine it can reach
- Mitigation options range from hard-coded MAC addresses to 'sticky' MAC addresses, 802.1X and NAC (Network Access Control)

**Port security** is a critical feature offered by managed switches (as opposed to unmanaged switches that offer no management interface).

Port security is primarily focused on controlling the MAC address that is allowed to connect to each port (and also to prevent multiple MACs on one port).

Options range from simple and automated (sticky MAC addresses) to simple and manual (hard-coded MAC addresses) to complex and automated (802.1X and NAC).

We will discuss these options next.

## Hard-Coded MAC Addresses

- One simple (but high-maintenance) option is to hard-code the MAC address of each connected system
  - Unused ports should be 'shutdown', requiring enabling on the switch before they may be used
- Here is a simple sample client configuration, details explained in the notes

```
interface FastEthernet0/5
  switchport access vlan 10
  switchport mode access
  switchport port-security
  switchport port-security mac-address 0022.64ae.1e0e
```

### Hard-Coded MAC Addresses

Let's break the configuration down:

```
switchport access vlan 10
```

- We have placed clients on VLAN 10.

```
switchport mode access
```

- This means it is an access port and VLAN tags will not be sent to this port (except for VOIP VLAN information)

```
switchport port-security
```

- Enable port security.

```
switchport port-security mac-address 0022.64ae.1e0e
```

- Only this MAC address may use this port.

Here is a configuration for unused ports. We added 'shutdown' (which administratively disables the port), and placed it on a dedicated VLAN for unused ports: VLAN 66.

```
switchport access
vlan 66
switchport mode access
switchport port-security
shutdown
```

## MAC Limiting and Sticky MAC Addresses

- MAC limiting limits how many MAC addresses may be associated with one port
- Sticky addresses mean the switch will learn the MAC address of each connected system, and automatically add them to the running configuration
  - This automates the process of manually adding addresses, shown on the previous slide

```
interface FastEthernet0/5
  switchport port-security
  switchport security max-mac-count 1
  switchport port-security mac-address sticky
```

### MAC Limiting and Sticky MAC Addresses

In addition to the options shown above, sites should decide how to handle a violation of the maximum MAC address count. As stated previously: this could be a sign of ARP cache poisoning. It could also indicate that a user has connected a network hub to a switch, or perhaps that a network device is malfunctioning. In all of those cases: the network engineering team or Security Operations Center (SOC) should know.

This command will automatically shut the port down when the maximum number of MAC addresses is exceeded::

```
Switch(config-if)# switchport port-security violation shutdown
```

This command will send an SNMP trap, and also increment the Security Violation counter:

```
Switch(config-if)# switchport port-security violation restrict
```

This command will show the port security settings, including the security violation count:

```
Switch(config-if)# show port-security interface FastEthernet0/5
```

## Layer 2 Attacks: ARP

- ARP (Address Resolution Protocol) is used to map layers 2 (MAC addresses) and 3 (IP addresses)
- Unlike CAM overflow and MAC spoofing (which target switches), ARP attacks target end systems
- Some of the worst internal attacks feature ARP spoofing and ARP cache poisoning
  - ARP Spoofing remaps an IP address to a new illegitimate MAC address
  - ARP cache poisoning tricks a system into caching the spoofed ARP entry
- ARP spoofing requires local layer 2 (LAN) access, which makes many sites consider these attacks low probability (and therefore low risk)
  - The reality is: sites may be 1-click away from an infected host
  - If an attacker can escalate privileges to root or Administrator/System: they may attempt ARP spoofing
  - Man-in-the-Middle (MitM) is a common attack: remap the default gateway to another host
  - New (bogus) gateway knows where the real one is, and can pass traffic accordingly

### Layer 2 Attacks: ARP

Note that ARP attacks target end systems: computers, routers, etc. The previous attacks discussed in this section targeted switches. The goal with ARP cache poisoning is to trick an end system into caching a bogus MAC/IP address pair and thus send data to the wrong system.

Cisco describes ARP:

*ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. For example, Host B wants to send information to Host A but does not have the MAC address of Host A in its ARP cache. Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. All hosts within the broadcast domain receive the ARP request, and Host A responds with its MAC address.<sup>1</sup>*

Some of the worst incidents handled by course authors included ARP spoofing attacks, usually remapping the default gateway to a new MAC address. If successful: the new malicious gateway knows the real gateway and can forward traffic accordingly. The victim hosts are now one hop further away from other networks, and now send packets via an additional malicious system

[1] <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dynarp.html#wp1082172>

## ARP: A Trusting Protocol

- Dynamic ARP uses no authentication or encryption
  - It trusts whatever answer is provided, which is common for layer 2 protocols

No.	Time	Source	Destination	Protcl	Length	Info
1	0.000000	HonHaiPr_fc:f1:...	Broadcast	ARP	60	Who has 24.39.21.195? Tell 24.39.21.193
2	0.000031	00:2a:e3:cc:a2:...	HonHaiPr_fc:f1:...	ARP	42	24.39.21.195 is at 00:2a:e3:cc:a2:2c

▶ Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)						
▶ Ethernet II, Src: 00:2a:e3:cc:a2:2c (00:2a:e3:cc:a2:2c), Dst: HonHaiPr_fc:f1:43 (90:48:9a:fc:f1:43)						
▼ Address Resolution Protocol (reply)						
Hardware type: Ethernet (1)						
Protocol type: IPv4 (0x0800)						
Hardware size: 6						
Protocol size: 4						
Opcode: reply (2)						
Sender MAC address: 00:2a:e3:cc:a2:2c (00:2a:e3:cc:a2:2c)						
Sender IP address: 24.39.21.195						
Target MAC address: HonHaiPr_fc:f1:43 (90:48:9a:fc:f1:43)						
Target IP address: 24.39.21.193						

### ARP: A Trusting Protocol

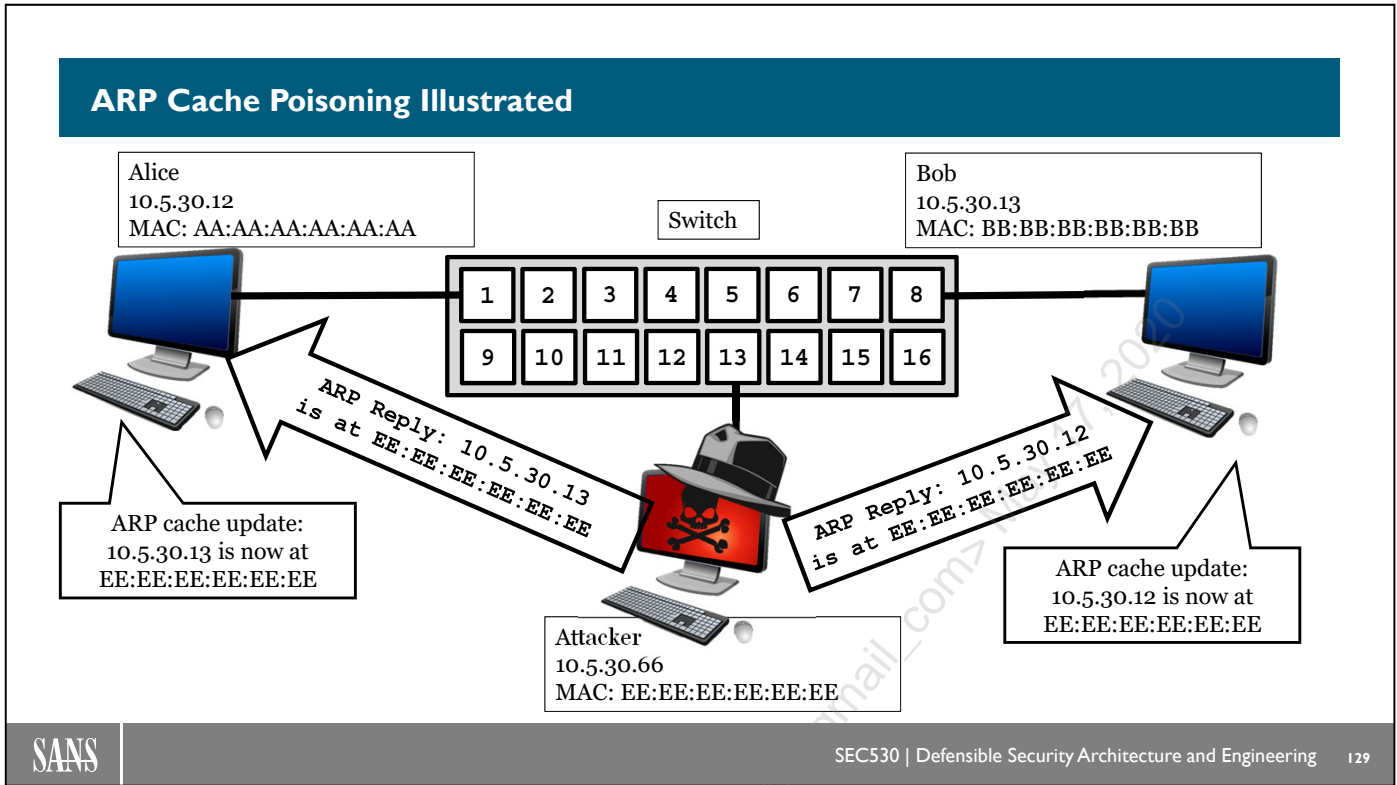
The screenshot above shows an ARP request and reply. The protocol is plaintext and uses no authentication or encryption. It trusts whatever answer it receives, which is common for old protocols (ARP dates to 1982<sup>1</sup>) and is based on the assumption that "the LAN is trusted" (a fallacy we discussed during 530.1).

Here the system at 24.39.21.193 wants to send data to 24.39.21.195. Data sent on a local subnet is addressed to the MAC address. So 24.39.21.193 sends a message the MAC broadcast address FF:FF:FF:FF:FF:FF (note the 'Destination' of 'Broadcast' in the screenshot above), which will be received by every system on that LAN.

Any system on the LAN may answer. In this case the real system at 00:2a:e3:cc:a2:2c answers and supplies its IP address (24.39.21.195).

There is nothing built into the dynamic ARP protocol to stop bogus answers, multiple answers, etc. This can be used maliciously to perform ARP cache spoofing, as we will discuss next.

[1] <https://tools.ietf.org/html/rfc826>



**ARP Cache Poisoning Illustrated**

The illustration above shows the attacker conducting an ARP Cache Poisoning Attack vs Alice and Bob. There are **two methods for performing this**: send a 'gratuitous ARP' (an ARP reply with no matching request) or send a reply when Alice or Bob sends an ARP request to the other. In that case: there is a race, if Alice sent the ARP request, both the attacker and Bob would reply.

Which reply wins? It is operating system (and configuration) dependent. In some cases: the last reply always wins, meaning any reply will replace what's in the cache.

On other operating systems: the first reply will win and be cached for a period of time. On Linux, the default cache time is 60 seconds, you may check the setting with this command:

```
# cat /proc/sys/net/ipv4/neigh/default/gc_stale_time
```

Older versions of Windows had a default ARP cache timeout of two minutes. On Windows Vista and newer: the default ARP cache timeout is randomly set between 15 and 45 seconds.<sup>1</sup>

This Windows command will show the ARP cache settings (listed as 'Reachable Time'):

```
C:\> netsh interface ipv4 show interface <interface number>
```

[1] <https://support.microsoft.com/en-us/help/949589/description-of-address-resolution-protocol-arp-caching-behavior-in-win>



## ARP Spoofing Tools and Mitigation

- Common ARP spoofing tools include Ettercap and Cain & Abel
  - Both are quite easy to use
- Switch-based ARP spoofing mitigations include:
  - DHCP Snooping
    - Configure the switch to trust DHCP responses from specific ports
    - Only allow DHCP responses from these ports
    - Clients will not receive bogus DHCP responses from non-trusted ports
  - Dynamic ARP Inspection (DAI)
    - DHCP snooping creates a binding database of valid MAC/IP pairs it learns by tracking valid DHCP traffic
    - Dynamic ARP Inspection checks this database before forwarding ARP responses

### ARP Spoofing Tools and Mitigation

Ettercap is available at: <http://www.ettercap-project.org/ettercap/>. Cain & Abel is available at: <http://www.oxid.it/cain.html>

Here are the commands to enable DHCP snooping on a Cisco switch:

```
Switch# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)# ip dhcp snooping  
Switch(config)# do show ip dhcp snooping1
```

Here are the commands to enable Dynamic ARP Inspection on a switch interface:

```
Switch# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)# interface fastethernet 5/12 Router(config-if)  
# ip arp inspection trust2
```

[1] <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dynarp.html#wp1062552>

[2] <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html#wpxref12371>



## arpwatch: A Simple ARP IDS

- arpwatch listens on an interface and reports all new layer 2/3 pairings it discovers
  - Logs via syslog, and also sends email for each new pair discovered
- arpwatch will quickly learn all active systems and then become quiet
- After that: it serves as a change detection agent for ARP, reporting:
  - New hosts
  - Changed IP/MAC pairs (possible MAC spoofing)
- arpwatch is quite handy on critical server networks
  - New MAC appears: is there an approved change occurring?

```
root@peaks:/var/log# grep arpwatch *log| grep 'new station'
syslog:Aug  3 15:08:08 peaks arpwatch: new station 24.39.21.193 90:48:9a:fc:f1:43 enp1s0
syslog:Aug  3 15:09:16 peaks arpwatch: new station 24.39.21.195 00:2a:e3:cc:a2:2c enp1s0
syslog:Aug  3 15:29:41 peaks arpwatch: new station 98.0.39.135 90:48:9a:fc:f1:41 enp1s0
syslog:Aug  3 15:35:35 peaks arpwatch: new station 10.105.249.89 90:48:9a:fc:f1:40 enp1s0
syslog:Aug  3 15:37:30 peaks arpwatch: new station 192.168.0.1 90:48:9a:fc:f1:43 enp1s0
```

### arpwatch: A Simple ARP IDS

arpwatch is available from Lawrence Berkeley National Laboratory's (LBNL) Network Research Group:  
<http://ee.lbl.gov/>

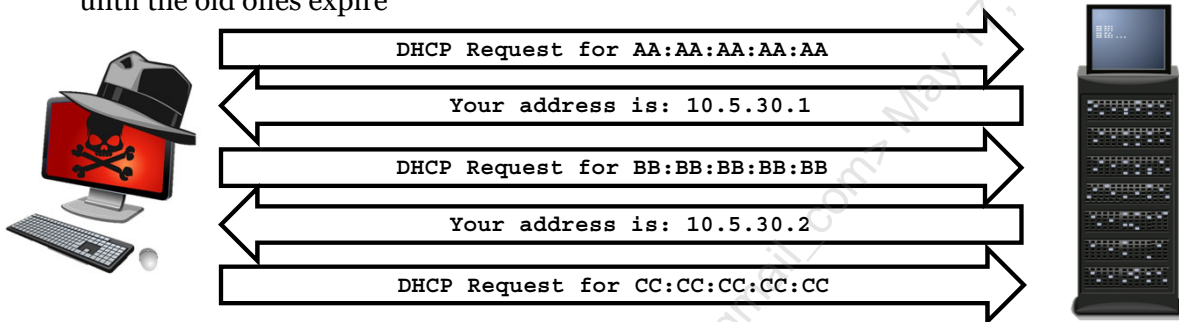
arpwatch reports the following behavior:

- *New activity*
  - *This Ethernet/IP address pair has been used for the first time six months or more.*
- *New station*
  - *The Ethernet address has not been seen before.*
- *Flip flop*
  - *The Ethernet address has changed from the most recently seen address to the second most recently seen address.*
- *Changed Ethernet address*
  - *The host switched to a new Ethernet address.<sup>1</sup>*

[1] <http://ee.lbl.gov/>

## DHCP Starvation

- An attacker may attempt to request all available DHCP addresses
  - This is called a DHCP starvation attack, which often leads to a rogue DHCP server attack (discussed next)
  - Most DHCP servers have a fairly small pool of addresses (often less than 255)
  - Once all leases are claimed: the DHCP server will not be able to offer new leases until the old ones expire



**DHCP starvation** is a simple attack, where one malicious stem requests all available DHCP addresses in the pool. DHCP servers commonly operate on a /24 (class C network), which had 256 total IP addresses.

Assuming the network is 10.5.3.0/24: the first (10.5.30.0) and the last (10.5.30.255) addresses are typically reserved as the network and broadcast addresses, respectively. There is also normally a router (assume it's at 10.5.30.1) and the DHCP server itself (10.5.30.2 in this case). That leaves a maximum of 252 addresses left for the DHCP pool.

Most DHCP servers have no built-in defenses against this type of attack, so the switch must be configured to stop it, as we will discuss in the next section.

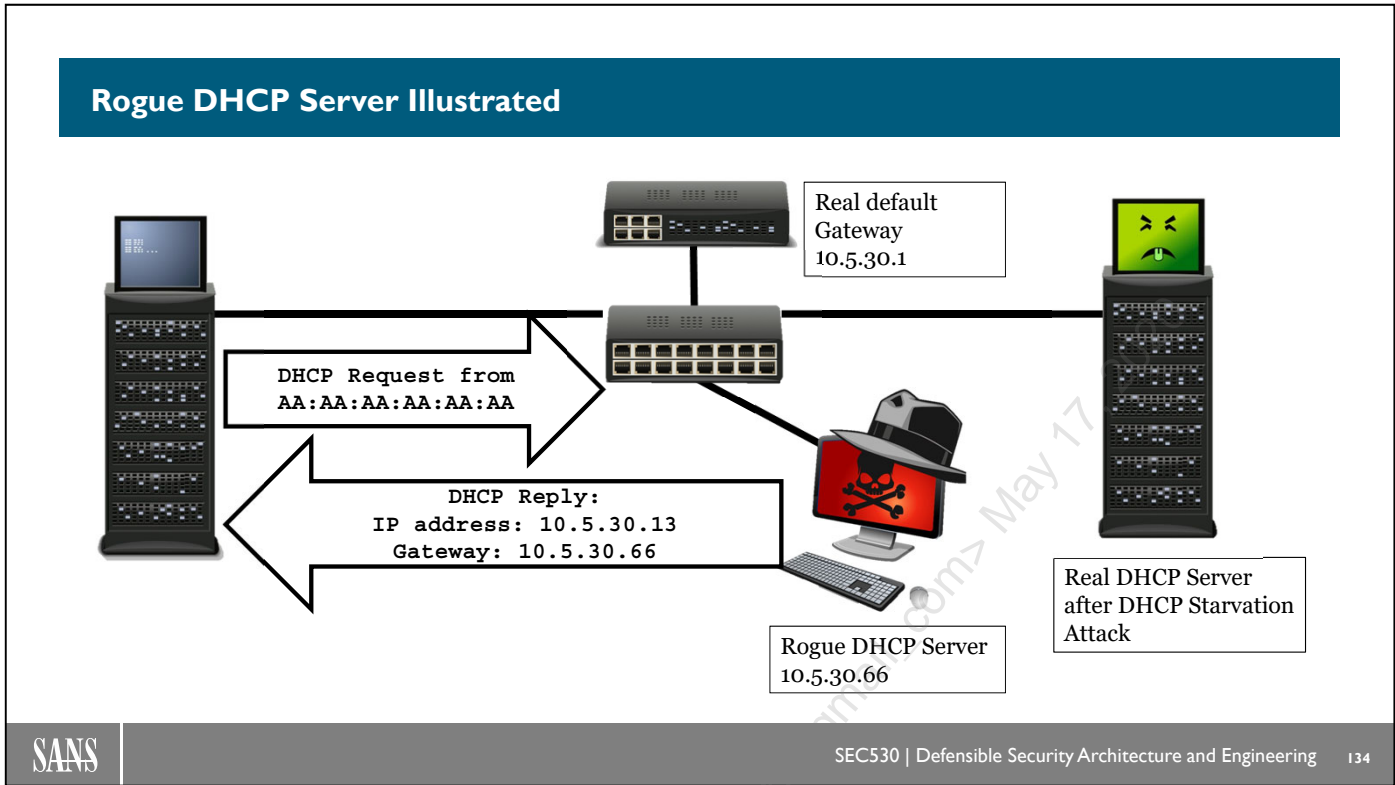
## Rogue DHCP Server

- A rogue DHCP server attack often follows A DHCP starvation attack
- Once the real DHCP server is out of leases: a rogue server can then serve addresses as well as additional information
  - Including the default gateway, DNS, etc.
- This makes launching Man-in-the-Middle attacks quite easy
- It also allows the rogue server to send clients forged DNS responses, directing clients to malicious sites

### Rogue DHCP Server

Any compromised client could potentially attempt a rogue DHCP server attack after performing a DHCP starvation attack. This is quite dangerous since it allows the infected system to set itself as the default gateway, allowing a Man-in-the-Middle (MitM) attack vs any local system. This attack allows the compromised system to see all traffic to/from the LAN, including traffic to other internet networks.

The compromised host can also declare itself (or another malicious server) as the DNS server, allowing it to send clients to malicious sites, such as fake bank sites that will attempt to steal sensitive credentials (and eventually steal money) from victim users.



### Rogue DHCP Server Illustrated

The illustration above shows a rogue DHCP server attack.

The client with MAC address AA:AA:AA:AA:AA:AA sends a broadcast DHCP request, which all systems on the LAN receive, including the real DHCP server. That server will not answer because the pool of DHCP leases is currently exhausted after a successful DHCP starvation attack.

The rogue server answers, serving an address on the local subnet. It will use one of the addresses received after the DHCP starvation attack performed previously. It will also set the default gateway to itself.

The rogue DHCP server knows the real default gateway is at 10.5.30.1, so it is able to forward packets from 10.5.30.13 to other systems via the real default gateway. In other words, the rogue DHCP server has inserted itself as a router, and the victim system is now one hop further away from all remote systems.

## Mitigations: DHCP Attacks

- DHCP Snooping filters DHCP requests sent to untrusted interfaces
  - This mitigates the rogue DHCP server attack
- To enable it on a switch:

```
# ip dhcp snooping
```
- Configure a trusted interface (the DHCP server interface):

```
# interface FastEthernet0/5
# ip dhcp snooping trust
```
- Then enable DHCP snooping non-DHCP server VLANs:

```
# ip dhcp snooping vlan 530
```

### Mitigations: DHCP Attacks

Cisco describes DHCP snooping:

*DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table...*

*DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.<sup>1</sup>*

Be sure to send switch logs to a centralized syslog server or SIEM (as we will discuss later in 530.1). DHCP snooping violations will create logs containing the string "%DHCP\_SNOOPING-5-DHCP\_SNOOPING\_UNTRUSTED\_PORT":

```
Mar 17 09:26:13.924 EST: %DHCP_SNOOPING-5-
DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untrusted
port, message type: DHCPPOFFER, MAC sa: 0012.64f2.1734
```

[1] [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/15-0\\_2\\_se/configuration/guide/3750x\\_cg/swdhcp82.html#49020](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-0_2_se/configuration/guide/3750x_cg/swdhcp82.html#49020)

## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. Course Overview
2. Defensible Security Architecture
3. Traditional Security Architecture Deficiencies
4. Winning Defensible Security Techniques
5. Security Models
6. Threat, Vulnerability, and Data Flow Analysis
7. **EXERCISE: Egress Analysis**
8. Physical Security
9. Wireless
10. Layer 2 Attacks and Mitigation
- 11. EXERCISE: Identifying Layer 2 Attacks**
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. **EXERCISE: Architecting for Flow Data**
16. 530.1 Summary

### Course Roadmap

We will next conduct a lab on identifying layer 2 attacks.



## Exercise 1.2: Identifying Layer 2 Attacks

- Exercise 1.2 is in the digital wiki found in your student VM (recommended)
- Alternatively, you may use your Workbook

### SEC530 Exercise: Identifying Layer 2 Attacks

We will now conduct an exercise on identifying layer 2 attacks.

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020

## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. Course Overview
2. Defensible Security Architecture
3. Traditional Security Architecture Deficiencies
4. Winning Defensible Security Techniques
5. Security Models
6. Threat, Vulnerability, and Data Flow Analysis
7. EXERCISE: Egress Analysis
8. Physical Security
9. Wireless
10. Layer 2 Attacks and Mitigation
11. EXERCISE: Identifying Layer 2 Attacks
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. EXERCISE: Architecting for Flow Data
16. 530.1 Summary

### Course Roadmap

We will next discuss private VLANs.



## Private VLANs (PVLANS)

- Private VLANs are (usually) one of the easiest 'wins' an organization may achieve for making pivoting more difficult to an attacker
  - 'Pivoting' describes the act 'moving behind enemy lines,' when malware (or a person) moves from one compromised internal host to another host
  - Lots of malware will attempt to pivot from one client PC to another
- A private VLAN is the wired equivalent to wireless station isolation
  - If this makes sense for wireless clients: why not wired?

### Private VLANs (PVLANS)

WatchGuard describes station isolation:

*When you configure an SSID for your AP device, you can optionally enable station isolation. The station isolation setting enables you to control whether wireless clients can communicate directly to each other through the AP device. Station isolation prevents direct traffic between wireless clients that connect to the same SSID on the same radio. Station isolation does not prevent direct traffic between wireless clients that connect to the SSID on different AP devices, or between wireless clients that connect to different radios...<sup>1</sup>*

Some wireless solutions also offer a pure guest mode: clients may not access any other devices, wireless or wired, and can simply reach the AP (which is also a switch and a router), and route to the Internet. This mode is great for pure Internet access (and we wish more hotels and coffee shops used this feature) but is not appropriate for the enterprise (which will normally require local access to other servers).

[1] [https://www.watchguard.com/help/docs/wsm/xtm\\_11/en-us/content/en-us/wireless/ap\\_station\\_isolation\\_c.html](https://www.watchguard.com/help/docs/wsm/xtm_11/en-us/content/en-us/wireless/ap_station_isolation_c.html)

## Potential Issues with Private VLANs

- In the enterprise: these issues sometimes come up (most have workarounds)
  - Poorly designed networks that intermingle clients and servers on the same LAN/VLAN
  - Peer-to-peer client traffic
    - Some audio and video chat systems work this way
    - Enterprise solutions can use gateways
  - Some commercial products, such as Tanium, can send updates between clients (in peer-to-peer fashion)
  - Windows 10 has a peer-to-peer patching mode
    - Designed for informal workgroups, and not recommended for the enterprise

### Potential Issues with Private VLANs

The Center for Internet Security (<https://www.cisecurity.org>) discusses private VLANs:

*All network switches will enable Private Virtual Local Area Networks (VLANs) for segmented workstation networks to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to move to compromise neighboring systems laterally.<sup>1</sup>*

The issues described above come up most frequently when testing private VLANs. Most have simple workarounds, such as configuring video and voice chat systems to use gateways (and therefore act in client-server mode).

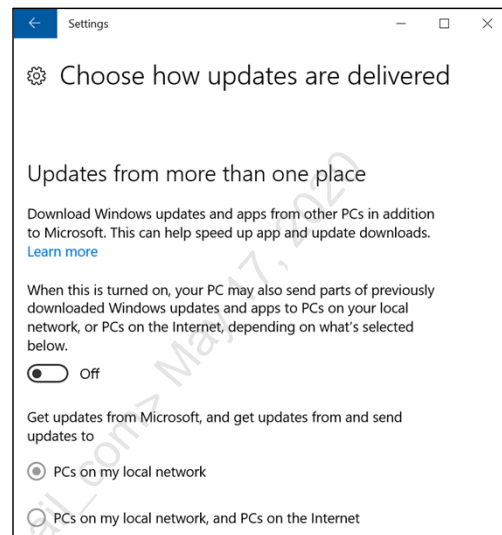
Poorly-designed networks that intermingle both clients and servers on the same layer 2 LAN should be reconfigured before configuring private VLANs.

Windows 10 has a peer-to-peer patching mode called 'delivery optimization,' designed for informal networks, which we will discuss next.

[1] <https://www.defensestorm.com/cybermind/is-your-network-soft/>

## Windows 10 P2P Patching

- Windows 10 offers 'delivery optimization', a peer-to-peer method for delivering software in P2P fashion between client PCs
  - This is designed for informal networks such as homes
- Enterprises should use more robust methods, such as WSUS, for deploying software
- Disable delivery optimization by going to Settings -> Update & Security -> Windows Update -> Advanced Options -> Choose how updates are delivered



### Windows 10 P2P Patching

Delivery optimization will not work if private VLANs are configured properly. This is a benefit, in the author's opinion. Microsoft describes delivery optimization (note the option to use 'PCs on the Internet'):

*In addition to downloading updates and apps from Microsoft, Windows will get updates and apps from other PCs that already have them. You can choose which PCs you get these updates from:*

**PCs on your local network.** *When Windows downloads an update or app, it will look for other PCs on your local network that have already downloaded the update or app using Delivery Optimization.*

*Windows then downloads parts of the file from those PCs and parts of the file from Microsoft. Windows doesn't download the entire file from one place. Instead, the download is broken down into smaller parts. Windows uses the fastest, most reliable download source for each part of the file.*

**PCs on your local network and PCs on the Internet.** *Windows uses the same process as when getting updates and apps from PCs on your local network, and also looks for PCs on the Internet that can be used as a source to download parts of updates and apps.<sup>1</sup>*

Note that Microsoft uses encryption to ensure the integrity of programs downloaded this way.

You may also disable delivery optimization via GPO (group policy object). Microsoft describes how here: <https://support.microsoft.com/en-us/help/3088114/how-to-use-group-policy-to-configure-windows-update-delivery-optimizat>

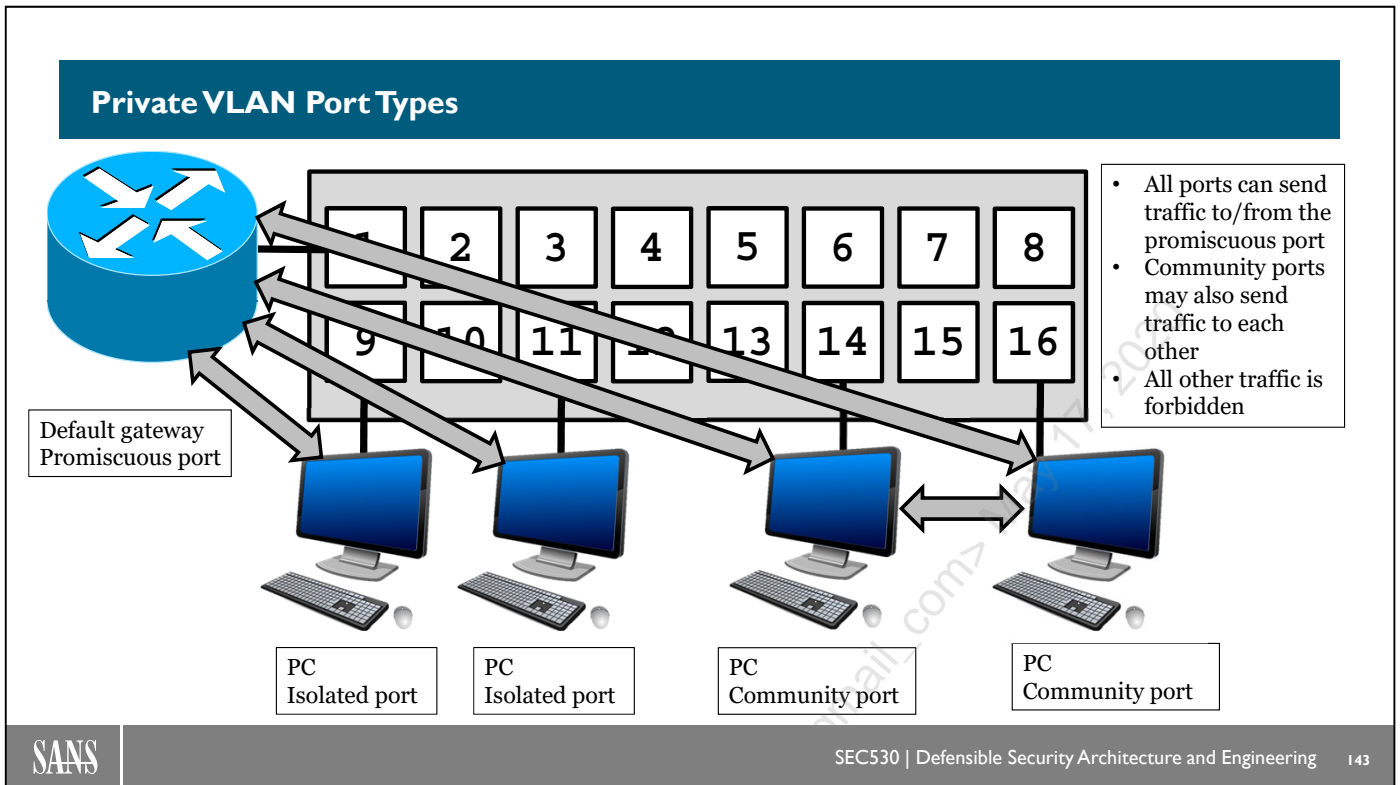
[1] <https://privacy.microsoft.com/en-us/windows-10-windows-update-delivery-optimization>

## Types of Private VLAN Ports

- Promiscuous
  - Able to send traffic to any device on the VLAN
  - Normally includes the default gateway
- Isolated
  - May only communicate with promiscuous ports
  - Cannot send traffic to other ports
- Community
  - May send traffic to promiscuous ports or other community ports
  - Cannot send traffic to isolated ports

### Types of Private VLAN Ports

Private VLANs can be quite flexible. They are able to support a requirement for some systems to speak to each other, such as allowing peer-to-peer traffic, or Tanium updates. In that case, you may place them in the same private VLAN community. They will be able to send traffic to each other, and also to the promiscuous port (normally the default gateway). They will not be able to send traffic to isolated systems. Private VLANs also support multiple communities: these ports may send traffic to members of the same community, but not other communities.



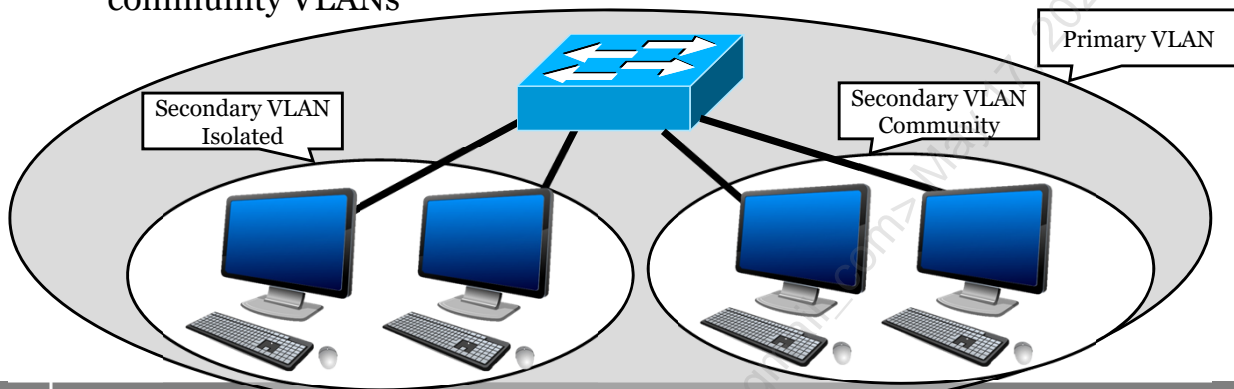
**Private VLAN Port Types**

The diagram above illustrates the three types of private VLAN ports. The router on port 1 can send traffic to all systems on the private VLAN. The PCs attached to the community ports may send traffic to each other, as well as the router. They cannot send traffic to isolated PCs. The isolated PCs may only send traffic to the router. They may not send traffic to each other, or the community PCs.

The diagram above shows one community, but as previously noted: multiple communities are allowed. In that case: members of the same community may communicate, but not to other communities.

## Primary and Secondary VLANs

- Private VLANs support primary and secondary VLANs
  - All systems on the LAN are part of the primary VLAN
  - Systems may also be part of secondary VLANs, such as isolated or community VLANs



### Primary and Secondary VLANs

The following Cisco IOS commands create the primary VLAN (530), as well as the secondary isolated (VLAN 531) and community (VLAN 532). It then associates the isolated and community VLANs with the primary. First, disable VTP (Virtual Trunking Protocol, details on the next page).

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 530
Switch(config-vlan)# private-vlan primary
Switch(config)# vlan 531
Switch(config-vlan)# private-vlan isolated
Switch(config)# vlan 532
Switch(config-vlan)# private-vlan community
Switch(config)# vlan 530
Switch(config-vlan)# private-vlan association 531,532
```

The figure above is based on Cisco Nexus 5000 Series NX-OS Software Configuration Guide, Chapter 'Configuring private VLANs', Figure 1-1, Private VLAN Domain.<sup>2</sup>

[1] [https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/solution\\_guide\\_c78\\_508010.html](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/solution_guide_c78_508010.html)

[2] <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html>

## Private VLAN FUD

- Some network engineers will resist private VLANs, often claiming they require a lot of work
  - This is normally FUD (Fear, Uncertainty, and Doubt)
  - ***The most damaging phrase in the language is “We’ve always done it this way!”***  
– Rear Admiral Grace Murray Hopper
- Many believe (falsely) that private VLANs require creating hundreds or thousands of VLANs (one for each client)
  - You may create a single client VLAN, configure it to be private, and place hundreds or thousands of clients on that single VLAN
  - PVLANS may be trunked with VTP 3 (see notes)
- Testing is certainly required, as discussed previously
  - However, enabling them is simple

### Private VLAN FUD

As noted on the previous page, we disabled VTP as the first step. VTP (Virtual Trunking Protocol) versions 1 and 2 are not compatible with Private VLANs. This error is generated when configuring a switch for private VLANs before disabling VTP:

```
Switch(config-vlan)# private-vlan primary

%Private VLANs can only be configured when VTP is in transparent/off
modes in VTP version 1 or 2 and in server/transparent/off modes in
VTP version 3 when pruning is turned off
```

Cisco describes VTP transparent mode:

*VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements, but transparent switches do forward VTP advertisements that they receive out their trunk ports in VTP Version <sup>1</sup>*

Instead of disabling VTP, another option includes using VTP 3, "In addition to supporting the concept of normal VLANs, VTP version 3 can transfer information regarding Private VLAN (PVLAN) structures."<sup>2</sup>

[1] [https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html#vtp\\_modes](https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html#vtp_modes)

[2] [https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/solution\\_guide\\_c78\\_508010.html](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/solution_guide_c78_508010.html)

## How to Configure Private VLANs

- Configure the primary and secondary VLANs (Cisco IOS commands in the notes of the previous 'Primary and Secondary VLANs' slide)
  - In our example we used:
    - VLAN 530: primary
    - VLAN 531: isolated (secondary)
    - VLAN 532: community (secondary)
- Configure the isolated private VLAN:

```
Switch(config)# int GigabitEthernet0/1
Switch(config)# switchport mode private-vlan host
Switch(config)# switchport private-vlan host-association 530 531
```
- Then configure the promiscuous and community (if used) VLANs, notes below

### How to Configure Private VLANs

The system on interface 0/0 is the router (promiscuous):

```
Switch(config)# int GigabitEthernet0/0
Switch(config)# switchport mode private-vlan promiscuous
Switch(config)# switchport private-vlan mapping 530 531 532
```

This is an isolated system:

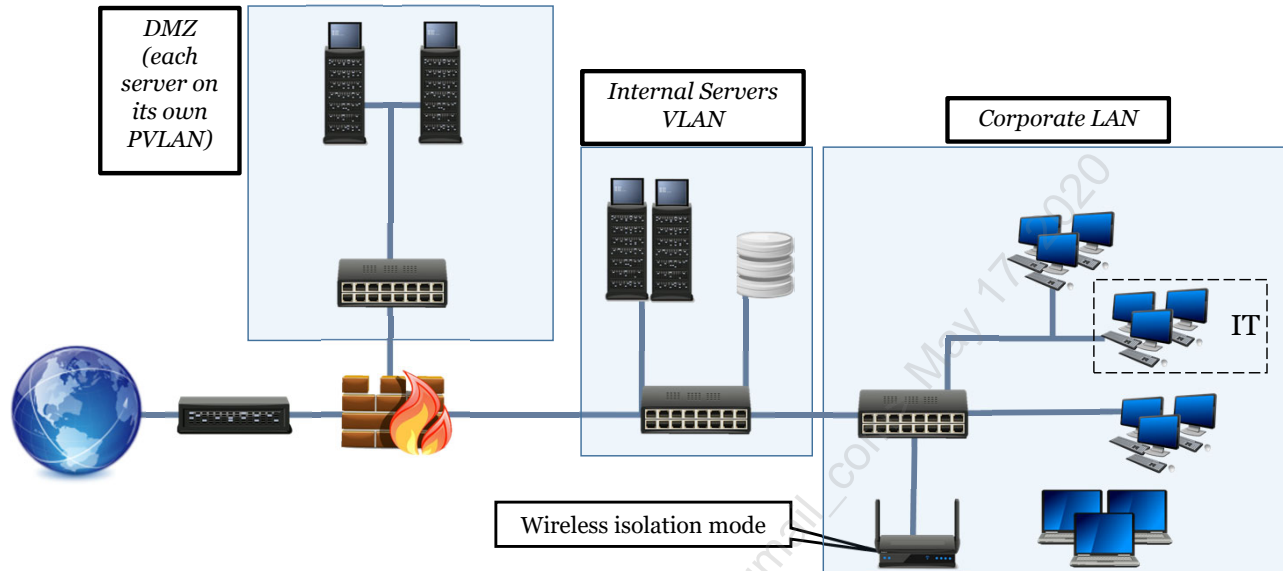
```
Switch(config)# int GigabitEthernet0/1
Switch(config)# switchport mode private-vlan host
Switch(config)# switchport private-vlan host-association 530 531
```

This is a community system:

```
Switch(config)# int GigabitEthernet0/2
Switch(config)# switchport mode private-vlan host
Switch(config)# switchport private-vlan host-association 530 532
```



### Case Study: Tyrell Corporation



This page intentionally left blank.

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020

## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. Course Overview
2. Defensible Security Architecture
3. Traditional Security Architecture Deficiencies
4. Winning Defensible Security Techniques
5. Security Models
6. Threat, Vulnerability, and Data Flow Analysis
7. EXERCISE: Egress Analysis
8. Physical Security
9. Wireless
10. Layer 2 Attacks and Mitigation
11. EXERCISE: Identifying Layer 2 Attacks
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. EXERCISE: Architecting for Flow Data
16. 530.1 Summary

### Course Roadmap

We will next discuss switch and router best practices.

## Switch and Router Security

- We will address best practices that may apply to both switches and routers in the upcoming sections
- This includes topics such as physical access, console and AUX ports, disabling unused services, and password security
- Note that many devices contain both switching and routing modules
  - These are often called 'layer 3' switches
  - We will treat switches and routers as logically separate, with separate sections for securing each

### Switch and Router Security

While many devices support both layer 2 and layer 3 functionality, the security concerns for each layer are (often) logically separate. We will discuss each layer in a separate section, beginning with switches.

That being said: there are some concerns that apply to both routers and switches. This includes physical access, console and AUX ports, disabling unused services, and password security. We will discuss those issues next.

Happy Router describes layer 3 switches:

*A Layer 3 switch works much like a router because it has the same IP routing table for lookups and it forms a broadcast domain. However, the “switch” part of “Layer 3 switch” is there because:*

1. *The layer 3 switch looks like a switch. It has 24+ Ethernet ports and no WAN interfaces.*
2. *The layer 3 switch will act as a switch when it is connecting devices that are on the same network.*
3. *The layer 3 switch is the same as a switch with the router’s IP routing intelligence built in.*
4. *The switch works very quickly to switch or route the packets it is sent.*

*In other words, the Layer 3 switch is really like a high-speed router without the WAN connectivity.<sup>1</sup>*

[1] <http://www.happyrouter.com/layer-3-switches-explained>

## Physical Access and Ports

- Switches and routers should be placed in secure locations, such as locked network management closets
- Physical access to the device allows a number of attacks, including (physical) man-in-the-middle attacks, to password recovery attacks, to factory resets, and others
- The console (typically used for connecting via a terminal emulator such as putty) and AUX (typically used for modem connections) ports should be secured with passwords
  - The AUX may also be disabled if only the console port is only used

### Physical Access and Ports

This will secure the console port, notes below. Substitute 'aux' for 'console' to secure the AUX port:

```
Router(config)# line console 0
Router(config-line)# exec-timeout 5 0
Router(config-line)# privilege level 15
Router(config-line)# logging synchronous
Router(config-line)# login authentication local_auth
Router(config-line)# transport output ssh
```

This configures console sessions to timeout after 5 minutes, allow privileged access, send console logging messages only after 'enter' is pressed, allow SSH connections \*from\* that session, and use local authentication (the authentication method is configured separately).

Cisco describes console and AUX port security in the *Cisco Guide to Harden Cisco IOS Devices*:

*In Cisco IOS devices, console and auxiliary (AUX) ports are asynchronous lines that can be used for local and remote access to a device. You must be aware that console ports on Cisco IOS devices have special privileges. In particular, these privileges allow an administrator to perform the password recovery procedure. In order to perform password recovery, an unauthenticated attacker would need to have access to the console port and the ability to interrupt power to the device or to cause the device to crash.<sup>1</sup>*

[1] <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#anc43>

## Use SSHv2

- Use SSHv2 for remote connections
  - Cisco's default SSH version is 1.99, which allows either SSHv1 or SSHv2
  - Disable SSHv1 and force SSHv2
  - Never use telnet across a network
- Cisco devices default to an RSA key size of 512 bits
  - Use a 2048 or 4096-bit key
- Set 'ssh authentication-retries' to 3, to make the device drop the connection after three failed logins

### Use SSHv2

Never use telnet via a network, The telnet protocol was first designed in 1971 (!), first described by RFC 137<sup>1</sup>, to run on the pre-IP ARPANET, using a layer 3/4 protocol called NCP (Network Control Protocol).

The following configuration forces the of SSH version 2 (and disables telnet). It first sets the hostname and domain name generates an RSA crypto key, applies this configuration to all VTYS (virtual terminals), and sets the authentication retries to count to 3.

```
Switch(config)# hostname Security530
Switch(config)# ip domain-name sec530.com
Switch(config)# crypto key generate rsa modulus 2048
Switch(config)# line vty 0 15
Switch(config)# transport input ssh
Switch(config)# ip ssh version 2
Switch(config)# ip ssh authentication-retries 3
```

VTYs are used for remote network management connections, such as SSH. The command '`line vty 0 15`' allows 16 simultaneous network management connections.

[1] <https://tools.ietf.org/html/rfc137>

## Disable Unused Services and Legacy Protocols

- *Defensible networks offer a minimum number of services*<sup>1</sup> – Richard Bejtlich
- Routers and switches can run unnecessary (and often legacy) services such as bootp and fingerd
  - The advice here is the same as in the UNIX, Linux, macOS and Windows world: disable unnecessary services
- Disable the following on routers and switches (Cisco IOS syntax is in the notes):
  - bootp, fingerd, httpd, mop, and pad
- Also disable the following if not being used: CDP and SNMP (details in an upcoming section)

### Disable Unused Services and Legacy Protocols

Disable legacy services (details below):

```
Switch(config)# no ip http server
Switch(config)# no ip http secure-server
Switch(config)# no ip finger
Switch(config)# no ip bootp server
Switch(config)# no cdp enable
Switch(config)# no mop enabled
Switch(config)# no service pad
Switch(config)# no service config
```

Description of legacy services:

- fingerd – the finger daemon (fingerd is disabled by default in IOS versions 12.1(5) and 12.1(5)T)
- BOOTP– boot protocol
- CDP – Cisco Discovery Protocol (discussed later)
- PAD (Packet Assembler/Disassembler (PAD), used by X.25 networks)
- MOP - Maintenance Operation Protocol (used by DECNET)
- no service config – disables loading configurations via TFTP (the Trivial File Transfer Protocol)

[1] <http://www.informit.com/store/>

## Enable Centralized Logging

- Enable centralized logging on all relevant network devices, including switches (this section) and routers (in the next section)
  - Send logs to a syslog server or SIEM
- In addition to being a best practice, layer 2 mitigations described in this section can create logs when triggered
- To enable centralized logging on a Cisco switch (to a syslog server at 10.5.30.5):

```
Router (config) # logging buffered
Router (config) # logging 10.5.30.5
```

### Enable Centralized Logging

This "logging buffered" command shown above sets up a log buffer of 4096 bytes (default size). A different size buffer may be chosen, for example:

```
Switch# logging buffered 8192
```

The maximum size is 2147483647 bytes. Cisco warns against large buffer sizes:

*Note Do not make the buffer size too large because the switch could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should not be set to this amount.<sup>1</sup>*

You may also save logs to flash locally:

```
Switch# logging file flash:filename
```

To send logs to multiple syslog servers, simply enter multiple logging commands:

```
Switch# logging 10.5.30.5
Switch# logging 10.5.30.6
```

[1] [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2\\_40\\_se/configuration/guide/scg/swlog.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg/swlog.pdf)

## Loopback Interface

- The loopback interface on a switch or router is used as a dedicated management IP address
  - Note this is a different concept than the IPv4 loopback adapter (lo) or the localhost address (127.0.0.1)
- Switch and router loopback interfaces are beneficial because these devices often have multiple interfaces with IP addresses
- Assume an 8-interface router without a loopback interface:
  - It could theoretically be managed via SSH through any of the interfaces
  - ACLs for controlling traffic from the router (such as syslog) can be challenging to write since any of the eight interfaces could be the source

### Loopback Interface

The Cisco Guide to Harden Cisco IOS Devices describes loopback interfaces:

*One of the most common interfaces that are used for in-band access to a device is the logical loopback interface. Loopback interfaces are always up, whereas physical interfaces can change state, and the interface can potentially not be accessible. It is recommended to add a loopback interface to each device as a management interface and that it be used exclusively for the management plane. This allows the administrator to apply policies throughout the network for the management plane. Once the loopback interface is configured on a device, it can be used by management plane protocols, such as SSH, SNMP, and syslog, in order to send and receive traffic.<sup>1</sup>*

The following commands will create interface Loopback0:

```
Router(config)# int LoopBack0
Router(config-if)# ip address 10.5.100.1 255.255.255.0
```

The same router with 8 interfaces described above could use this loopback address, with advertised routes via all 8 interfaces. That way, the loopback address would be reachable as long as any of the eight interfaces remain up. Also, all management traffic sent from the router would have a source address of the loopback address (regardless of which interface sends it).

[1] <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>



## Use Secure Passwords

- Cisco devices support a variety of password types, with strengths ranging from none (plaintext), to poor (type 7), to reasonable, to strong
- The default password type is type 0 (plaintext)
 

```
Switch(config)# username user0 password Security530
```
- Here is resulting Cisco IOS configuration entry:
 

```
username user0 password 0 Security530
```
- Do not use type 7 passwords (Vigenère Cipher): they are extremely weak
- In order of preference, use type 9 (SCRYPT), type 8 (PBKDF2) or type 5 (salted MD5)
  - We will discuss these next

### Use Secure Passwords

Password security is paramount because switch and router passwords can often be exposed by configuration management systems (which archive switch and router configurations, often on a daily (or faster) basis. They can also be exposed via SNMP (discussed later in 530.2). Or they can sometimes be exposed when a black hat gains access to a less privileged account that is able to show the running configuration (but lacks access to change the device.

Type 0 passwords are the default and are surprisingly common. Type 0 passwords will be changed to type 7 (Vigenère Cipher) with this command. The command is here for documentation purposes: please don't use it (use type 5, 8 or 9).

```
Switch(config)#service password-encryption
```

This results in the 'ciphertext' of '113A1C06020002181D7F7874'. A simple Perl script cracked this under 1 second:

```
Terminal - econrad@Security530:~
File Edit View Terminal Tabs Help
*****
* Cisco (type 7) password tool from www.m00nie.com :D *
* Use for any malice or illegal purposes strictly prohibited! *
*****

1. Decrypt a password
2. Encrypt plain text
3. Quit

Pick either 1, 2 or 3: 1
Enter the encrypted password: 113A1C06020002181D7F7874

Encrypted pass was: 113A1C06020002181D7F7874
Decrypted pass is: Security530
```

## Cisco Type 5, 8, and 9 Password Hashes

- Cisco supports the following password hashes that offer more security
  - Fair: Type 5 (Salted MD5)
  - Better: Type 8 (PBKDF2 –SHA256)
  - Best: Type 9 (SCRYPT)
- Type 8 (PBKDF2-SHA256) and Type 9 (SCRYPT) password hashes were added to Cisco IOS 15 in as of version 15.3(3)M3 (released in 2014)
  - They are relatively new, and many organizations are unaware of them
  - Most sites use type 5 (MD5) which is better than types 0 or 7, but fairly weak today
- Do not use type 4: it is weaker than type 5
  - Type 4 uses one round of SHA256 with no salt<sup>1</sup>
  - This option has been removed from recent versions of Cisco IOS

### Cisco Type 5, 8, and 9 Password Hashes

Here is how to set a type 5 (salted md5) password:

```
Switch(config)# username user5 secret Security530
```

This results in the following Cisco IOS configuration:

```
username user5 secret 5 $1$ToD/$NCPYA7/IrPv8zmgtf4Bwf.
```

Cisco released a security bulletin regarding weaknesses in type 4 passwords:

*Due to an implementation issue, the Type 4 password algorithm does not use PBKDF2 and does not use a salt, but instead performs a single iteration of SHA-256 over the user-provided plaintext password. This approach causes a Type 4 password to be less resilient to brute-force attacks than a Type 5 password of equivalent complexity.<sup>1</sup>*

[1] <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130318-type4>

## Slow Encryption

- There are two basic uses for hashes in information security, with differing needs
  - Hashing for integrity should be cryptographically strong and computationally **inexpensive** (fast)
  - Hashing for passwords cryptographically strong and computationally **expensive** (slow)
- Both PBKDF2-HMAC-SHA256 (Type 8) and SCRYPT (Type 9) are cryptographically strong
  - PBKDF2 is slow, while SCRYPT is even slower
  - Either is reasonable, and type 9 is preferred

### Slow Encryption

This command set the enable password to PBKDF2-HMAC-SHA256 (type 8):

```
Switch(config)# enable algorithm-type sha256 secret Security530
```

This results in the following Cisco IOS configuration:

```
enable secret 8
$8$ageyXcLD68zbSI$fp/flgr3IPMPE.jQjMnZvsbBLingKK/n59gum6ttW2g
```

This command sets the enable password to SCRYPT (type 9):

```
Switch(config)# enable algorithm-type scrypt secret Security530
```

This results in the following Cisco IOS configuration:

```
enable secret 9
$9$7HMiVNcHwGuyyI$qe5Geds4Vvcij5fl6asR3wAv07pDft/iJddDM6gKaF2
```

## Why Use Slow Encryption for Password Hashes?

- Slow encryption is used by modern password hashing algorithms to punish password cracking
- Speed comparisons of cracking common password hash algorithms using an eight NVidia GTX 1080 rig<sup>1</sup>
  - Unsalted MD5: 200 billion hashes/second
  - LM: 148 billion hashes/second
  - Unsalted SHA1: 68 billion hashes/second
  - Hashed MD5 (Cisco IOS type 5): 79 million hashes/second
  - PBKDF2-HMAC-SHA256 (Cisco IOS type 8): 9.4 million hashes/second
  - Scrypt (Cisco IOS type 9): 3.4 million hashes/second
  - Bcrypt: 105,000 hashes/second

### Why Use Slow Encryption for Password Hashes?

Historically, password hashes used algorithms that were computationally fast, such as MD4 and MD5. Windows LanMan (LM), is based on MD4, for example.

Modern password hashing algorithms are designed to punish password cracking. **PHP versions 5.5+ use Bcrypt by default for this reason.**<sup>2</sup>

Ashley Madison suffered a breach, and initially, Bcrypt hashes were all that were available to security researchers:

*Pierce gave up once he passed the 4,000 mark. To run all six million hashes in Pierce's limited pool against the RockYou passwords would have required a whopping 19,493 years, he estimated. With a total 36 million hashed passwords in the Ashley Madison dump, it would have taken 116,958 years to complete the job... Unlike the extremely slow and computationally demanding bcrypt, MD5, SHA1, and a raft of other hashing algorithms were designed to place a minimum of strain on light-weight hardware. That's good for manufacturers of routers, say, and it's even better for crackers. Had Ashley Madison used MD5, for instance, Pierce's server could have completed 11 million guesses per second, a speed that would have allowed him to test all 36 million password hashes in 3.7 years if they were salted and just three seconds if they were unsalted (many sites still do not salt hashes).<sup>1</sup>*

[1] <https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40>

[2] <http://php.net/manual/en/function.password-hash.php>

[2] <https://arstechnica.com/information-technology/2015/08/cracking-all-hacked-ashley-madison-passwords-could-take-a-lifetime/>

## Banners

- Cisco switches and routers support the following banners:
  - Login (shown before all logins)
  - Exec (shown after all logins)
  - MotD (Message of the Day, shown before all logins except SSH, where it is shown after)
- The Login banner is the most critical, since it displays the banner text before authentication is attempted
- Sample configuration syntax shown in the notes

### Banners

The following commands will configure the login banner (shown before all methods of authentication). The banner text above was provided from the United States Department of Justice.<sup>1</sup>

```
Router(config)# banner login ^  
Enter TEXT message. End with the character '^'  
  
This system is for the use of authorized users only. Individuals using this  
computer system without authority, or in excess of their authority, are  
subject to having all of their activities on this system monitored and  
recorded by system personnel. In the course of monitoring individuals  
improperly using this system, or in the course of system maintenance, the  
activities of authorized users may also be monitored. Anyone using this  
system expressly consents to such monitoring and is advised that if such  
monitoring reveals possible evidence of criminal activity, system personnel  
may provide the evidence of such monitoring to law enforcement officials.  
^
```

Cisco devices also support narrower-use banners, including incoming (used with reverse telnet sessions) and slip-ppp banner (used with SLIP and PPP connections)

[1] <https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/cslbul1993-03.txt>

## Cisco Smart Install

- *Smart Install is a plug-and-play configuration and image-management feature that provides zero-touch deployment for new switches. You can ship a switch to a location, place it in the network and power it on with no configuration required on the device.*<sup>1</sup>
- CVE-2018-0171 (released March 28, 2018)<sup>2</sup> describes a remote code execution flaw in Smart Install
- Additionally: the Smart Install protocol **does not require authentication**<sup>3</sup>
  - Patching mitigates CVE-2018-0171 , but not the authentication flaw
- Filter TCP port 4786, and/or disable Smart Install  

```
Switch(config)# no vstack
```

### Cisco Smart Install

A lot of organizations were caught flat-footed by the vulnerabilities in Cisco Smart Install. As noted above: the protocol does not use authentication. This fact was publicly announced by Cisco in February 2017<sup>4</sup>. CVE-2018-0171 received a lot more press (and a CVE number) , but the lack of authentication is more serious, since a fully-patched device may still be compromised.

As we will discuss on the next slide: the widespread DoS and defacement of Cisco switches (initially in Russia and Iran) was originally attributed to CVE-2018-0171 but were more likely caused by the authentication flaw, combined with insufficient filtering of TCP port 4786.

The best solution is patching CVE-2018-0171, filtering port 4786, and disabling Smart Install where it is not used. If Smart Install is required: use ACLs to restrict access from required devices only.

[1]

[https://www.cisco.com/c/en/us/td/docs/switches/lan/smart\\_install/configuration/guide/smart\\_install/concepts.html#37974](https://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install/concepts.html#37974)

[2] <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2>

[3] <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi>

[4] Ibid.





## Shodan Search: port:4786 Cisco

## Shodan Search: port:4786 Cisco

Shodan is:

*...a search engine for Internet-connected devices. Web search engines, such as Google and Bing, are great for finding websites. But what if you're interested in measuring which countries are becoming more connected? Or if you want to know which version of Microsoft IIS is the most popular? Or you want to find the control servers for malware? Maybe a new vulnerability came out, and you want to see how many hosts it could affect? Traditional web search engines don't let you answer those questions.<sup>1</sup>*

The Shodan (<https://www.shodan.io>) search shown above was conducted on April 10, 2018. As noted in the screenshot: **163,388 devices were discovered listening on TCP port 4786, while using "Cisco" in the returned banner.**

The detailed stats are:

## TOP COUNTRIES

- United States 45,530
- Russian Federation 12,039
- China 9,821
- Japan 9,312
- Korea, Republic of 7,922<sup>1</sup>

[1] <https://help.shodan.io/the-basics/what-is-shodan>

[2] <https://www.shodan.io>



## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. Course Overview
2. Defensible Security Architecture
3. Traditional Security Architecture Deficiencies
4. Winning Defensible Security Techniques
5. Security Models
6. Threat, Vulnerability, and Data Flow Analysis
7. EXERCISE: Egress Analysis
8. Physical Security
9. Wireless
10. Layer 2 Attacks and Mitigation
11. EXERCISE: Identifying Layer 2 Attacks
12. Private VLANs
13. Switch and Router Best Practices
- 14. Network Flow**
15. EXERCISE: Architecting for Flow Data
16. 530.1 Summary

### Course Roadmap

We will next discuss network flow data.

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020

## Network Flows

A network flow is a log of connections between systems

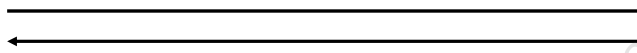
10:33:14 PM

10.5.30.21



Port 53482

Packets 3  
Bytes 234



Packets 3  
Bytes 318



104.24.22.114



Port 443

10:33:19 PM

### Network Flows

The power of flow data is that it provides a log of what happens between two systems. The details of the log include source and destination IP addresses, source and destination ports, and start and end time of the connection. Flow data may also include additional details such as the sourcing network interface.

Flow data is a powerful component that informs organizations about their environment. A single connection can be sufficient to identify malice or abnormalities. For example, a workstation connecting to another workstation is a form of internal pivoting. Flow data easily identifies the connection.

## Flow Data Sources

### Traditional

Direct from network equipment

- Switches / Routers / SDNs
  - NetFlow / Sflow / JFlow
- Firewalls
- VPN Appliances
- Hypervisor Networking
  - Includes cloud flow generation
  - Example: Amazon VPC Flows<sup>1</sup>

### Untraditional

Generate flows from network monitoring

- Suricata
- Zeek
- Packetbeats

Generate flows from endpoints

- Packetbeats
- Sysmon

### Flow Data Sources

Flow data comes in multiple formats and sources. The most common source for flow data is directly from networking equipment such as switches, routers, firewalls, and VPN appliances. These networking devices will generate flow logs as connections are made through networking devices. Cloud environments may also support exporting flow data. Amazon customers can enable VPC flow logs which outputs flow data tied to specific virtual private cloud networks to an Amazon S3 bucket or Amazon CloudWatch<sup>2</sup>.

Alternative methods of generating flow data exist. One modern method is using network security monitoring solutions such as Suricata or Zeek to analyze network traffic and generate flows passively. The advantage to network security monitoring solutions is they are software-based and can make exceptions or adjustments to the flow data that is generated. Another alternative is having a special agent on endpoints that generate flow data. Agent-based flow logging is especially useful in cloud infrastructure that is unable to generate flow logs.

[1] <https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

[2] <https://aws.amazon.com/cloudwatch/>

## Why Flow Data?

- Flow data summarizes network traffic
  - Beyond network summary data, it allows creating utilization graphs at layers 2-4
  - Also helps identify "top talkers" at various layers, and helps understand and baseline normal network applications and services
  - Help trained analysts spot Denial-of-Service (DoS) attacks
  - Can detect network anomalies, including malware beaconing
- Flow data is able to summarize encrypted traffic (since it doesn't inspect the payload data)
- Flow data helps achieve the goal of "Know Thy Network"
  - In the right hands: Flow data is a form of anomaly-based Intrusion Detection System

### Why Flow Data?

Flow data is the Internet equivalent to traffic analysis, developed as part of military communications intelligence (COMINT), which itself is part of signals intelligence (SIGINT). Traffic analysis was pioneered leading up and during World War II.

Traffic analysis is:

*the study of the external characteristics of a message, address, length, time of transmission, frequency and any indicators, along with the location information provided by Huff Duff (High Frequency Direction Finding) allowed intelligence officers to derive a lot of critical information even without reading the contents of a message. Over time the command circuits of the enemy could be identified, allowing for the generation of "Order of Battle" information, i.e. the specific identities of opposing units and their command relationship with superior and subservient units. Analysis of routine messages could identify such things as weather reports, contact reports, unit returns. Deviation from the volume and length of messages could indicate planning for movement or action.*

Cryptanalysis followed traffic analysis but wasn't always necessary to gather actionable information from encrypted transmissions. If an enemy's encrypted radio transmission was headed over the Atlantic Ocean, with a certain frequency and duration: a bomber could fly along the path of the transmission, seeking to destroy that ship that was receiving it.

[1] <http://www.ticomarchive.com/home/singit-in-ww-ii>

## NetFlow Introduction

- NetFlow is an open standard invented by Cisco
  - NetFlow V9 was initially described by RFC 3954<sup>1</sup>, which is an "informational" RFC
  - NetFlow V5 and V9 are commonly used today
  - NetFlow V9 supports layer 2 NetFlow, as well as IPv6
- NetFlow V9 added support for templates, making the protocol more flexible
  - Templates allow adding new features (including support for new protocols) without altering the NetFlow protocol itself.

### NetFlow Introduction

RFCs (Request for Comments) are used to both discuss internet standards under development (labeled "Informational"), as well as publish final internet standards (labeled "Internet Standard"). This can lead to confusion, where some assume all RFCs are 'final'.

As a result, RFC 1796 is an RFC about RFCs, "Not All RFCs are Standards":

*The "Request for Comments" (RFC) document series is the official publication channel for Internet standards documents and other publications of the IESG, IAB, and the Internet community. From time to time, and about every six months in the last few years, someone questions the rationality of publishing both Internet standards and informational documents as RFCs. The argument is generally that this introduces some confusion between "real standards" and "mere publications"...*

*The IAB believes that the community benefitted significantly from having a single archival document series. Documents are easy to find and to retrieve, and file servers are easy to organize. This has been very important over the long term. Experience of the past shows that subseries, or series of limited scope, tend to vanish from the network. And, there is no evidence that alternate document schemes would result in less confusion. Moreover, we believe that the presence of additional documents does not actually hurt the standardization process. The solution which we propose is to publicize better the "standard" status of certain documents, which is made relatively easy by the advent of networked hypertext technologies.<sup>2</sup>*

[1] <https://www.ietf.org/rfc/rfc3954.txt>

[2] <https://tools.ietf.org/html/rfc1796>

## NetFlow

- NetFlow summarizes network traffic, based on frame and packet headers
- Version 9 is able to report:
  - Byte and packet counts
  - Protocol
  - Source and destination addresses (IPv4 and IPv6) and netmasks
  - IP and TCP flags
  - TCP and UDP ports
  - ICMP types and codes
  - Interface used
  - BGP information including Autonomous System
  - ... and much more

**NetFlow** version 9 was expanded to handle more type of protocols, including IPv6, GRE, BGP, MPLS and others. As noted previously, the addition of templates makes NetFlow V9 very flexible, allowing additional protocol support to be added without altering the NetFlow protocol:

*New fields can be added to NetFlow flow records without changing the structure of the export record format. With previous NetFlow versions, adding a new field in the flow record implied a new version of the export protocol format and a new version of the NetFlow collector that supported the parsing of the new export protocol format.<sup>1</sup>*

NetFlowV9 records are grouped into "FlowSets":

*FlowSet is a generic term for a collection of Flow Records that have a similar structure. In an Export Packet, one or more FlowSets follow the Packet Header. There are three different types of FlowSets: Template FlowSet, Options Template FlowSet, and Data FlowSet.<sup>2</sup>*

[1] <https://www.ietf.org/rfc/rfc3954.txt>

[2] Ibid.

## Configuring NetFlow Exporters

- Here is the syntax for setting up Cisco NetFlow exporter

```
Router(config)# ip flow-export destination netflow.sec530.com  
udp-port 2055
```

```
Router(config)# ip flow-export version 9
```

- Then configure each interface to export NetFlow:

```
Router(config)# interface GigabitEthernet0/0
```

```
Router(config-if)# ip flow egress
```

- 'egress' send outbound interface traffic, 'ingress' sends inbound

- Linux syntax is in the notes

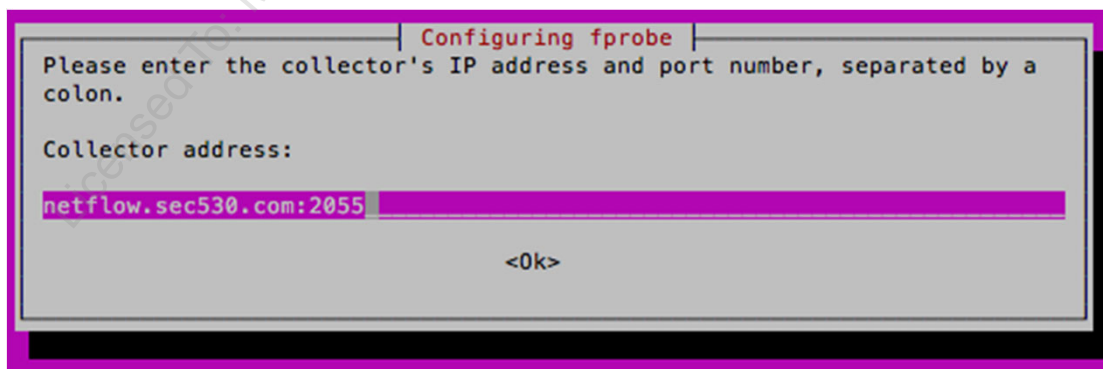
### Configuring NetFlow Exporters

There are a variety of NetFlow exporters available for Linux. One of the easiest to set up is "fprobe", here are the Ubuntu Linux installation instructions:

```
$ sudo apt-get update
```

```
$ sudo apt-get install fprobe
```

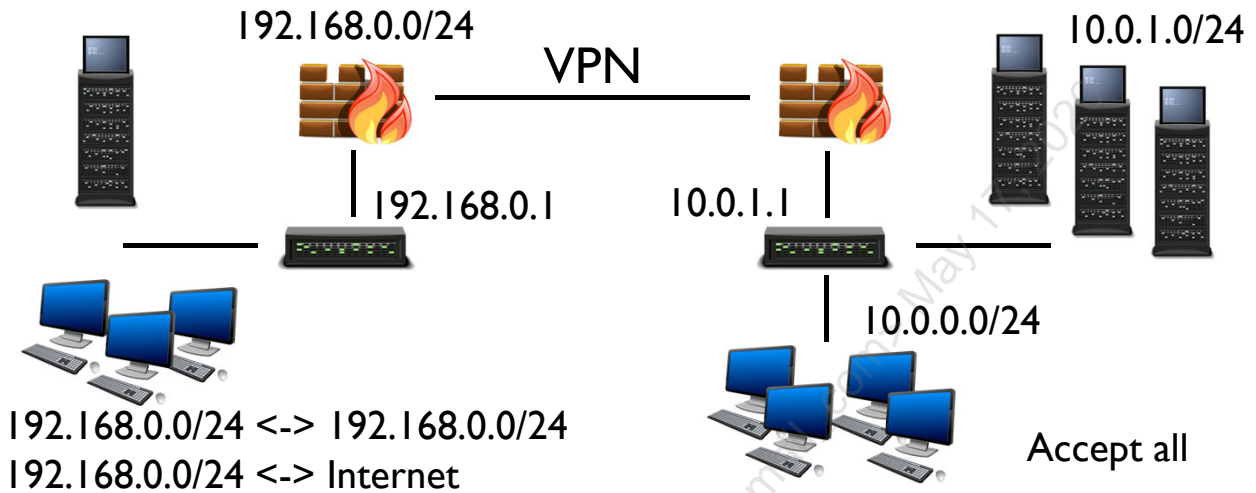
The curses-based install will start. Then choose the interface (such as eth0), and the NetFlow collector name or IP address, and port:



That's all there is to it; fprobe has a very simple setup!

**Flow Planning**

Careful planning is needed to stop duplicate flow creation



**Flow Planning**

One issue that needs to be addressed is the possibility of data duplication. This happens quite frequently with flow data. If you enable flow exports from all switches, then connections that pass multiple switches will generate duplicate logs. For example, if a workstation with an IP of 192.168.0.50 talks to a server at 10.0.1.2 in this diagram, then both switches will see the flow and log it. This is not ideal.

This can be handled in one of two ways. If the software that is creating the flow allows exclusions, then filtering should be done there. Unfortunately, most devices and software do not provide flow filtering. In this case, the data can be sent to a log aggregator, and the aggregator can filter things based on the source of the log.

This slide demonstrates a possible method for eliminating duplicate flow records. In this slide, flow records from 192.168.0.1 that are for sessions from 192.168.0.0/24 to or from 192.168.0.0/24 are accepted. Flow records from 192.168.0.0/24 to and from the Internet are also accepted. Everything else is dropped. This means a flow record that comes from 192.168.0.1 about a session between 192.168.0.50 and 10.0.1.2 would be dropped. However, the flow record would still get sent from 10.0.1.1, and that record would be accepted. The switch at the corporate location would not be filtered. This design works well for organizations with many satellite offices.

If Security Onion (Bro, Snort/Suricata) is used to create flow data, know that it has the capability to filter out data at each sensor. This is done within /etc/nsm/bpf.conf and uses standard BPF syntax.



## Cloud Flows

Infrastructure-as-a-service (IaaS) may support exporting flow data

- Export process different than traditional flows

Amazon supports **VPC Flows**

- Requires flows to be exported to CloudWatch<sup>1</sup>
- Or an S3 bucket<sup>2</sup>
  - Most SIEM solutions natively read files from S3
  - Scripts capable of reading for manual analysis

### Cloud Flows

Some cloud solutions natively support exporting flow logs although it is usually for Infrastructure-as-a-service (IaaS). IaaS solutions incorporate special software-defined networking fabrics that allow exporting flow logs. Amazon is an example of an IaaS solution that supports flow data. In Amazon's solution, one needs to enable VPC flows and then select whether to output them to Amazon's proprietary CloudWatch<sup>1</sup> solution or an Amazon proprietary S3 bucket<sup>2</sup>.

CloudWatch allows you to analyze the logs directly within Amazon's platform. An S3 bucket allows you to use a SIEM or script to ingest the logs and analyze them automatically.

[1] <https://aws.amazon.com/cloudwatch/>

[2] <https://aws.amazon.com/s3/>

## Suricata Flow

**Suricata** is an intrusion detection system that is also capable of network security monitoring (NSM)

- Flow generation is a key component of its capabilities

Flows can be generated unidirectionally or bidirectionally

- **Unidirectional** means source -> destination and destination -> source are two flows
- **Bidirectional** means source <-> destination is one flow

Requires port mirroring or network taps

### Suricata Flow

Software-based flow logging provides a modern approach to a fully customizable approach to flow data. Suricata is an example of a software-based flow solution. Suricata allows analyzing network packets often provided by a port mirror or tap. During analyzing the packets, Suricata will generate either a unidirectional log or a bidirectional log.

A desktop connecting to a web server would generate two logs under unidirectional logging. One log would be for the desktop connecting to the web server, and the other log would be for the web server connecting back to the desktop. With bidirectional flow logs, only one log is generated that contains all the connection information.

## Suricata BPF Filtering

### Software controls exceptions

- Easy to ignore hosts
- Easy to ignore networks
- Easy to ignore combinations of things

Allows eliminating duplicates

```
# Vulnerability scanner
!(host 10.5.30.7) &&

# Logging network
!(net 10.5.31.0/24) &&

# Noisy service
!(dst host 10.5.30.8 &&
dst port 80)
```

### Suricata BPF Filtering

A major benefit from software-based flow logging solutions is the ability to generate logs conditionally. For example, if an organization had three network sensors and a packet passed through each of them, then a flow log would be created three times with the same data. However, a filter can be installed on two of the sensors to ignore traffic from specific hosts, networks, or ports to eliminate duplicate flow logs.

## Filtering Flows

### Traditional

To **lower** chance of duplication

- Limit flow collection points
- Design for ingress or egress
- Use SDN fabrics

To **eliminate** storing duplicates

- Purchase commercial solution
- Send flows to it

### Untraditional

Software flows

- Conditionally log flow data

Endpoint flows

- Conditionally log flow data

### Filtering Flows

Collecting flow logs often result in duplicate data. Duplication is caused because flow data is generated at multiple locations such as routers that traffic passes through. There are multiple strategies to minimize or eliminate duplicate flow logs.

One method is to selectively enable flow logging on network equipment or change flow logs to only be on inbound or outbound traffic by port. However, port exceptions can be unwieldy to manage. Instead, traditional flow logs such as NetFlow can be sent to a commercial analyzer that supports eliminating duplicate flows and potentially supports combining unidirectional flows into bidirectional flows.

Software-based flow logs from endpoints or network solutions offer a lot of flexibility when dealing with duplicate flows. Each asset on its own does not offer duplicate detection. However, each asset can be configured not to generate certain flows thus preventing duplicates and lessening the hardware consumption of the asset.

## Flow Components

Flow data requires the following components:

- Flow exporter
  - Switch, router, firewall, system, etc., that sends flow records to a collector
- Flow collector
  - A system that collects flow records
  - Examples include fprobe, nprobe, and SiLK
- Flow analyzer
  - A system that analyzes and displays flow data
  - Examples include NFsen and ntopng
    - ntopng can collect local NetFlow, and relies on nprobe to collect remote flows
- Some software offers combined flow collector and analyzer functionality
  - Examples include SolarWinds and Scrutinizer

### Flow Components

As discussed above: Flow data requires three components: an exporter, a collector, and an analyzer. Most commercial products offer combined collectors and analyzers.

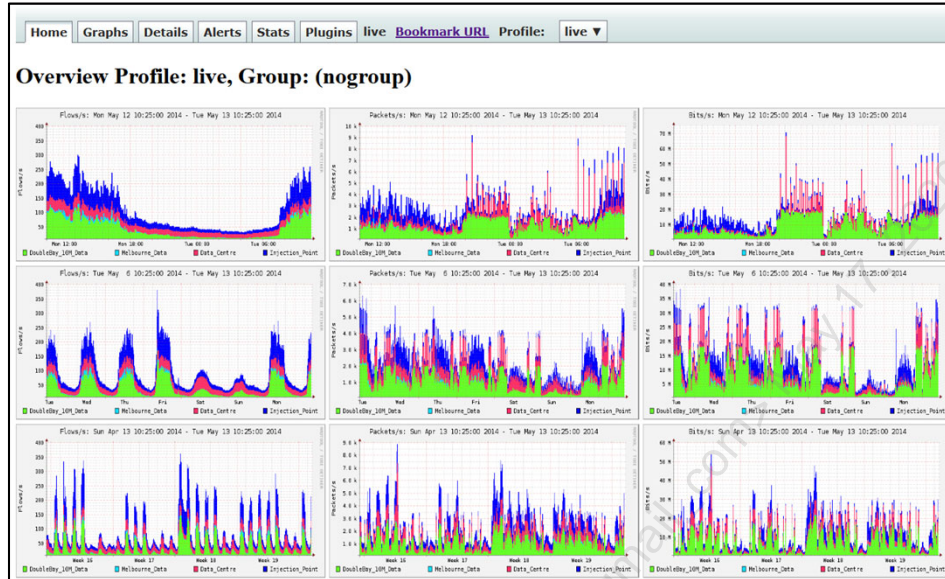
ntopng is an analyzer that also collects local NetFlow. It uses nprobe to collect remote NetFlow. Note that ntopng is the replacement for ntop:

*The way the original ntop was designed was IMHO very advanced for that time, but today is no longer so for many reasons. Today people want to have a flexible network monitoring engine able to scale at multi-Gbit, using limited memory, immune to crashes “no matters what”, scriptable and extensible, able to see what’s happening in realtime with 1-second accuracy, capable of characterising hosts (call it host reputation if you wish) and storing monitoring data on the cloud for (de-) centralised monitoring even of those devices that have no disk space. Over the past years, we have tried to address ntop open issues, but the code base was too old, complicated, bug-prone. In essence, it was time to start over, preserve the good things of ntop, and learn from mistakes. So basically looking forward by creating a new ntop, able to survive (hopefully) 15 more years and set new monitoring standards.<sup>1</sup>*

ntopng is available in community (free), professional and enterprise editions.

[1] <https://www.ntop.org/ntop/its-time-for-a-completely-new-ntop-say-hello-to-ntopng/>

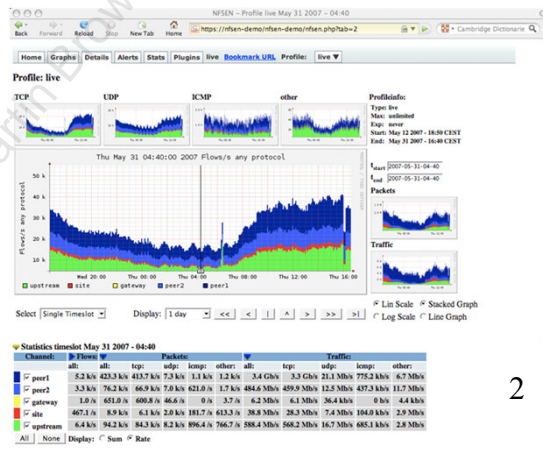
## NFsen NetFlow Analyzer



1

### NFsen NetFlow Analyzer

The NFdump collector and NFsen NetFlow analyzer are one set of open source options. NFsen relies on RRDTool for generating the graphs, which is why the graphs shown above may look familiar to those who have used RRDTool (Round Robin Database Tool. Available at: <https://oss.oetiker.ch/rrdtool/>). The NFsen General Overview Page is shown above. Clicking on any graph takes you to a Navigation Page:



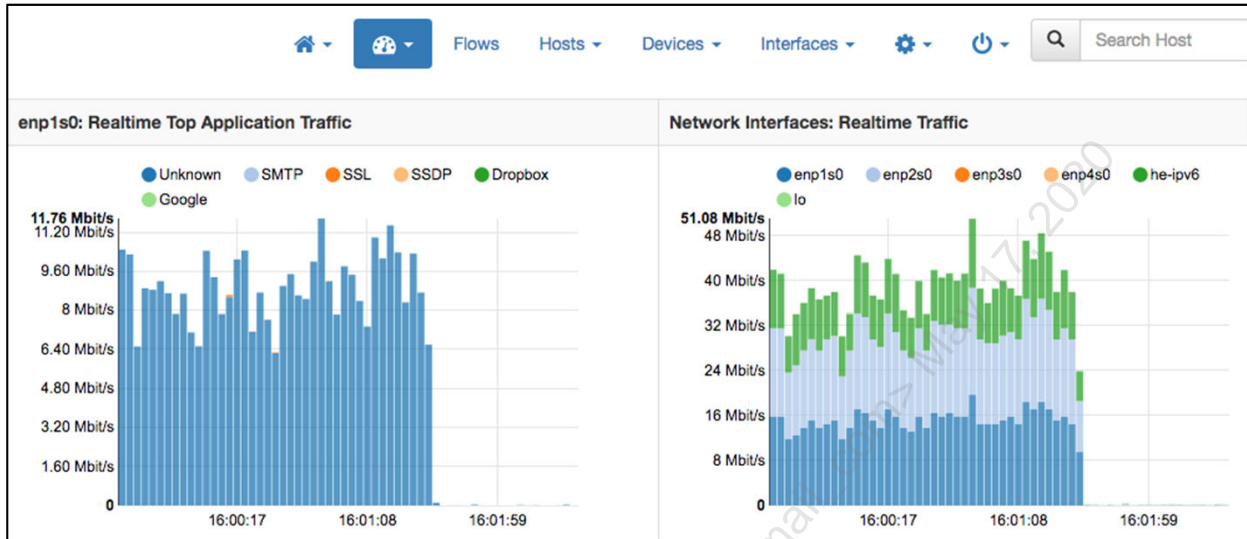
2

- NFdump is available at: <http://nfdump.sourceforge.net/>
- NFsen is available at: <https://sourceforge.net/projects/nfsen/>

[1] <https://sensol.com.au/?tag=sysadmin>

[2] <http://nfsen.sourceforge.net/>

ntopng



ntopng offers one of the easiest installations of the various free options. Installing on Ubuntu Linux was a breeze. The ntopng package repository is here: <http://packages.ntop.org/>

ntopng requires PF\_RING. ntopng will automatically collect local flows and uses nprobe to collect remote flows. Packages for PF\_RING, ntopng, and nprobe for various operating systems are available at the repository linked above.

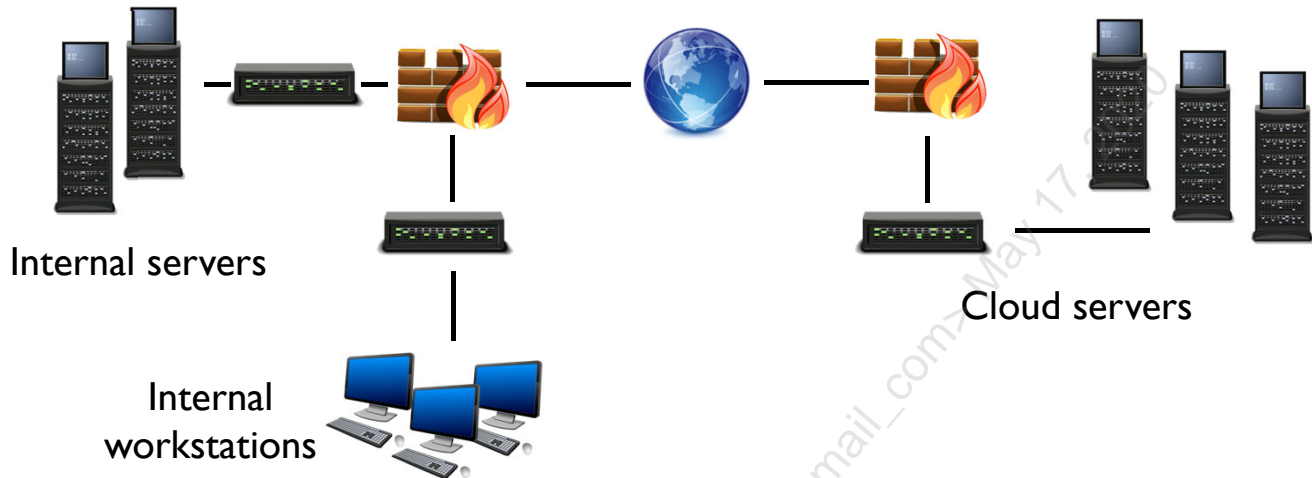
Ntopng contains a wealth of dashboards, here's the Active Flow dashboard:

Active Flows									
	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	Unknown	IPv6	mcs-24-39-21-195.nys.bl...	184.105.253.14	1 min, 29 sec	Client Server	2.66 kbit/s	55.07 KB	
Info	SMTP	TCP	185.244.209.254:44976	mcs-24-39-21-195.nys.bl...:smtp	4 sec	Client Server	0 bps	27.92 KB	
Info	SSL_Microsoft	TCP	mcs-24-39-21-195.nys.bl...:51413	v10.vortex-win.data.micr...:https	1 min, 3 sec	Client Server	0 bit/s	13.73 KB	v10.vortex-win.data.micr...
Info	SSL	TCP	mcs-24-39-21-195.nys.bl...:83566	ghostery-collector.ghost...:https	1 min, 5 sec	Client Server	0 bit/s	13.19 KB	ghostery-collector.ghost...
Info	SSDP	UDP	192.168.0.1:1901	239.255.255.250:1900	1 min, 30 sec	Client	0 bit/s	14.24 KB	
Info	SSL	TCP	mcs-24-39-21-195.nys.bl...:83636	api.shodan.io:https	13 sec	Client Server	0 bit/s	9.74 KB	api.shodan.io
Info	SSL_Dropbox	TCP	mcs-24-39-21-195.nys.bl...:83637	beacon.dropbox.com:https	0 sec	Client Server	0 bit/s	5.73 KB	beacon.dropbox.com
Info	SSL_Dropbox	TCP	162.125.18.133:https	mcs-24-39-21-195.nys.bl...:88403	0 sec	Client Server	0 bit/s	4.12 KB	
Info	SSL_Google	TCP	108.177.112.168:https	mcs-24-39-21-195.nys.bl...:61342	1 min, 25 sec	Client Server	0 bit/s	3.42 KB	
Info	SSL	TCP	mcs-24-39-21-195.nys.bl...:83649	api.shodan.io:https	9 sec	Client Server	0 bit/s	4.82 KB	api.shodan.io



## Flow Design

What would be the ideal flow sources for this environment?



### Flow Design

In this diagram flow, data can be generated in many locations. Traditional flows can be generated at switches, firewalls, and cloud-based IaaS flow logging. Untraditional logs can be generated with software-based network security monitoring or endpoint agents. The question is what combination of flow logs would be ideal for this infrastructure. Multiple right and wrong answers exist.

Cloud IaaS flow logs need to be enabled; otherwise, connections outside the organization would not be logged. Within the organization's infrastructure flow data could be enabled on the switch in front of the workstations and then within a network security monitoring solution in the server subnets. Enabling flow logs on the workstation switch would allow logging workstation to workstation traffic and workstation to server or workstation to the internet traffic. Using a network security monitoring solution within the server subnets would allow logging server to server, internet to the server, and server to internet traffic while making exceptions to not log traffic from or to workstations or the cloud networks. In this example, only traffic from workstations to or from the cloud systems would cause duplicate traffic.



## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. Course Overview
2. Defensible Security Architecture
3. Traditional Security Architecture Deficiencies
4. Winning Defensible Security Techniques
5. Security Models
6. Threat, Vulnerability, and Data Flow Analysis
7. **EXERCISE: Egress Analysis**
8. Physical Security
9. Wireless
10. Layer 2 Attacks and Mitigation
11. **EXERCISE: Identifying Layer 2 Attacks**
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. **EXERCISE: Architecting for Flow Data**
16. 530.1 Summary

### Course Roadmap

We will next conduct a lab on architecting for flow data.

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020



## Exercise 1.3: Architecting for Flow Data

- Exercise 1.3 is in the digital wiki found in your student VM (recommended)
- Alternatively, you may use your Workbook

### SEC530 Exercise: Architecting for Flow Data

We will now dive into a lab on architecting for flow data. This lab focuses on how to establish flow logging from various sources. Please go to lab workbook section 1.3.

## Course Roadmap

- **Day 1: Defensible Security Architecture**
- Day 2: Network Security Architecture
- Day 3: Network-Centric Application Security Architecture
- Day 4: Data-Centric Application Security Architecture
- Day 5: Zero Trust Architecture
- Day 6: Capstone: Hands-On Defend the Flag Challenge

### DEFENSIBLE SECURITY ARCHITECTURE

1. Course Overview
2. Defensible Security Architecture
3. Traditional Security Architecture Deficiencies
4. Winning Defensible Security Techniques
5. Security Models
6. Threat, Vulnerability, and Data Flow Analysis
7. EXERCISE: Egress Analysis
8. Physical Security
9. Wireless
10. Layer 2 Attacks and Mitigation
11. EXERCISE: Identifying Layer 2 Attacks
12. Private VLANs
13. Switch and Router Best Practices
14. Network Flow
15. EXERCISE: Architecting for Flow Data
16. 530.1 Summary

### Course Roadmap

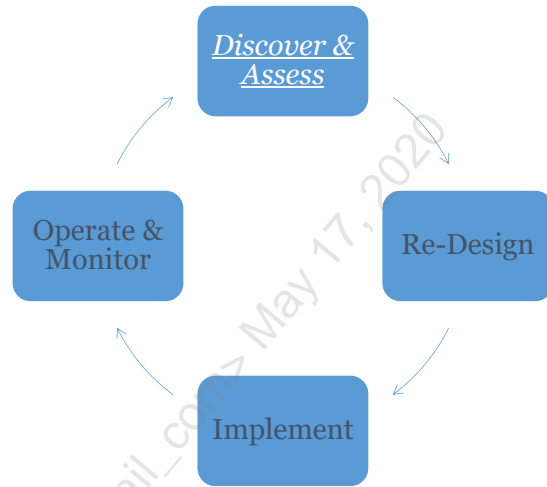
That wraps up 530.1!

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020

Discover & Assess on 530.1



- Physical inspection
- Active and passive discovery of rogue devices
- Unknown and insecure protocols
- Switches and routers configuration
- Identify unused services
- Identify P2P traffic

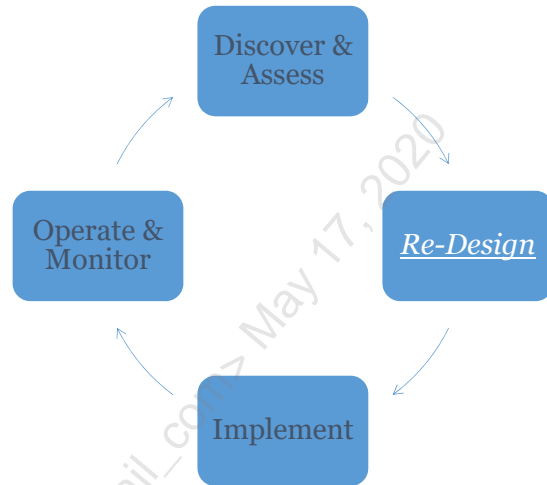


This page intentionally left blank.

## Re-Design on 530.1



- Layer 2 prevention and detection controls
- Supported wireless protocols, according to security settings
- Layer 2 segmentation and authentication according to data classification and flow analysis
- Allow for network monitoring through span ports or taps



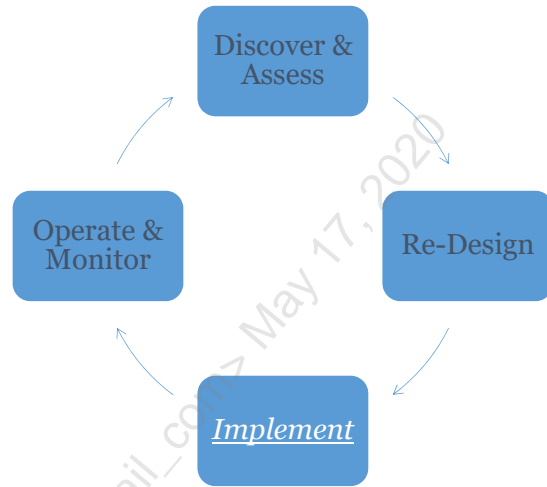
This page intentionally left blank.

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020

## Implement on 530.1



- Robust physical security
- Color-coding and good quality cables
- Disable unused switch ports, and place them on a disabled VLAN
- Use MAC address filtering, 802.1X or NAC
- Use wireless isolation and PVLANS
- Implement VLAN ACLs
- Harden switches/routers against layer 2 attacks
- Disable unused services
- Enable centralized logging
- Use strong passwords

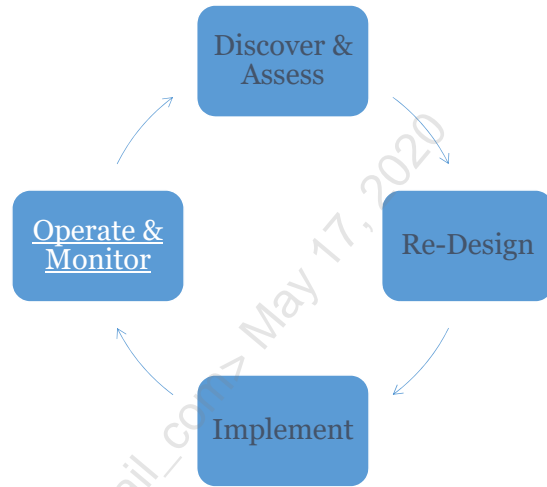


This page intentionally left blank.

## Operate & Monitor on 530.1



- Track all staff, visitors and contractors with access to IT equipment
- Manage switches and routers over secure protocols (SSHv2)
- Monitor layer 2 attacks
- Monitor changes on switches and routers via built-in mechanisms or differential configuration snapshots
- Enable span ports (or use TAPs)



This page intentionally left blank.

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020

## 530.1 Summary

- That wraps up 530.1
- We will continue network security during 530.2
- See you then!

That wraps up 530.1.

We will continue network security during 530.2, covering the following topics:

- Routers
- Securing routing protocols
- Securing NTP and SNMP
- Bogon Filtering, Blackholes and Darknets
- IPv6
- Firewalls
- And more...

See you then!