SEC301 | INTRODUCTION TO CYBER SECURITY
GIAC Information Security Fundamentals (GISF)

301.4

Wireless Security, Network Attacks, & Malware

SANS | GIAC CERTIFICATIONS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

SEC301.4 | Introduction to Cyber Security

SANS

Wireless Security, Network Attacks, & Malware

This page intentionally left blank.

Module 11: Wireless Security & IoT

- Wi-Fi / Wireless Fidelity / 802.11x
- Bluetooth
- Mobile Device Security
- The Internet of Things (IoT)

COURSE ROADMAP

- **Module 11: Wireless Security & IoT**
  - Lab 4.1: Wireless Access Point Configuration
- Module 12: Network Attacks
- Module 13: Malware and Anti-malware
  - Lab 4.2: Anti-malware Scanning

NOTE:

- **We call this device a "Wireless Access Point" or "Access Point".**
- **You are used to calling it a Wireless Router or Router.**
- **It is actually a wireless device, a switch, a router, and possibly many other network functions rolled into one.**

Module 11: Wireless Security

This page intentionally left blank.

SANS

- Wi-Fi Family
- WEP / WPA / WPA2
- SSID Broadcast
- Access Point Authentication
- Wi-Fi Protected Setup (WPS)
- MAC Address Filtering
- WarXing
- Wi-Fi Security and Distance
- Rogue Access Points

Wi-Fi / Wireless Fidelity / 802.11x

This page intentionally left blank.

Wi-Fi 4, 5, and 6 are explained on the next slide…

Wi-Fi Family

- 802.11a (Sep 1999):
  - 5GHz: 54Mbps theoretic throughput
- 802.11b (Sep 1999):
  - 2.4GHz: 11 Mbps theoretic throughput
- 802.11g (June 2003):
  - 2.4GHz: 54Mbps theoretic throughput
- 802.11n (Oct 2009): Wi-Fi 4
  - 5 or 2.4 GHz: 450 to 600Mbps theoretic throughput
- 802.11ac (Jan 7, 2014): Wi-Fi 5
  - 5GHz: 1.3Gbs throughput
- 802.11ax (late 2019- 2020 for widespread availability): Wi-Fi 6
  - Possibly up to 4x throughput—stay tuned

Note: Both the access point and the NIC must support a standard to use it. If the access point is 802.11ac, but the NIC is 802.11n – they will use 802.11n.

Wi-Fi Family

Wi-Fi or Wireless Fidelity is a group of standards put out by the Institute of Electrical and Electronics Engineers (IEEE). Note that this is very different from the protocols we discussed in networking which are open standards that anyone and everyone has input on. Here, the IEEE pretty much says, "This is what we are going to use and how it will work."

The 802.11 family of standards define Wi-Fi and was originally created in 1997, but there were no usable standards until 802.11b was released in 1999 (just days before 802.11a). Since then, calling the growth of Wi-Fi "explosive" would be an understatement. And the growth is accelerating.

Above, you can see the significant versions of the 802.11 Wi-Fi standard. Today, 802.11n and 802.11ac are the most important. 801.11n is going to be around for a while; it takes time for older standards to phase out. (You may still run across an 802.11b access point from time-to-time.) 802.11ac is fully supported by all major access point makers as well as computer makers (both in the Microsoft PC and Mac worlds).

A new standard, 802.11ax has been announced by the IEEE. You might start finding products on the market anytime in late 2021 that support this new standard, but widespread availability probably won't happen until 2022.

Above, notice the Wi-Fi 4, Wi-Fi 5, and Wi-Fi 6 nomenclature… What is that about? Let's go to the next page to find out.

Wi-Fi's New Names

- In October 2018, a new naming convention for Wi-Fi Standards was announced:
  - 802.11n is now Wi-Fi 4
  - 802.11ac is now Wi-Fi 5
  - 802.11ax is now Wi-Fi 6
  - Intended to eventually lower confusion over the naming of the standards

Wi-Fi's New Names

In October 2018, the Wi-Fi Alliance and IEEE announced a new naming convention for Wi-Fi. As you see on the slide, they traditionally had names such as 802.11n, 802.11ac, etc. The new names and their graphical icons are as follows:

- 802.11n is now Wi-Fi 4
- 802.11ac is now Wi-Fi 5
- 802.11ax is now Wi-Fi 6

We have to assume there will one day be a Wi-Fi 7 and so on. The idea of this change is to eventually make the identification of Wi-Fi Standards less confusing.

Legacy Wi-Fi Encryption: WEP & WPA

- Wireless transmission of data requires security
- WEP & WPA are Legacy Wi-Fi Security Standards (still in use unfortunately):
  - Both can be broken in under an hour
  - Wired Equivalent Privacy (WEP) 1999
  - Wi-Fi Protected Access (WPA) 2003
- Unfortunately, still much too common
  - Some ISP's still issue these to customers
  - They are still found in public Wi-Fi
- Do Not Use WEP or WPA!!!

Legacy Wi-Fi Encryption: WEP & WPA

As soon as you decide to put your data on the airwaves, you should know that security is going to be necessary.

Wi-Fi was originally intended for the home network environment. Nobody foresaw it moving into the enterprise, retail, medical, and so on. With hindsight, we can agree this should have been foreseen, but it wasn't. Therefore, the original security specification, known as WEP, was thought to be good enough for the low-risk home environment.

Unfortunately, Wi-Fi did make the move into the higher-risk environment, and WEP was found to have an implementation flaw. It became possible for attackers to predict your next 40-bit WEP encryption key and decrypt data. To fix this, the IEEE changed the specification to use 128-bit keys. However, it could not fix the fundamental implementation flaw. It was soon realized that the same attack could discover the 128-bit keys in only a slightly longer time frame. (The time frame is measured in minutes.)

Because the flaw that makes this attack possible is so integral to how WEP works, it was not possible to simply fix WEP. It had to be replaced.

While the IEEE went back to the drawing board to design a permanent solution, they also gave us an interim fix called Wi-Fi Protected Access (WPA). It was never adopted as a formal standard but was simply a stopgap Band Aid to try and stop the bleeding until a long-term solution could be found.

One of the limitations of WPA is that because it was a temporary fix, it had to run on WEP-capable hardware. That hardware put a hard ceiling on how good the security could be.

WPA utilized a key exchange protocol called Temporal Key Integrity Protocol (TKIP). The bottom line of TKIP is that each packet encrypts with its own AES key. Although TKIP was solid when WPA was in widespread use, there are now attacks for it. Attacking WPA takes about twice as long as attacking WEP, but you still measure the time in minutes, not hours.

Implement WPA2 as soon as possible. Move to WPA3 when available.

Current Wi-Fi Encryption: WPA2 & WPA3

- **WPA2 or RSN (Robust Secure Network)** (2004):
  - Completely new security specification
  - Supports stronger encryption (AES256)
  - Uses a 4-way handshake for key exchange
- **WPA3 is coming**:
  - Some availability in 2021, but 2022 for wide availability
  - Individualized data encryption
    - Better privacy on public networks
  - Robust Pre-Shared Key Protection
    - Protection against rapid brute force
  - Better IoT security support
    - Easier for devices with no screens
  - 192 Bit DoD approved encryption
    - Higher Security for Government, Defense, and Industrial Applications
- Uncertain – But WPA3 will probably require new hardware

Current Wi-Fi Encryption: WPA2 & WPA3

In 2004, the IEEE released the 802.11i standard that has since become widely known as WPA2 or RSN (Robust Secure Network). If you go to a store today to purchase an access point, you will probably see WPA2 on the package. You might also see 802.11i, though IEEE officially dropped that term. You may also see RSN. It all means the same thing.

The WPA2 specification requires new, more powerful hardware. It is not possible to install and run WPA2 on WEP-capable hardware.

WPA2 uses AES encryption up to the 256-bit key. To date, there are no known attacks against the WPA2 specification. However, in October 2017, a researcher discovered a flaw in how many vendors implemented that specification (known as the Krack attack). The flaw would allow for the decryption, and occasionally the manipulation of data. Most vendors have issued patches that fix this flaw (though that will be slow in coming for Android and Internet of Things (IoT) devices). The Krack attack exploits one of the methods of deploying WPA2 (and the most common way in the home and small office environment) is to use a Pre-Shared Key (PSK). It is possible for an attacker to brute force the PSK because it is a form of password. If you deploy PSK, ensure you have a proper, long PSK with plenty of entropy (unpredictability or randomness). The author recommends a minimum of 20 characters in the PSK. You should also change it periodically.

It is also possible to deploy WPA2 with 802.1 authentication methods. (Note that is 802.one, not 802.eleven.)

One of the most important things you can do to secure your home and work environments is to get rid of any WEP/WPA hardware and upgrade to WPA2 only. Doing so should be a top priority following class. It is incredible that WPA2 has been out for over 14 years, yet you still find way too many WEP installations in both the home and enterprise/retail spaces. Having said that…

On Jan 9, 2018, the Wi-Fi Alliance announced the release of a new Wi-Fi encryption certification to certify devices as compatible with a new IEEE security standard called WPA3. Manufacturers will have to go through a certification process, so you might find some WPA3 certified products in late 2021, but you probably will not see wide-spread support until 2022. Once products are available, you will have to have both a wireless NIC and wireless access point that support the new standard to get the new features.

The specification implements four new main features:

1. "Individualized data encryption" which means that even when you use an open Wi-Fi hotspot in a coffee shop, your data still encrypts to the wireless access point. WPA3 includes Opportunistic Wireless Encryption (OWE) which provides individualized data encryption to users connecting to public open networks. So even at a coffee shop, data is encrypted.
2. To prevent offline password-guessing attacks employed by tools such as coWPAtty and Aircrack-NG, WPA3 will deploy protections against brute force and dictionary attacks, even when users choose pre-shared keys (or shared secrets) that are not as strong as they should be. (This will prevent the Krack attack discussed above).
3. When WPA2 came out in 2004, the Internet of Things (IoT) was not really a thing yet. We now want to connect Amazon Echo, Google Home, smart light bulbs, smart thermostats, and so on. These devices obviously do not have screens. So WPA3 will simplify the process of configuring devices with Device Provisioning Protocol (DPP).
4. For high-security government and military networks, WPA3 will employ a Commercial National Security Algorithm (CNSA) Suite mode.

WPA3 also requires the use of AES encryption, up to 256-bit key, and the use of Elliptical Curve Diffie-Hellman key exchange. This is a very good thing.

As of this writing (March 2021), there is nothing firm saying you must purchase new hardware to implement WPA3. However, products must undergo a lengthy and expensive certification process before they can display the WPA3 logo. That would apply to existing hardware products as well. Most vendors will probably opt to only have new products tested and certified. So it looks like an upgrade to WPA3 will probably require new hardware.

Once WPA3 devices—both access points and clients such as laptops, tablets, and phones—are widely available, you will want to upgrade. There will be distinct security advantages.

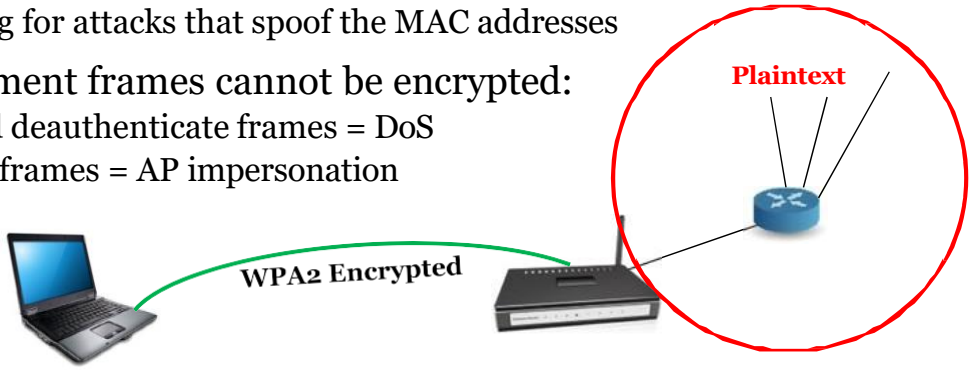
Reference:

https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-cybersecurity-technical-report-wpa3.pdf

Encryption and decryptions can only occur on the devices where the key resides!

Limitations to Wi-Fi Encryption

- The MAC addresses cannot be encrypted:
  - Allowing for attacks that spoof the MAC addresses
- Management frames cannot be encrypted:
  - Spoofed deauthenticate frames = DoS
  - Beacon frames = AP impersonation



- Data encrypts from the wireless client to the wireless access point:
  - Once it reaches the access point, it is unencrypted and sent across the wire

Limitations to Wi-Fi Encryption

While the fact that there is good encryption available in Wi-Fi via WPA2 is a very good thing, it is also a fact that the implementation has some limitations. Please note that these limitations are inevitable. This is not a failing in the implementation, it is simply a fact that certain information cannot be encrypted in order for Wi-Fi to work.

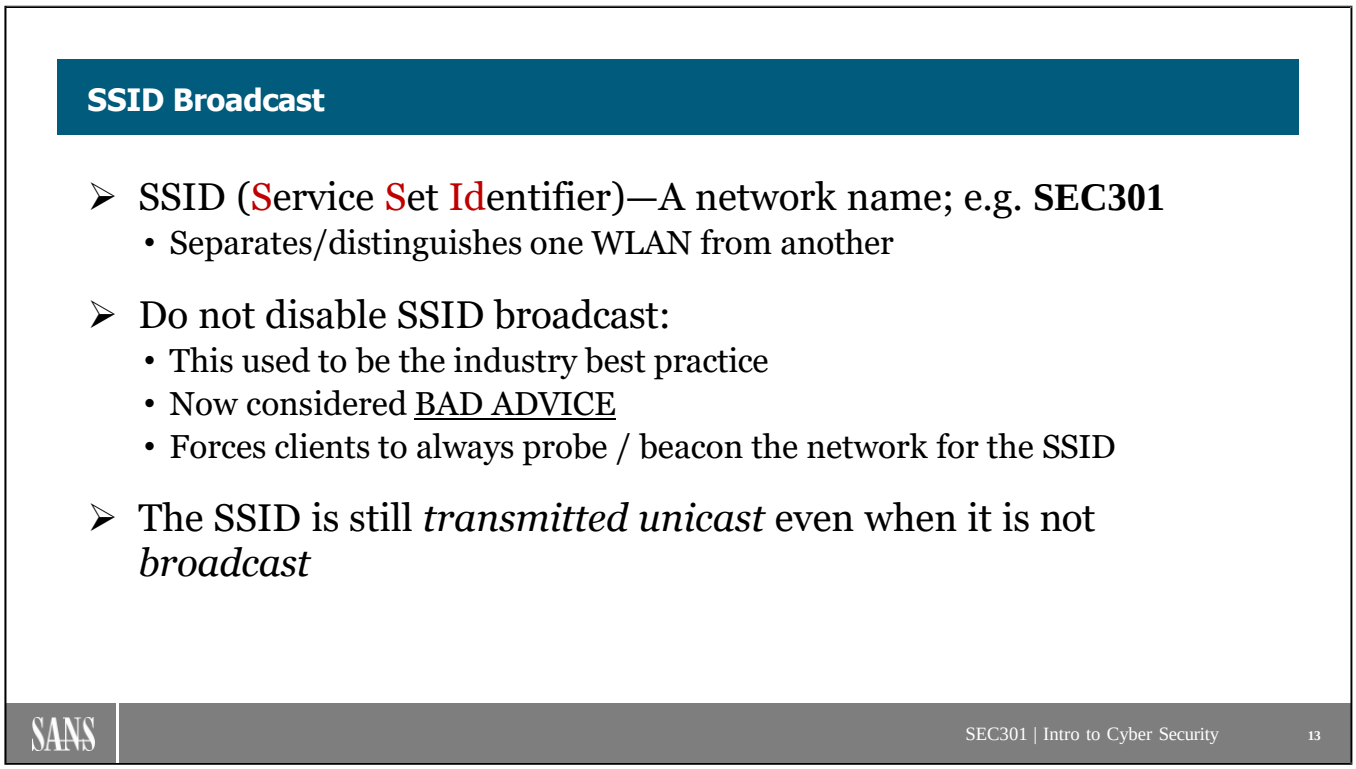
First, the MAC addresses cannot be encrypted. If you did encrypt them, the wireless client (i.e. your laptop or cell phone) and the wireless access point could not tell that the packet is destined for them. Because it is wireless, every system sees every packet of data. It is the MAC address that indicates to the systems which system the packet is destined to.

Think about your SEC301 classroom. You and every other student in the room are connected to a wireless access point in the classroom. When that wireless access point sends a packet of information to your computer, how do all the other student's computers know that the information is not destined to them? The answer is that each of those computers sees the packet and looks at the MAC address. If the MAC address matches the MAC address of that computer's wireless NIC, then the computer processes the packet. If the MAC address does not match, the computer ignores the packet.

Second, for much the same reason, the various management frames cannot be encrypted either. These frames of information are how the wireless environment is managed, hence the name "management frames". Combining the fact that MAC addresses and management

frames cannot be encrypted means that it is trivial to spoof management frames that look like they came from someone else's computer. Take, for example, the deauthenticate frame that a computer sends whenever it wishes to disconnect from an access point. Even when WPA2 encryption is in use, an attacker can see your MAC address in all the packets to and from your computer, and deauthenticate frames are never encrypted. So, an attacker can simply send a plaintext deauthenticate frame spoofing your MAC address and disconnect you from the access point. This is a very simple Denial of Service (DoS) attack.

Third, regardless of the encryption method being used (WEP, WPA, or WPA2), the wireless signal encrypts from your computer to the wireless access point. Once it arrives at the access point, it is decrypted and sent across the wired network in plaintext. So, unless you employ end-to-end encryption such as an IPSec VPN tunnel, anyone looking at traffic on the wired network can see your traffic.



SSID Broadcast

A Service Set IDentifier (SSID) is a network name. On some home access points, there is only one SSID, or sometimes two if there is a "guest network." For example, you might have one access point in your home with two networks. One is called "family" and one is called "family-guest". In this case, you have two separate networks in your home, one for your use and one for the use of guests to your home. You can give guests the access information for "family-guest" and they can access the internet, but they cannot access your internal network. In the example above, "family" and "family-guest" are both SSIDs.

Each SSID can have its own security settings. In the example above, the "family" SSID might use WPA2 encryption, have a very long Pre-Shared Key (PSK), and use a 10.1.1.0 network address. Whereas "family-guest" might also use WPA2 encryption but have a simple PSK and a network address of 192.168.1.0. Note that in implementations as described here, the wireless access point employs firewall technology (almost always stateful inspection) to keep the internal and guest networks separate.

At one time, it was considered an industry best practice to disable SSID broadcast to make your wireless network undiscoverable by attackers. This is now considered BAD ADVICE. When you have SSID broadcast enabled, your access point transmits the SSID every few seconds. This makes it easy for any wireless client (including the attacker's) to discover the SSID of an access point.

However, discovering the SSID of a wireless network when broadcast is disabled is still trivial. When you disable SSID broadcast, the access point does not transmit the SSID *except* when someone connects to the access point. At that time, the SSID must be transmitted on the airwaves and can still be intercepted by anyone within range (yes, the SSID is unicast to a specific MAC address, but it is still transmitted). So, it might take attackers a little longer to discover the SSID, but they can still discover it easily.

Also, when SSID broadcast is disabled, wireless clients must continually beacon for the SSID, meaning they continually transmit queries to see if an SSID they are configured to connect to is present. To use the SSID from the example above, this means that the wireless client (your laptop, cell phone, etc.) continually shouts out, "Hey, family access point—are you there?"

Access Point Authentication

- Pre-Shared Key (PSK) or Shared Secret:
  - Effectively a password shared by all who have access
  - Enter a PSK on the access point
  - Enter the same PSK on the client (i.e., laptop)
  - Recommend minimum 20-character PSK
    - See the Haystack Lab earlier in the course
- Enterprise level authentication:
  - Typically ties into the organization's central authentication system
  - RADIUS, TACACS+, Active Directory, etc.

Access Point Authentication

Once you set up security such as WPA2, there needs to be some method by which you authenticate to a wireless access point. For wireless in the home environment (and in some enterprise environments as well), the most common authentication method is called a "Pre-Shared Key" or PSK. Some devices refer to this as a "Shared Secret." This is a string that you enter in the wireless access point's configuration. When you attempt to connect to the wireless access point for the first time, you enter the same string on your wireless client such as your laptop. If the string on the access point and the string on the client match, you are authenticated. You normally do not have to re-enter the PSK on the client again unless you change the PSK on the access point.

At the enterprise level, access points have the ability to tie into the organization's central authentication system. There may be several options available for this. Any central authentication such as RADIUS, TACACS+, or Active Directory are candidates for enterprise level authentication.

MAC Address Filtering

- Feature available on most Wi-Fi access points
- Only allow preconfigured MAC addresses to connect to the A/P:
  - Easy to manage in a small office
  - Nightmare to manage in a large environment
  - Remember – MAC addresses cannot be encrypted, so defeating this protection is trivial
- Not a certain security measure:
  - Easy to spoof the MAC address

MAC Address Filtering

Another option on some access points is MAC Address Filtering. Meaning that you enter authorized MAC addresses into the access point and only devices with those MAC addresses are allowed to connect.

There are a few things you should understand about this feature:

- Managing MAC Address Filtering in an enterprise environment would be extremely difficult
- It is trivial to change the MAC address on a modern computer
- Meaning if an attacker knows one of your MAC addresses, he can defeat this control easily
- This is effective for home networks; if you want to keep your ***novice*** neighbors out of your network
- Attackers with even a fairly low level of knowledge can defeat the protection

In other words, this can be an effective security measure as long as you understand its limitations.

Wi-Fi Protected Setup (WPS)

- Automated setup of Wi-Fi devices
  - Access point "shares" all the security settings with the client
- PIN Mode
  - You enter a PIN on the client that matches the one on the access point
    - Susceptible to brute force attacks: Disable if possible
- Push-Button Mode
  - You push a button on the access point: The two devices sync
    - Automatically disables once synced or after a period of time (less than 2 minutes)
- Near-Field Communication or USB modes
  - Both very rare

Note: Universal Plug and Play or UPnP is a similar issue.

Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup, or WPS, is a protocol designed for automated setup and synchronization of wireless devices. When you use WPS, the access point shares all of the security settings (including the PSK) with a wireless client. This is extremely simple to use and does not require the user to have any knowledge of security settings or to even know the PSK.

There are three modes of WPS:

- PIN mode has the user enter a PIN on the access point's configuration. Then, when connecting a new wireless client to the network, the user only has to enter this PIN. Since
  the PIN is much shorter and easier to enter than the PSK, this is much simpler to use. Unfortunately, a major security flaw was discovered in 2011 that allows the PIN to be brute forced. It is now a recommendation that you disable PIN mode if the access point allows you to do so.
- Push-Button mode is just what it sounds like. You push a button on the access point that temporarily enables WPS, typically for between 30 seconds and 2 minutes. You then instruct the client device to connect. As soon as the two devices synchronize, the WPS feature disables (it also disables after the time-out period).
- Neither the Near-Field Communication mode (requiring the two devices to be held close to each other) or the USB mode (requiring the use of a USB thumb drive between the devices) is common.

WarXing

- Wardriving/Warwalking/Warparking/ Warsitting/Warflying/Warbiking/etc.
- Free Tools:
  - Mac: NetSpot
  - Windows: NetSpot and inSSIDer
  - Android: Wigle and Wi-Fi Analyzer
  - iPhone: None currently available
  - Linux: Kismet – Completely passive
  - Several tools built into Kali Linux

Fluke AirCheck - $2K

WarXing

Years ago, someone connected a high-gain antenna to their laptop, installed a piece of software called Network Stumbler, and went driving around finding wireless access points. This became known as *Wardriving*. Then someone did it while walking around and it was *Warwalking*. From a parking lot, it is *Warparking*; from a park bench, it is *Warsitting* … you get the idea. For some reason, this is one of those things that apparently needs a new name every time someone does it in a slightly different way.

There is now a great deal of software available for WarXing in whatever method you prefer. You can do it with Windows, Android, Apple iOS products, Linux, and more. Some of this software is extremely good.

Warning: Some of the Android-based Warwalking software reports the GPS coordinates of any access point you find back to the developers. You might not want to use those within your corporate environment. It is possible some iPhone apps do the same. Check the required permissions of any such app carefully.

(**Note:** The Network Stumbler tool mentioned is indeed what was originally used for Wardriving. That tool is now out of date; it has not been updated since 2004.)

Wi-Fi Security and Distance (1)

- Interception: Search on "Wi-Fi Pringles Can" or "Wi-Fi Cantenna":
  - Wire a Pringles Can: Turn it into a directional antenna
  - Called a "Cantenna"
  - Works from more than 3/4 mile
  - Costs about $26 (plus a can of Pringles)

SANS SEC301 | Intro to Cyber Security 19

Wi-Fi Security and Distance (1)

When you build a wireless network, you need to worry about distance. All your wireless clients have to be close enough to the access point to connect.

When you secure a wireless network, *ignore distance*! Do a quick internet search on **Wi-Fi Pringles Can**. You will get more than 1.5 million results: This is a well-known trick!

For around $26 of electronics, you can turn a Pringles (or similar) can into a powerful directional antenna. The typical 150 feet that you have to be from the access point to connect now exceeds three quarter of a mile.

The author of this course has heard of Wi-Fi connections working successfully at ranges from 5 miles up to 55 miles—though those claims fall into the category of rumor. The author cannot substantiate the claims.

But the point remains. When you need to secure a wireless network, the limited distance of the technology should not be part of your consideration.

Instructions to build a Cantenna from a Pringles can are located at:

http://www.makeuseof.com/tag/how-to-make-a-wifi-antenna-out-of-a-pringles-can-nb/

https://www.turnpoint.net/wireless/cantennahowto.html

Wi-Fi Security and Distance (2)

- Addressing the distance problem ... **Use WPA2 / WPA3**
- Conduct a site survey—know where the signal is traveling
- Dial down the power level on the transmitters:
  - Usually only a feature of enterprise-level Wi-Fi access points
    - Called "Transmit Power Control," or TPC
- NOTE: Using directional antennas is often recommended
  - Actually, this is BAD ADVICE
  - Extends the range outside the far side of the building

Wi-Fi Security and Distance (2)

In the enterprise environment, you can address this distance problem in a couple of ways. First, you need to conduct a site survey. Meaning that you employ Wi-Fi scanners (such as those mentioned previously) and determine exactly how far the wireless signal of your devices is traveling. If it is traveling outside of your facility, and it almost certainly will be, then you need to address the issue by deploying WPA2 encryption and strong authentication mechanisms.

You can dial down the power of the antenna or, more specifically, of the transmitter. This keeps the access point from sending its signal as far and therefore makes it harder to intercept from greater distances. The setting you look for to make this adjustment is called the "Transmit Power Control," or TPC.

You will often see recommendations to use directional antennas in order to address the distance problem. This is actually BAD ADVICE. This simply causes the signal to travel farther out the far side of the building, which actually makes the problem even worse.

Note: Changing transmitter strength is usually NOT an option with Wi-Fi access points designed for use in the home environment. This would be an option on enterprise-level equipment only.

Rogue Access Points

- The name given to an unauthorized access point on your network:
  - Find them by "Warwalking" your own network
  - *Forbes* magazine had an access point in it in April 2013
- Also used to describe fake public access points:
  - For example, you connect in a coffee shop
  - There are two access points available:
    - CoffeeShopFree
    - CoffeeShopSuperFast
  - Which will you choose?
  - This is also sometimes called an "evil twin" access point

Mobile users are motivated to use any available Wi-Fi network to avoid using their data plan, saving money.

Rogue Access Points

Another issue to be aware of is the *Rogue Access Point*. The term is actually used in two ways.

First, it describes an unauthorized access point on your network. These are sometimes put in place by your own users, especially if the use of wireless is limited within your organization. These have also been discovered being put in place by outside attackers who gain physical access to office space. Indeed, this can be done as simply as walking into your organization carrying a magazine. In April of 2013, a Microsoft advertisement in *Forbes* magazine had the magazine embed a small wireless access point inside the magazine.

You discover these by Warwalking your own area. Obviously, you need to know how many authorized access points you should find and then identify additional unauthorized access points.

Second, this term also applies to access points set up in areas where public Wi-Fi is available (airports, hotels, coffee shops, and such). People attempt this because if you connect to their access point, they can become a man in the middle, potentially seeing all your data.

Train your users on the need to ensure they connect to the correct access point SSID when connecting in public areas (if they connect at all). When they see two SSIDs, "CoffeShopFree" and "CoffeeShopSuperFast," they need to double-check with the establishment before connecting to either one.

Lab Time

- LAB 4.1: Wireless Access Point Configuration

- Objectives:
  - Access a wireless access point
  - Change the configuration from insecure defaults
  - End with settings meeting industry best practice
    - Gives you a set of instructions you can apply at home to secure your own wireless access point!
  - Estimated completion time: 30 minutes
  - Be sure to read the Tips in this lab
    They explain many of the changes you make

Lab Time

LAB 4.1: Wireless Access Point Configuration

SANS

Introduction
Security
Attacks
Distance and Security

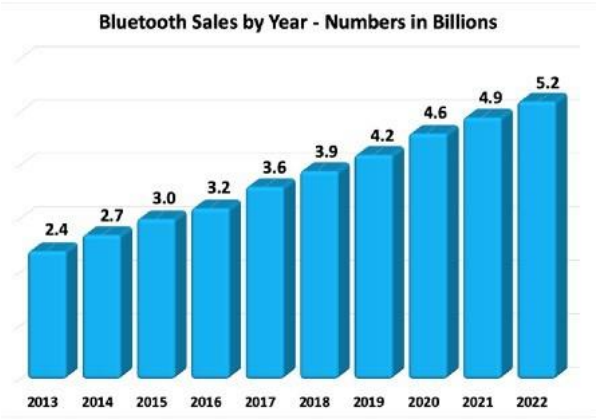
Bluetooth

Bluetooth

This page intentionally left blank**.**

Bluetooth Intro (1)

- Device sales continue to grow
- In part driven by IoT
- It is not going away
- We need to understand it
- So we can secure it!



12% Combined Annual Growth Rate (CAGR)

Bluetooth Intro (1)

According to the Bluetooth SIG at Bluetooth.com, several billion Bluetooth devices per year are sold. The number of devices has been growing at a Combined Annual Growth Rate (CAGR) of around 12%. Extrapolate that out over the next few years and you have their projection of 5.2 billion devices sold in the year 2022. Frankly, given the explosive growth of the Internet of Things (IoT), we think that is a very conservative estimate.

The point of this slide: Bluetooth is here to stay. We will deal with more and more of it as time goes by. Therefore, we need to understand Bluetooth and how to secure it.

Source:

https://www.bluetooth.com/bluetooth-resources/2018-bluetooth-market-update/

Bluetooth Intro (2)

- Cable replacement technology:
  - Anything that can use a cable can use Bluetooth
- Wireless communication:
  - Class 1: 100 mW–100 Meters
  - Class 2: 2.5 mW–10 Meters
  - Class 3: 1 mW–1 Meter
- Often used for cell phone headsets (class 2)
- Can also set up complete networks (Called a piconet)

Bluetooth Intro (2)

The idea behind Bluetooth is straightforward. If you can send it over a cable of any kind, you can send it over Bluetooth. It is, simply put, a cable replacement technology.

There are three classes of Bluetooth: 1, 2, and 3. By far, the most common is Class 2, which has a 10-meter range. This is what you find on your headset and most other Bluetooth devices.

Bluetooth 5 – 2X the speed, 4X the range, 8X the data, but no significant change to security.

Bluetooth Intro (3)

- There are several versions of Bluetooth
  - Our focus is on recent versions (4.1 and later)
  - Specifically, our focus is the security of "Secure Simple Pairing" (SSP)
- NOTE: If you have older versions of Bluetooth devices …
  - Older Bluetooth is far less secure
  - Newer devices revert to the old versions' capabilities when connecting with legacy devices
- Update to the latest devices possible for better security capability

Bluetooth Intro (3)

There are many versions of the Bluetooth specification released through the years. Some improved functionality or capability. Some focused on battery life. Occasionally, there was a focus on security.

The result is that later versions of the Bluetooth specification have far better security features and capabilities than earlier versions. Of course, only more modern gadgets have the newer versions of Bluetooth.

Interestingly, one of Bluetooth's strengths is also a significant security weakness. The strength is that modern devices can connect with and use older legacy devices. For backward compatibility, this is terrific. However, to accommodate this backward compatibility, the new device must revert to using only the capabilities of the older device; including the security capabilities. In other words, if you connect a new device (version 4.2 came out in 2014) to an old 2.0 device from 2004, the new device will revert to version 2.0 capabilities and be far less secure.

One of the most critical security recommendations surrounding Bluetooth is to upgrade to the latest devices you can. Of course, you also have to ensure the new devices support the better security mechanisms (not all do).

Note: Bluetooth 5 came out in December 2016 and is now available in a wide variety of devices. It provides 2 times the speed, 4 times the range, and 8 times the data bandwidth. The specification did not change Bluetooth security.

Secure Simple Pairing

- Introduced in v2.1: Improved significantly in v4.1
- Simplifies the pairing process—while also making it more secure
  - Provides varying levels of device authentication
  - Uses Elliptical Curve Diffie-Hellman (ECDH) for key exchange
  - AES 256-bit encryption
    - All very good—if implemented correctly
  - Provides four "Association Models" (see next slide)

For some "light reading" on Bluetooth: NIST SP 800-121r2, Guide to Bluetooth Security, Released May 2017
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

Secure Simple Pairing

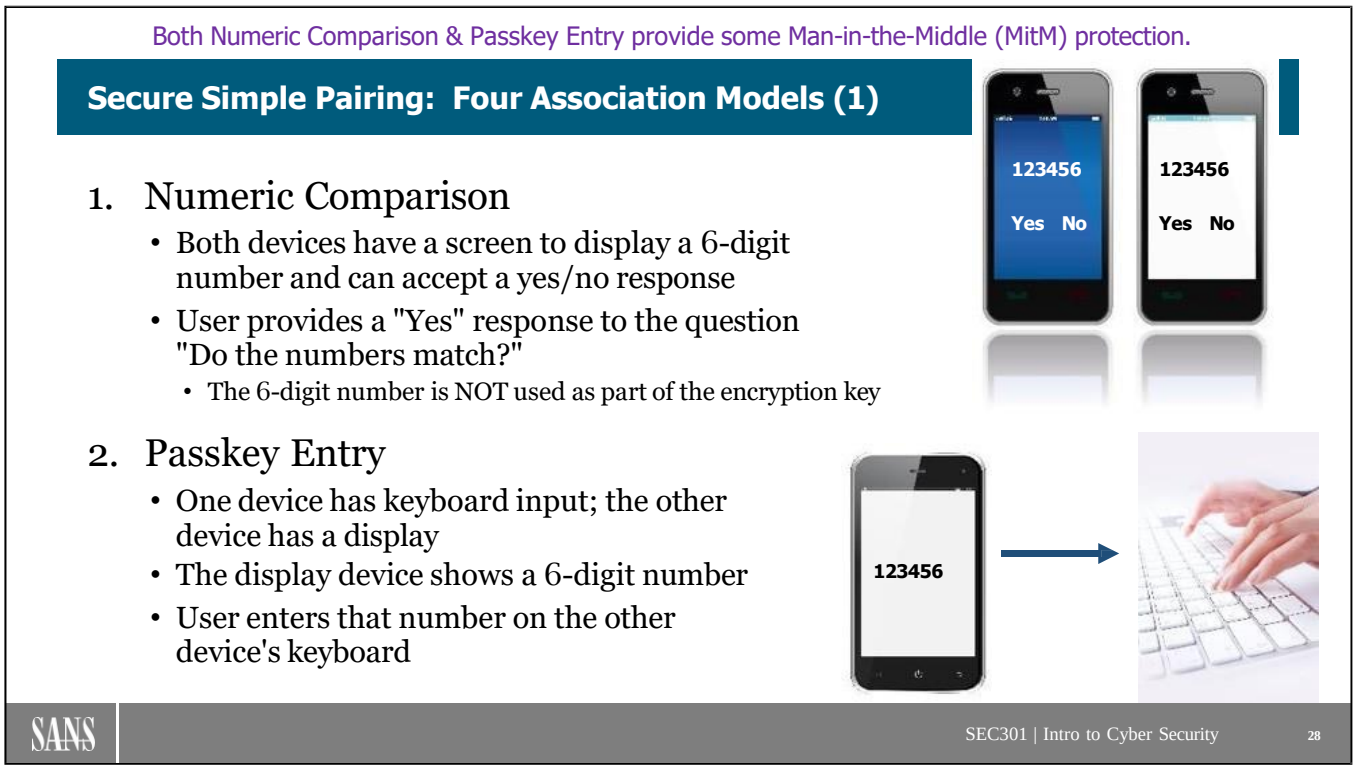
Old Bluetooth used remarkably insecure pairing methods involving PIN numbers. The PIN number was almost always four zeros, and on most devices, you could not change it. This was a significant problem since the encryption key was a combination of the PIN number and MAC address of the initiating device. Meaning that if someone sniffed the MAC address (which can never be encrypted) and "guessed" the 0000 PIN, they knew the encryption key and could "listen in" on your Bluetooth session.

Version 2.1 introduced Secure Simple Pairing (SSP). It was a significant improvement, but it still had issues. Version 4.1 updates SSP and makes it pretty good. SSP not only simplifies the pairing process, but it also makes it more secure. For example, there is the opportunity to prevent Man-in-the-Middle attacks. Note that not all implementations take advantage of these security features, but they are there.

With SSP, there is:

- A level of authentication (sometimes a significant degree)
- Secure key exchange using Elliptic Curve Diffie-Hellman
- AES 256-bit encryption of data

SSP also provides for four "Association Models," which we will look at next.



Secure Simple Pairing – Four Association Models (1)

Secure Simple Pairing supports four Association Models for pairing devices. On this page and the next, we will explain each in turn.

1. **Numeric Comparison**: When both Bluetooth devices can display a 6-digit number, and both have the ability for the user to enter a "yes" or "no" response. When pairing the devices, each device displays a 6-digit number and provides a "Yes" or "No" response capability (e.g., a pair of buttons on a screen). If the numbers match, the user inputs a "Yes" on both devices. The devices then pair with each other. If they do not match, the user enters "No" and pairing fails. Note that unlike older Bluetooth security implementations, this 6-digit number is not part of the cryptographic key generation process. Therefore, even if an attacker obtains the 6-digit number, it provides no insight into the crypto key.

2. **Passkey Entry**: In a situation where one Bluetooth device has an input capability (e.g., a keyboard), and the other device has a display, but no input capability, you cannot use Numeric Comparison (it requires input on both devices). Passkey Entry displays a 6-digit number on the display only device. The user enters this number on the device with the keyboard. If the number entered matches the number displayed, pairing is successful.

Note that both methods provide a level of protection against Man-in-the-Middle (MitM) attacks. This attack occurs when you pair two devices, but an attacker inserts themselves into

the process. You unknowingly pair your device with the attacker's Bluetooth device and perhaps share information with them. With these two Association Models, the attacker does not have prior knowledge of the 6-digit number and therefore cannot insert themselves into the process quickly enough.

Secure Simple Pairing: Four Association Models (2)

3. Just Works
   - When at least one device has neither a display nor a keyboard
   - Devices do authenticate, but not as thoroughly as with Numeric Comparison or Passkey Entry
     - Therefore, provides no MitM protection
   - This is almost certainly the most commonly used model

4. Out of Band (OOB)
   - Uses Near Field Communication (NFC) or wired connection for pairing
   - Should be designed to ensure no MitM or eavesdropping

SANS SEC301 | Intro to Cyber Security 30

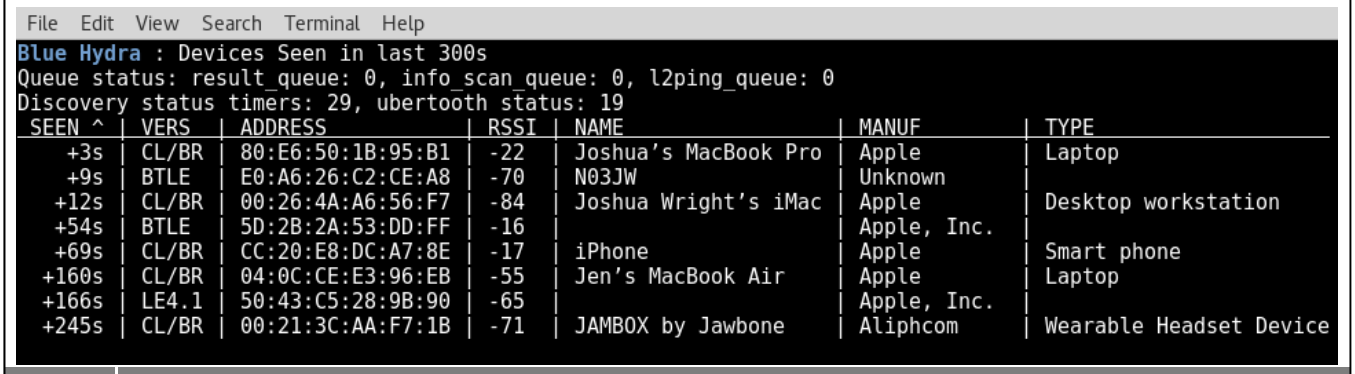
Secure Simple Pairing – Four Association Models (2)

3. **Just Works**: In situations where at least one device you are pairing has neither a display nor a keyboard, you will have to use the Just Works model. It is a very apt name, in that it really does "just work." However, because there is no opportunity to verify the 6-digit number between the devices, the user must accept the connection without being certain it is the legitimate device. In other words, there is a distinct possibility of a MitM attack with Just Works. You should, therefore, only use this pairing method in trusted environments whenever possible.

4. **Out of Band (OOB)**: A small number of devices support the OOB model. Here, both devices must have either Near Field Communication (NFC) capability or be able to connect via a wired connection. With the NFC method, you can simply "tap" the devices together, and they pair. This method must guard against MITM attacks in some way. However, with the limited range of NFC (approximately 4 centimeters), the opportunity for an attacker is fairly limited.

Bluetooth WarXing

- Like Wi-Fi, attackers scan for and enumerate Bluetooth devices
  - Using standard Bluetooth dongles and specialty Bluetooth hacking tools (Ubertooth)
  - Blue Hydra, released at DEF CON 2016



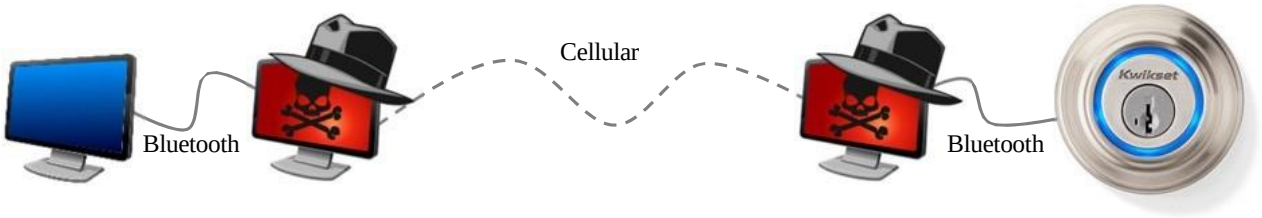
Bluetooth WarXing

Just as with Wi-Fi, there is WarXing with Bluetooth. Using standard dongles and specialty hacking tools such as Ubertooth, locating Bluetooth connection points becomes trivial.

A tool called Blue Hydra was released at DEF CON 2016. This tool continually scans the airwaves to almost instantly detect a Bluetooth device coming in range. As soon as it detects a Bluetooth device, it probes that device to determine the device name, firmware version, Bluetooth version they're running, the manufacturer, and what services the device offers.

Bluetooth Attacks

- Bluetooth relay attacks: Requires two adversaries (or automated devices)
- Bluetooth privacy attacks: Tracking users
- Bugs in Android, iOS, Mac OS, Windows, and Linux allow attackers to execute commands on vulnerable systems



Bluetooth Attacks

Unfortunately, there are attacks in Bluetooth. For example, a Bluetooth relay attack allows for an attacker to effectively proxy the security, meaning that while the Bluetooth signal itself is secured, the attacker has impersonated the device on the distant end. The security negotiation was with the attacker instead of with the device it was intended for, so the attacker can decrypt and read the data. This attack would require two attackers to participate simultaneously.

There are also privacy attacks whereby a Bluetooth can be used to track a device. For example, if you leave Bluetooth enabled on your cell phone, you can potentially be tracked via that signal.

And of course, every operating system that has implemented Bluetooth has had at least one bug that allowed attackers to remotely issue commands in that operating system. Any attack that allows for remote command execution is a serious problem.

Bluetooth Security and Distance

- Interception:
  - Build a "BlueSniper rifle"
  - Intercepts Class 2 from more than a mile

http://www.tomsguide.com/us/how-to-bluesniper-pt1,review-408.html

Bluetooth Security and Distance

Just like with Wi-Fi, when securing Bluetooth, ignore distance. The tomsguide.com website (and several others now) gives instructions on how to build a "BlueSniper Rifle."

The device has been demonstrated to capture Class 2 (with a 10-meter range) from over a mile away.

Bluetooth Recommendations

- Use the latest generation devices and BT versions possible:
  - They are generally more secure:
    - Though that is not a certainty—bad implementations are out there
  - Use v4.1 or later on all devices whenever possible
- ALWAYS pair devices in a safe environment
- If you *must* use a PIN, use the longest and most complex allowed (16 digits)
- Disable Bluetooth if you are not using it

Bluetooth Recommendations

To make Bluetooth both more functional and more secure, upgrade devices whenever possible to the latest versions. Then understand that even with the latest version, there can be insecure operating modes. (The v4.0 "Just Works" mode is a perfect example.)

Always pair devices in a trusted environment. This is especially important if you use older versions of the specification that have not addressed pairing security well.

If you use a Bluetooth device that requires a PIN, use the longest and most complex PIN your device supports. Unfortunately, the PIN is usually limited to 16 characters. Even worse, on some devices, you can enter only numeric characters. If you find yourself with a device that allows only 16-digit numbers for security, you should *really* upgrade the device as soon as possible. If you can't upgrade, do not use that device for any type of sensitive communication.

Of course, the number one recommendation for Bluetooth or anything else: If you are not using it, turn it off.

Mobile Computing (Smartphones)
Camera Proliferation
USB Devices and External Storage

Mobile Device Security

Mobile Device Security

In this section, we discuss:

- Mobile computing (that is, smartphones)
- Camera proliferation
- USB devices and external storage

Smartphone Security (1)

- There's an APP for that! Hacking your smartphone, that is:
  - If a calculator app wants access to your GPS function, your contacts, your calls, your texts, etc., don't install it
  - More difficult if the app actually does require the access:
    - Only get apps from trusted app stores
      - Google Play store, Apple App store
    - Use the app from the developer with the best reputation

- App Testing
  - Google – Fully Automated – takes 24 hours from submission to posting
  - Apple – Done by humans – takes 2 weeks to 2 months from submission to posting

Smartphone Security (1)

There is an app for just about anything, and the vast majority of them are completely innocent and useful. However, some are anything but innocent. In fact, they are in the category of malware (malicious software).

One of the first rules of thumb to follow when securing a smartphone is this: When you install an app for whatever function, look at the permissions required by that app. Does a simple calculator need access to your GPS coordinates, your contacts, your phone calls? If the app needs more permissions than logical, don't install the app. There are dozens more that can do the same thing and don't need the extra permissions.

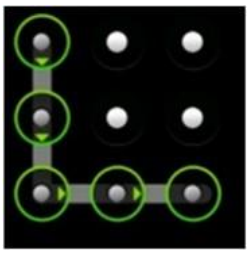
That advice can be hard to follow when you need an app that legitimately does need all those permissions. Now what do you do? We agree; it is tough. The best advice at this point follows:

- Use the most trusted app store you can (Google's Play store, Apples iTunes app store, Microsoft's app store)
- Go with the most reputable app developer you can

All the reputable app stores have ratings on both the apps and the developers.

Smartphone Security (2)

- Most phones allow "screen locks":
  - Often a series of dots that you have to trace your finger over
  - The pattern must be correct to unlock the phone:
    - Watch for screen smudges that reveal the pattern



- Good, strong passwords for smartphones are a must!
  - More than a 4-digit pin: 10-digit minimum
  - 10-digit is much better
    - Device now available to brute force iPhone PIN Numbers
      - 4 digit – average 6.5 minutes
      - 6 digit – average 11.1 minutes
      - 8 digit – average 46 days
      - 10 digit – average 4,629 days

Smartphone Security (2)

Most smartphones and tablets today allow screen locks. Use them! One of the less secure methods is the *finger swipe*. There is a series of dots displayed on your screen and you swipe your finger in a presaved pattern. Two clear problems with this method include the fact that the patterns are easy to "shoulder surf" and the screen tends to get smudged with the pattern.

More and more, phones now allow for PIN numbers and passwords. These are more secure than the finger swipe method, provided you have a good PIN/password and change it from time to time. A 4-digit PIN number isn't strong enough. You should consider an absolute minimum of 8 digits. 10 digits is even better.

Note that a company now has a device that can brute force a pin number due to an undisclosed flaw in the USB port of the iPhone. The source for the unlock times above is: Source: Matthew Green, Johns Hopkins.
https://twitter.com/matthew_d_green/status/985885001542782978

iOS v11.4.1 introduces USB Restricted Mode and enables it by default. While this cannot prevent the brute force attack above, it does limit the window of opportunity.

Smartphone Security (3)

- Several anti-virus apps now available for Android:
  - But they do not typically run "protected"
    - Easier to attack and shut down
    - Still worth using
  - Traditional anti-virus cannot work on iPhone/iPad iOS
- Malware for mobile platforms is increasing:
  - Odds of infection are actually fairly low
  - 1,000 apps for anything, and perhaps only 1 is malware
  - Over 99% of all mobile malware targets the Android operating system

Note: Malwarebytes for iOS & Android is *not* anti-virus. It is a malicious activity blocker.
https://www.malwarebytes.com/ios/ or https://www.malwarebytes.com/android/

Smartphone Security (3)

The anti-malware apps available for smartphones and tablets are increasing. This is a good thing. However, you should understand some limitations of this software.

On a PC, anti-malware (aka antivirus) often runs with special capabilities and permissions. It literally becomes a trusted part of the operating system's kernel. This is good because it makes it more difficult for malware to attack and shut down your anti-malware solution. In tablets and smartphones, anti-malware is just another app. It has no special permissions or capabilities. Other apps can potentially shut it down and evade detection by other means because of this.

The ability to fix this (specifically through Mandatory Access Controls) is now built into the Android operating system. However, that is a recent development, and few if any anti-malware apps are taking advantage of the feature at this point.

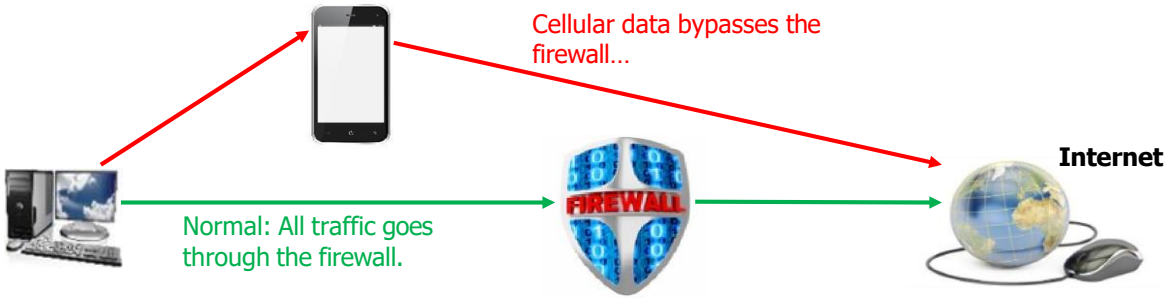
Note that a lot of hype is currently surrounding malware in this space, particularly for the Android platform: Claims of a 3,000% increase in one year and so on. The claim is true, but when you start with a tiny handful of malware at the start of the year, a 3,000% increase actually isn't all that much in raw numbers. We are not saying malware in Android is not a problem; it is. We are saying don't be concerned by every sensational headline you read.

Also, keep in mind the sheer volume of apps makes the likelihood of infection quite low. Per Statista, in March 2017 there were 2.8 million apps in the Google Play store and 2.2 million

apps in the Apple store. When there are 1,000 apps for something, and only 1 of them is malicious, your odds of choosing a safe app are good. However, you should note that per F-Secure, over 99% of all mobile malware targets the Android operating system (which is 8% of all malware, behind 67% targeting Windows):
https://blog.f-secure.com/another-reason-99-percent-of-mobile-malware-targets-androids/

Smartphone Security Bypass

- Phones can bypass perimeter controls:
  - Many phones can now act as Wi-Fi access points
  - Or can tether via USB cable:
    - Both allow a PC direct access to the internet
    - Bypasses company firewalls, IDS, Content filters, and so on



Smartphone Security Bypass

Another huge problem with smartphones in particular: They can act as Wi-Fi access points and "tether" to a PC via USB cable. In either case, your users can now access the internet directly from their corporate PC without going through the organization's security perimeter—meaning phones allow users to bypass firewalls, gateway antivirus, content filters, and so on. This is an extraordinarily difficult thing to prevent and manage. Pretty much, if you allow cell phones into the environment, you allow for this possibility. You can write policy and monitor for it, and then punish employees who violate the policy.

Public Conversations on Phones

A topic for Awareness Training…

- Public conversations on a phone:
  - People discuss things in a public place on a cell phone that they would never otherwise discuss in public
  - And do it on speakerphone!!!
- Awareness training really needs to address this!

SANS SEC301 | Intro to Cyber Security 41

Public Conversations on Phones

It is always amazing the phone conversations you hear in airports, hotel lobbies, restaurants, and so on. People have phone conversations in public places about topics they would never discuss in public otherwise – and they do it on speakerphone!!!

This includes employees discussing sensitive information. One of the worst offenders is the traveling sales force discussing how it plans to go after customers, what it intends to charge, services it plans to offer, and more. Now that some airplanes allow for Wi-Fi-based phone calls, these conversations can even take place at 30,000 feet, where everyone in the cabin of the aircraft will hear each word.

Your awareness program needs to make sure employees are cognizant of their surroundings when making mobile phone calls. Who can overhear the conversation? Is it OK for those people to hear the discussion?

Android and iOS Updates

- Worldwide, Android is about six times more popular than iOS
- Android devices are lax in getting software updates:
  - Handset manufacturers make money on handset sales, not Android updates
  - 2018 – Google changed its contract with handset makers
    - Must install 4 updates the first year, regular updates the second year
    - Only impacts new handsets
- iOS devices have a typical 4+ year support lifetime
  - Unscheduled but regular iOS updates
  - Apple makes money on app store sales, wants to continue supporting devices to continue making money

When selecting a platform, consider the total cost and availability of security fixes

Android and iOS Updates

While Android is globally more common than Apple's iOS, an argument could be made that the iOS update model is more secure. The problem can be summed up simply—Android device makers make money selling devices, not by providing updates to the Android operating system. By contrast, Apple makes money from iPhone sales, but it makes far more from App sales. The more up-to-date the iOS is, the longer it can continue selling apps for the devices. Therefore, iOS updates come out for the iPhone on a more regular basis than what is common on the Android.

The next slide spells the story out in even more graphic detail.

Note: Before purchasing phones by Huawei or Xiaomi, we recommend you look at the information at the following links:

Huawei:

https://money.cnn.com/2018/02/14/technology/huawei-intelligence-chiefs/index.html

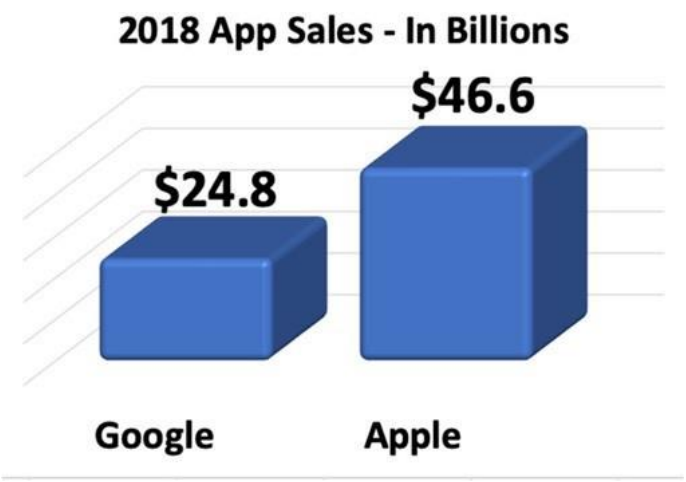
Xiaomi:

https://www.cnbc.com/2018/05/03/xiaomi-will-have-a-hard-time-selling-phones-in-the-us.html

The App Revenue / OS Update Money Trail

- Google & Apple make money on App sales
- Handset makers do not

- Google & Apple test apps on the latest version of the OS
  - Therefore, they know the apps work there
  - And want you using that version



The App Revenue / OS Update Money Trail

Google and Apple make a lot of money from App sales in their respective stores. Both companies test apps on the latest version of the OS so they know the apps will work there. They do not know if apps will work on old versions of the OS. Therefore, both companies have a vested monetary interest in you being on the latest version of their operating system.

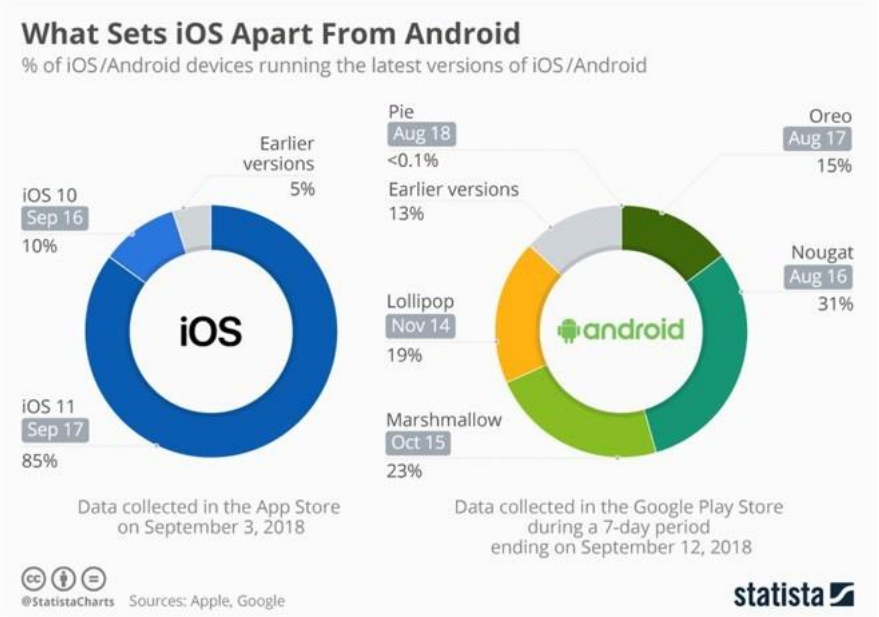
The historic problem for Google is that handset makers make $0.00 on App sales. They, therefore, had no monetary driver to update the OS on their devices. This explains Google's new approach in adding contract language requiring updates for at least two years.

Most current data available as of Aug 12, 2021.

Android and iOS Install Base

95% of iOS devices use a version LESS than 2 years old.

85% are less than 1 year old.



55% of Android devices use a version MORE than 2 years old.

Huge improvement! In Jan 2018, it was 70%.

44

Android and iOS Install Base

The chart above illustrates the issue well.

- Over 55% of Android devices use a version of the Android OS that is MORE than two years old. While that is not good, it is a huge improvement. The same chart from Jan 2018 showed more that 70% of Android devices used a version more than two years old. Going from a bad 70% to a much better 55% in just 9 months is proof that Google's efforts to rectify this problem are working.

- 95% of Apple iOS devices use a version of the iOS that is LESS than two years old. If you look closely, the iOS data is from September 2017 and iOS 11 came out a year earlier, yet 85% of devices had that upgrade.

This chart provided courtesy of Statista under the Creative Commons, Attribution, No Derivatives license.

The original is found at:

https://www.statista.com/chart/5930/adoption-of-ios-and-android-versions/

Huawei Phones (pronounced wah-way)

- There are now phones from the company Huawei
  - They do not use Android or iOS—they use their own operating system
  - FBI, CIA, and NSA recommends against buying these phones
  - The company has "extremely close ties to the Chinese Government"
    - Reading between the lines, it is probably a Chinese Government-backed company
  - With the massive user base in China, India and other countries, these are now the most common phones in the world

The number of both internet and mobile phone users in China is more than twice the total U.S. population.

Huawei Phones (pronounced wawway)

There is another player in the phone market that many people have never heard about. The company is Huawei. This is a Chinese phone maker who makes a phone that, by all reports, is really good. It does not run either Google's Android or Apple's iOS; it has its own operating system.

Based on reports from the U.S. Government, you might want to avoid this phone since the company has "extremely close ties" to the Chinese government. To read between the lines of that statement, it is probably a Chinese government-backed company. Six top intelligence chiefs including the FBI, CIA, NSA and others have strongly recommended that you not purchase these phones.

The phones have become wildly popular in both China and India as well as some other countries. In fact, these phones are now the most popular phones in the world. Meaning this is also the most popular phone operating system as well.

Details on why you might think twice about purchasing a Huawei phone can be found at:
https://www.engadget.com/2018/02/14/fbi-nsa-cia-warn-against-huawei-smartphones/
https://money.cnn.com/2018/02/14/technology/huawei-intelligence-chiefs/index.html

Note: These recommendations are controversial. They give no reason beyond the "close ties to the Chinese Government" as justification.

Camera Proliferation

- Digital cameras are EVERYWHERE:
  - Everyone now has a camera in their pocket
- Trivial to capture data:
  - Simply walk through an office snapping pictures of documents sitting on desks
  - Walk out; data exfiltration made easy

Camera Proliferation

It seems everybody above the age of 5 has a camera in their pocket these days. Cell phones and tablets almost universally have cameras built in to them. Some of these cameras deliver HD quality and a few cameras even include "super zoom" capability. Those last two have led to documented incidents of pictures being taken of someone's credit card from across a store while the victim is standing in the checkout line.

For organizational security, it is a trivial matter for someone who can enter our facilities to capture a lot of information in pictures and carry that information out. Simply walking through to take pictures of physical security designs is bad enough. But remember that data is on printed paper as well. Taking pictures of documents as you walk past a desk is actually simple. And even if you routinely search backpacks and briefcases of employees leaving for the day (rare), you might not have the legal right to search through their cell phone pictures.

Think about this issue and how a "clean desk policy," meaning that all documents must be off the desk and secured in locking drawers at night, might affect it. If documents are left on desks at night, how many dozens or hundreds of pages of information could the janitorial service exit your organization with every night? This can defeat your million-dollar security architecture with a handheld smartphone that costs a few hundred dollars!

USB Devices and External Storage (1)

1TB = 4,481
Pallets of Paper

- Historically, most data was stored inside data centers
- Today, external storage is cheap and plentiful:
  - A 1TB USB HDD = $50
  - A 4TB USB HDD = $99 (Almost 18,000 pallets of paper)
  - The SDXC standard now goes up to 2 terabytes on something slightly larger than a postage stamp (largest available today: 512GB = $174)
  - It is simple to walk out of an organization with a LOT of data

Prices accurate as of Aug. 2018

USB Devices and External Storage (1)

Not that many years ago, most data was stored inside the computer only. Sure, some documents might have been on floppy disks, but the storage capacity on them was so small it was difficult to have much data stored that way. (Not to mention, they were REALLY slow.)

Fast forward to today. External storage is remarkably cheap and plentiful. As of December 2017, an Amazon.com search for **external USB hard drive** returned over 25,000 results. A good quality 1TB (one terabyte) USB hard drive costs $50 and a 4TB is just $99. That 4TB hard drive could hold approximately 2 billion pages of text. With some of the new external Solid-State USB drives, the rate at which you can write data to those drives is incredible. You could write a terabyte to one of those drives in approximately 30 seconds.

You may have a digital camera that uses the SecureDigital SDXC cards. They are slightly bigger than a postage stamp. Those are not just for use in cameras. They can also be used to store data files on a PC. You can't buy an SDXC card this large yet, but the specification allows the storage on those devices to go to 2TB—1 billion pages of text—on a postage stamp—walking out of your organization. That is extremely difficult to detect.

USB Devices and External Storage (2)

- External drives are also an infection vector
- "USB Seeding" is becoming more common:
  - Leaving infected thumb drives in the parking lot for employees to find
  - Thumb drive in the restroom labeled "Salary Data" or "Layoffs"

A simple autorun script for USB or CD:

```
[autorun]
;Open=PlayMe.exe
ShellExecute=PlayMe.exe
UseAutoPlay=1
```

Note: Mac does not support autorun scripts.

USB Devices and External Storage (2)

The proliferation of USB devices has created other problems as well. They are a fantastic infection vector because people plug a stranger's USB thumb drive into their computer without even pausing to think about it. Several methods of infecting a computer come about at that point. One of the most common is called Bad USB, which infects a PC as soon as a malicious thumb drive is plugged in.

This ties directly into USB Seeding. (It goes by many names.) Think about a malicious USB thumb drive left sitting on top of the paper towel dispenser in the restroom. The thumb drive is marked "Corporate Layoffs" or "2018 Salary Info." How many employees would grab that thumb drive, rush back to their desk, and plug it in? As soon as that happens, you have an infection spreading across your corporate network.

References

USB Seeding Links:

http://www.darkreading.com/attacks-breaches/social-engineering-the-usb-way/d/d-id/1128081?

https://www.schneier.com/blog/archives/2006/06/hacking_compute.html

https://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc137730(v=msdn.10)

SANS

What is IoT & IIoT
Growth Statistics
Security Issues with IoT

The Internet of Things (IoT)

Internet of Things (IoT)

In this section, we'll discuss:

- What is IoT and IIoT
- Growth Statistics
- Security Issues with IoT

What Is IoT – An IIoT?

- IoT = Internet of Things
  - Blu-ray players, televisions, game consoles, surveillance cameras, light bulbs, smart speakers (Amazon's Echo, etc.), cars, watches, smart phones, and the list goes on
- IIoT = Industrial Internet of Things
  - Parking meters, gas meters, streetlights, HVAC, physical security systems, traffic management detection, and list goes on
- Most experts predict that IIoT will be many times larger than consumer IoT and "smart home" technology

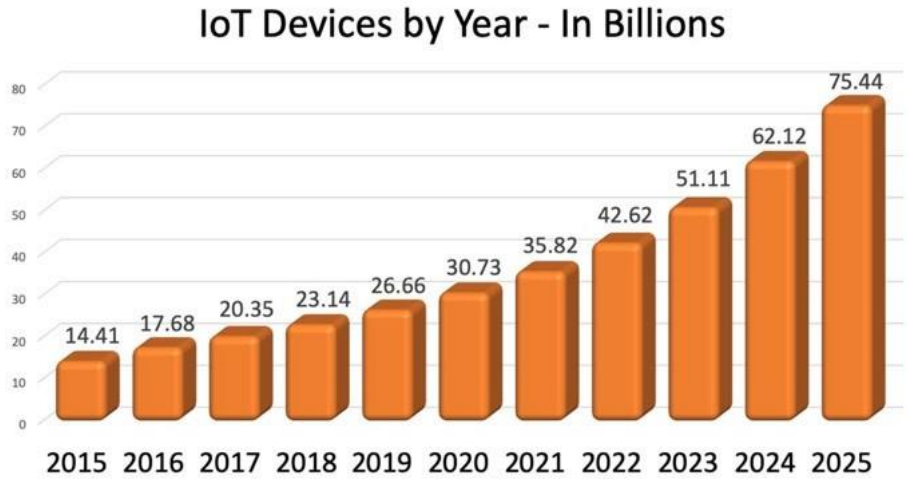
What Is IoT – An IIoT?

To put it simply, any device connected to the internet is part of the Internet of Things or IoT. On the consumer side, this includes a rapidly growing number of devices in our "smart home". We can tell our smart speaker, such as Amazon's Echo, to turn on the lights, close the blinds, open the garage door, turn on the coffee maker, start the garden sprinkler, and a host of other things. We can also check on our pets from our smart phone connecting to a camera inside our home—making both the smart phone and camera part of IoT.

A newer but rapidly growing category is IIoT or Industrial Internet of Things. Municipalities are flocking to this technology to control parking meters, remotely read gas or electric meters, monitor traffic patterns, etc. Companies use it to control Heating Ventilation and Air-conditioning (HVAC), lighting, and other services. Keeping the lights and HVAC off in unoccupied areas saves companies money on utilities and raises profits.

Most of the buzz you hear about on the news centers around the consumer smart home technology, but that will probably be the much smaller category. Most estimates show there will be thousands of times more IIoT devices than IoT devices.

Growth of IoT Devices



- Just as with Bluetooth, the growth of IoT means this is not going away.
- We need to understand it so we can secure it!
- This chart depicts a five-fold increase in five years.

Growth of IoT Devices

Much like with Bluetooth, the growth of IoT devices is pretty astounding. Therefore, it is not going away any time soon and we need to understand it in order to secure it. Note: Much of the Bluetooth growth is driven by IoT growth, since such a high percentage of IoT devices have Bluetooth as well.

Source:

https://www.businessinsider.com/intelligence/bi-intelligence-iot-research-bundle?IR=T&itm_source=businessinsider&itm_medium=content_marketing&itm_campaign=report_teaser&itm_content=learn_more_text&itm_term=bundle_subscription_text_link-internet-of-things-report

IoT (in)Security

Unfortunately…

- IoT Security standards do not yet exist
  - There are some proposals, but nothing formal
- Security testing on devices ranges from extensive to none
  - This includes medical devices such pacemakers and insulin pumps in some cases
  - Too often devices don't have an update or patch capability
    - "I think we will find this to be the biggest security risk of the coming decade"
      -- Doc Blackburn (2021) University of Colorado Denver/SANS Instructor
- All too often, we implement technology before we think it through well!

IoT (in)Security

It is unfortunate but true, there really are no current standards for IoT security. Yes, there are some proposals, but nothing formal. At present, it looks like it may be years before we do have formal standards. The problem is that if you look at the growth statistics on the previous slide, security is being overtaken by events. One simple example: A few years ago a really serious vulnerability was discovered in the Linux operating system shell Bash. The name of the vulnerability is "ShellShock". It is estimated that over 80% of IoT devices run Linux and are, therefore, susceptible to the ShellShock vulnerability. Look at the prior slide, figure out how many billions and billions of devices we are talking about, and then come up with a plan to patch the ShellShock vulnerability on all of them. It is a monumental task.

Part of the problem is that too many vendors are trying to rush to market with minimal expenditure. This means that they:

- implement older chipsets (for example, chips with older, less-secure Bluetooth),
- do little or no security testing,
- and, they release the devices with little thought to updating them after the sale.

There are definite exceptions to those statements. Some vendors are doing a very fine job of security. Unfortunately, there is nothing forcing anyone to implement security, and doing so would cost extra.

I have said this for years! "All too often, we implement technology before we think it through well!"

Module 12: Network Attacks

- Attack Theory
- Network Attacks

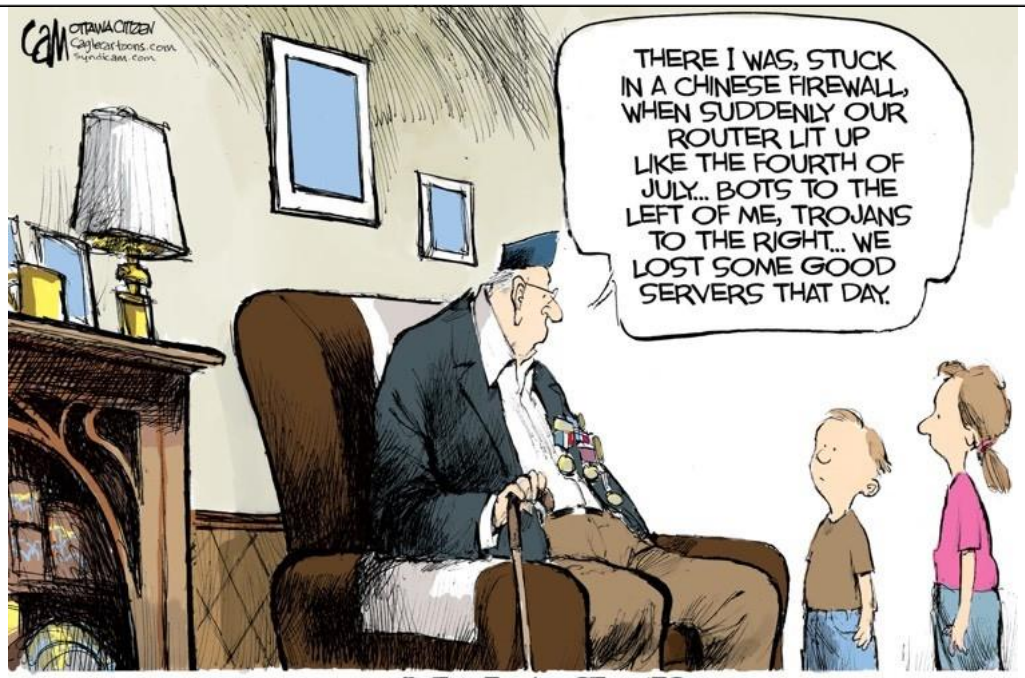
COURSE ROADMAP

- Module 11: Wireless Security & IoT
  - Lab 4.1: Wireless Access Point Configuration
- **Module 12: Network Attacks**
- Module 13: Malware and Anti-malware
  - Lab 4.2: Anti-malware Scanning

Module 12: Network Attacks

We spent the better part of the previous modules talking about terms, concepts, theories, devices, and strategies—all the things that go into building your network infrastructure and your security program. It's time to see how all that theory stands up in the real world by looking at some of the different types of attacks that might be launched against your infrastructure.

We also discuss malware: What it is and some of the ways in which it can be delivered.



Future War Stories

Some students feel there is "a lot of scary content" on this particular day of class. While the author fully understands and appreciates the sentiment, please know that "scaring you" is hardly the intent of this day. Yes, we will talk about many attacks and bad things that can happen on a network and the internet. Please do not let this information intimidate you. We have our foundation in place now to understand the technologies we use to thwart these attacks.

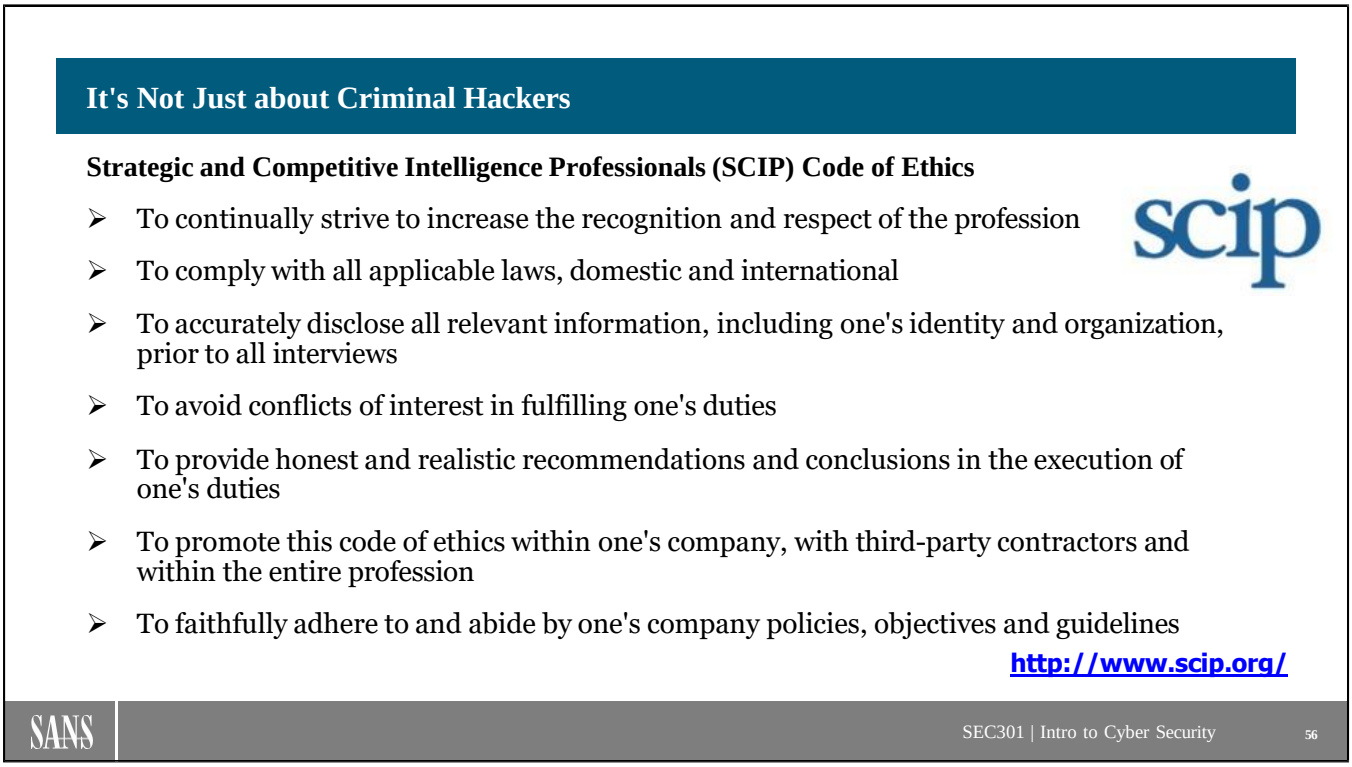
However, are we currently involved in a global cyber war? Yes, we indeed are. Where wars in the past had names like the Korean War, the Vietnam War, etc. This current war might be appropriately named the "Insidious War." The definition of insidious is; "proceeding in a gradual, subtle way, but with harmful effects." That is certainly what is going on now. Like all wars, it is a battle the good guys must win.

Note: The cartoon on this slide has a paid unlimited reproduction license for the SEC301 course books only from the creator of the comic, Daryl Cagle (Cagle Cartoons Inc.) You can find this and his other work at https://politicalcartoons.com.

What Every Attack Has in Common

Every attack (or exploit) ever invented has one thing in common with every other attack ever invented: Every attack takes some thing (or some things) that exists for perfectly valid reasons and misuses it in invalid, malicious ways. Always!

To the security practitioner, this means that we must have a fairly deep understanding of the valid. Then, and only then, do we have any hope of understanding the invalid, malicious misuse. This is exactly why this course spends time on how things like networks and cryptography work—so that you understand and can see the potential for the misuse.



It's Not Just about Criminal Hackers

Far too many companies believe their only threat vector is the criminal hacker (or teenager in their mother's basement). The truth is very different. Businesses of any real size (say 1,000 employees or more) have a department devoted to competitive intelligence. This is a professional specialty geared toward learning as much as possible about your competitors (primarily via open source outlets) to gain competitive advantage.

In fact, there is a professional organization devoted to helping strategic intelligence professionals improve their craft. The Strategic and Competitive Intelligence Professionals (SCIP) has its headquarters in San Antonio, TX. In case you were wondering, this is NOT a fringe organization. From the FAQ on the SCIP.org website:

"... membership is approximately 3,000 - from over 60 countries worldwide. There are more than 52 SCIP chapters in the US, and 14 international chapters."

This slide depicts the Strategic and Competitive Intelligence Professionals Code of Ethics. So long as you conduct competitive intelligence following this code of ethics, the activity is considered both ethical and legal.

As a security professional, you want to ensure you are ready to thwart as many of these activities as possible. Rest assured, your competitors are actively engaged in this type of espionage!

Source: http://www.scip.org/?page=CodeofEthics

(**NOTE:** This organization was formerly known as the Society for Competitive Intelligence Professionals—also with the acronym of SCIP.)

This is a "Shampoo Process" – Wash, rinse, repeat.

The 5 Phases of an Attack

1. Reconnaissance
   - Primarily Passive
2. Scanning
   - Active – expand on what was learned in recon
3. Gaining access
   - Take advantage of info learned in steps 1 & 2
   - Almost certainly gives non-privileged access – must elevate to admin/root
4. Maintaining access
5. Covering tracks
   - Phase 5 is necessary for phase 4

➢ Repeat with recon for newly visible systems

The 5 Phases of an Attack

Although attacks come in a variety of sizes and shapes, common phases of a cyber attack appear on this slide. Earlier models sometimes depicted three phases (for example, reconnaissance, attack, and maintaining access). We look at some of the elements of the phases in this module and the next.

1. Reconnaissance involves identifying assets that might be a target for exploitation. Recon is primarily a passive exercise using tools such as Google to research the target organization.

2. Scanning can be used to identify vulnerable assets that are candidates for compromise. The attack moves from passive to active when you begin scanning publicly available IP addresses for open ports. Part of this phase includes enumerating the operating systems of visible computers and the specific software and version running on any open ports.

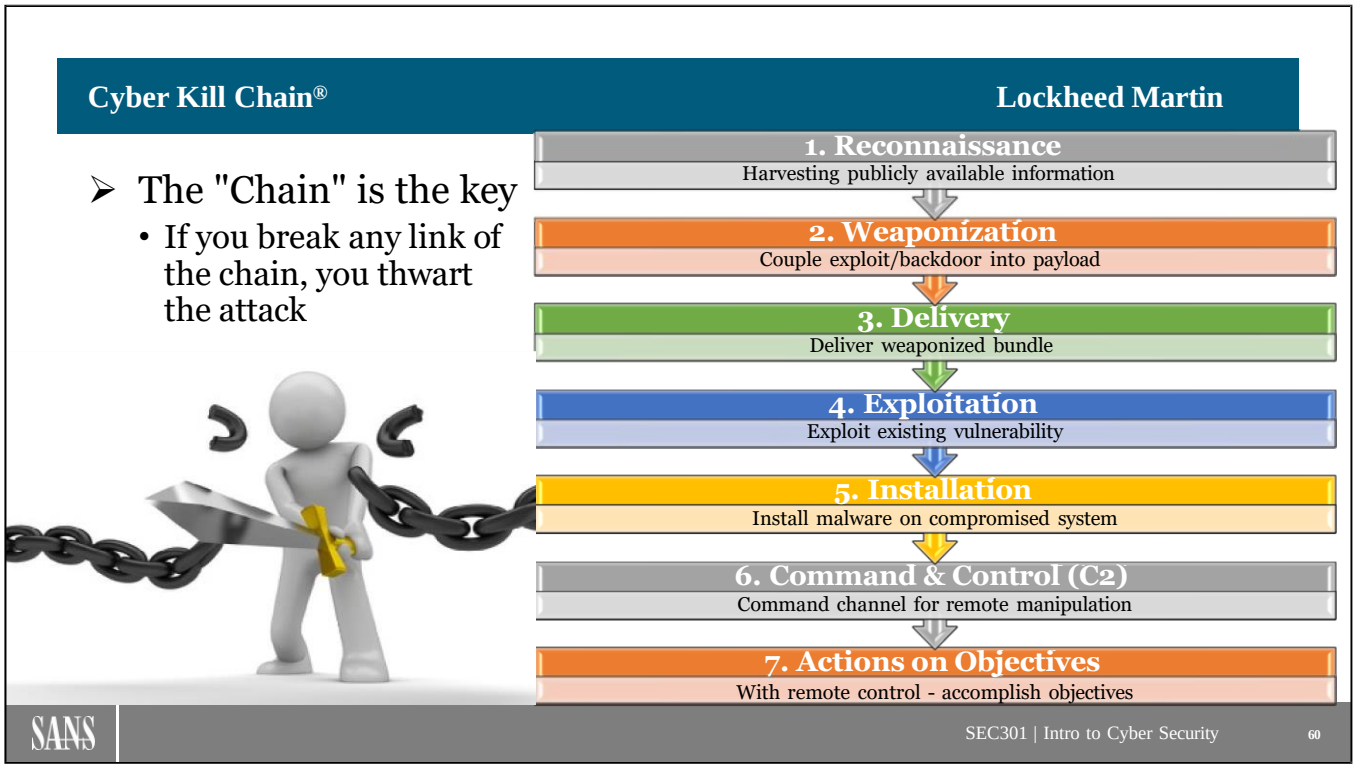
3. Gaining access may be via the network, the operating system, or one of the applications. The information obtained in phases 1 and 2 should provide enough information to find something the attacker can take advantage of. NOTE: There is usually a 3.5 step required as well. In most cases, initial access is to a non-privileged account. To move to the next two phases, the attacker must escalate their privileges to Administrator or Root.

4. Maintaining access involves installing tools that permit the attacker to return undetected. Maintaining access also involves phase 5, covering tracks.

5. Covering tracks refers to those activities undertaken by the attacker to hide (or mask) the activities associated with the compromise. The better they accomplish this phase, the better the attacker can maintain access as described in phase 4.

It is also important to note that this is an iterative process or what some like to call a "shampoo process." If you ever read the instructions on a bottle of shampoo, they say, "wash, rinse, repeat." The example applies here because as soon as you gain access to an organizations system, other systems become visible. Perhaps from the internet, you were only able to observe three public IP addresses. As soon as you gain access to one of those, 20 more become visible to you. Meaning your very next step is to move back to recon, scanning, and so on to repeat the process on the newly visible targets.

Wash, rinse, repeat!



Cyber Kill Chain®

There is another well known and widely referenced "attack model." It comes from Lockheed Martin and is called the Cyber Kill Chain®. The chain shows the typical actions of the attacker:

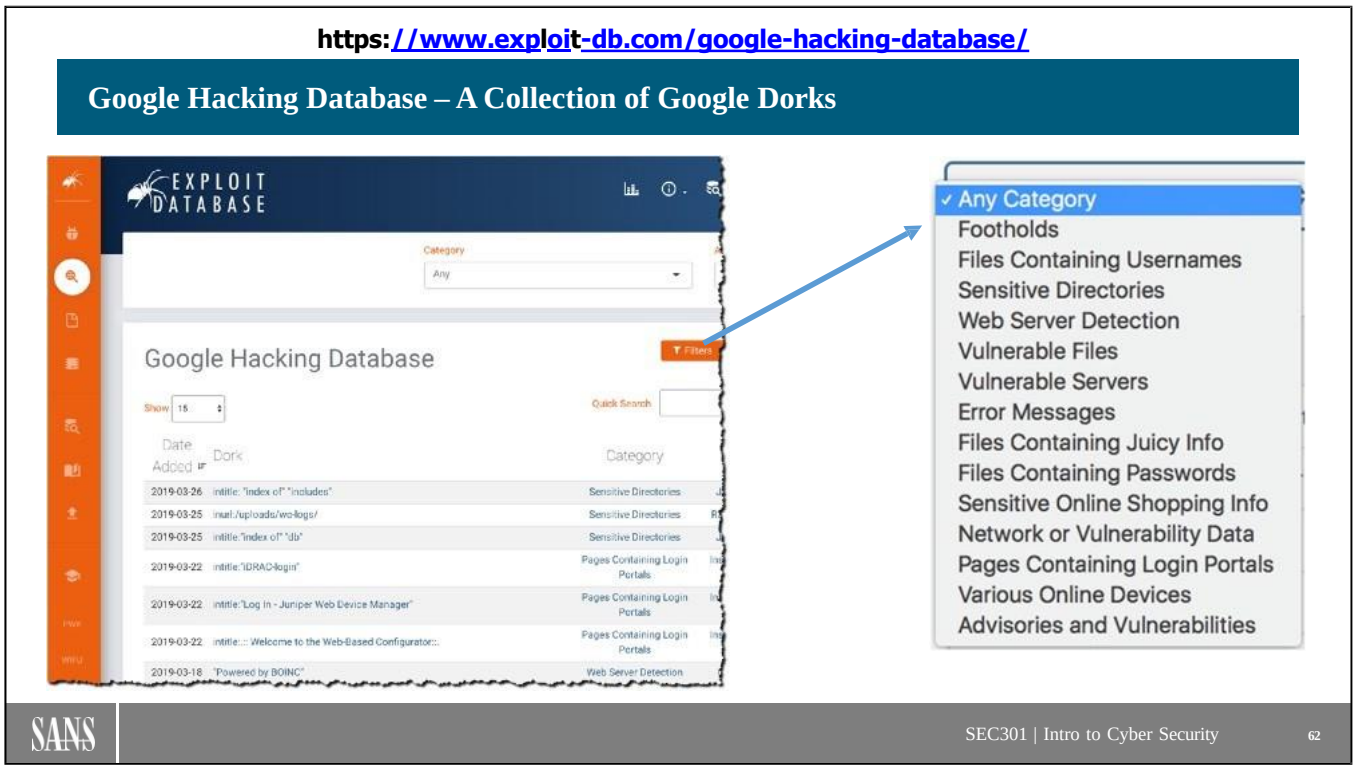
1. Reconnaissance: Harvest publicly available information
2. Weaponization: Couple an exploit/backdoor into a payload
3. Delivery: Deliver the weaponized bundle
4. Exploitation: Exploit an existing vulnerability
5. Installation: Install malware on compromised system (via backdoor placed in prior steps)
6. Command & Control (C2): Establish a Command and Control channel for remote manipulation
7. Actions on Objectives: With C2 "hands on keyboard" access, intruder accomplishes their goals

The most important aspect of the Cyber Kill Chain® is that it is indeed a chain. If you break any link of the chain by disrupting those activities, you thwart the attack. For example, the attacker might make it all the way to step number 5, installation. If you configure your systems in such a way that the attacker cannot perform that step, then the attacker cannot move further along the chain.

Even if the attacker makes it as far as step 6 (Command & Control), if you can prevent them from issuing instructions to the compromised system, then you have still broken the chain. The attacker is unable to do step 7 and Act on their Objectives.

Note: Lockheed Martin granted permission for inclusion of the Cyber Kill Chain® in this course.

https://www.exploit-db.com/google-hacking-database/



Google Hacking Database – A Collection of Google Dorks

Google is a far more powerful tool than many people realize. With advanced search operators, you can search in incredibly powerful ways. With the use of a site operator, you can limit those powerful searches to the potential victim's domain.

(In the example below, do NOT worry about the details, we are simply using a search from this website and adding the "site:" operator to that example.)

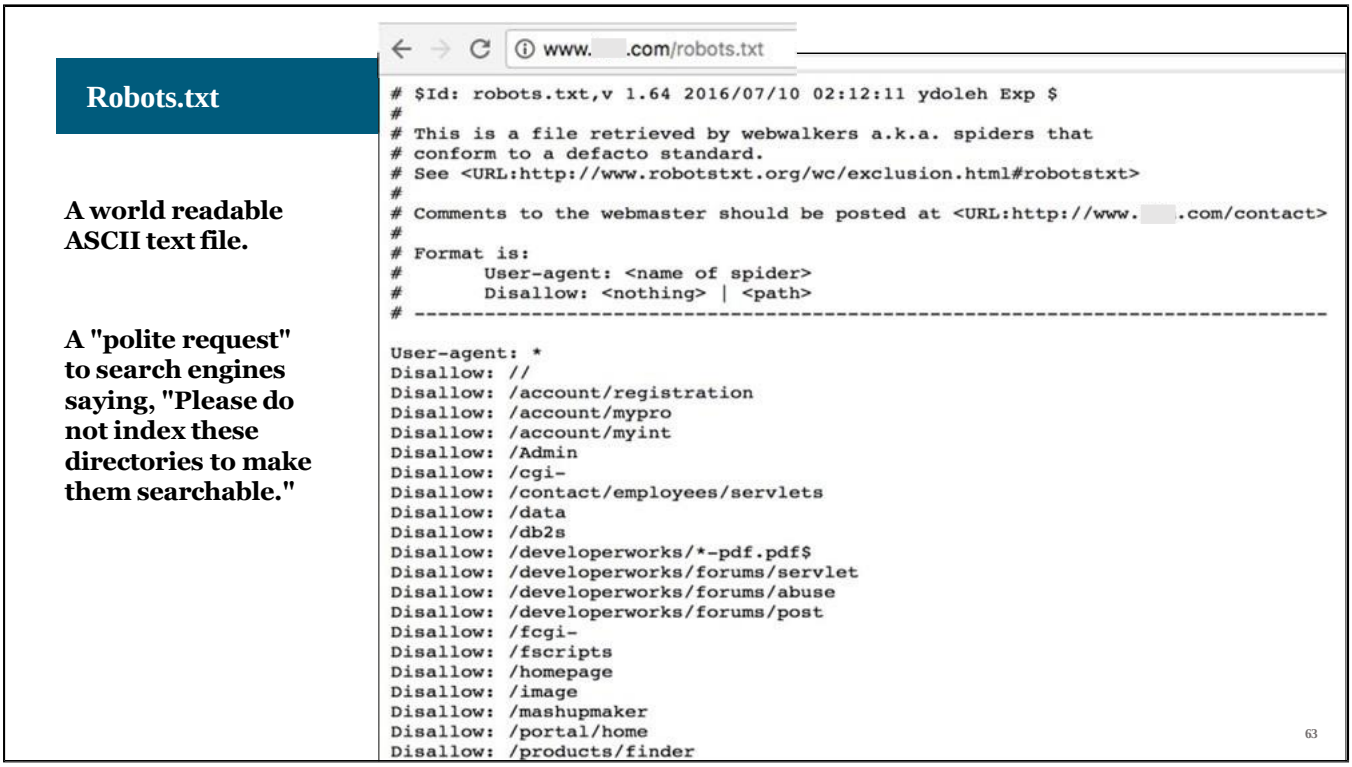
For example, to identify an admin page for websites built with Python Django framework, you would use the following search string (called a Google Dork):

intitle: "Django site admin" inurl:admin -site:stackoverflow.com -site:github.com

To determine if the netip.com domain, in particular, is susceptible, you would add "site:netip.com" to the beginning of the search string. It would now look like this:

site:netip.com intitle:"Django site admin" inurl:admin -site:stackoverflow.com -site:github.com

Hacking Database,maintained by the folks at the company Offensive Security. This is the same company that creates and maintains the Kali Linux penetration testing distribution. They call the search strings maintained at this site "Google Dorks".



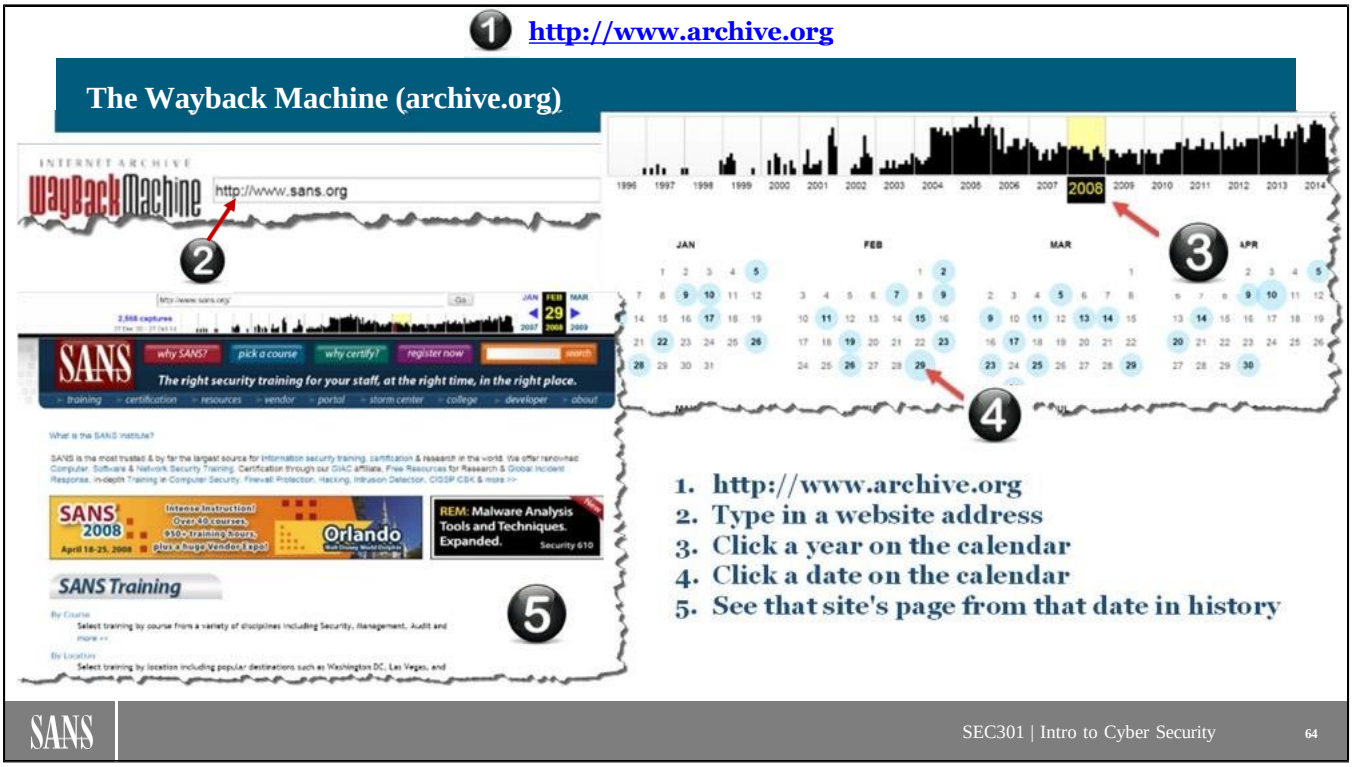
Robots.txt

The robots.txt file is a world readable ASCII text file found on a web server. It constitutes a polite request to search engine spiders used by Google, BING, and others to please not make these directories searchable. It is a polite request that the search engine can choose to ignore. Google and BING both honor the request, but there are a few search engines that ignore it.

To view a robots.txt file, simply enter www.someurl.com/robots.txt as you see in the graphic on the slide (we have hidden the company name as a courtesy. By looking at the robots.txt file above, we see they've disallowed crawling of multiple directories, including the top-level directory.

Please understand that having a robots.txt file on your web server is a good thing. There are directories that you must have on your server and you do not want them indexed. The directory named cgi-bin is a good example of this. However, an attacker might use this to poke and prod in areas that your normal website visitors didn't even know existed. A line like "Disallow: /salesfigures/" might suggest that http://www.company.com/salesfigures/ might be worth a look. Or, looking at the file displayed above, what might be found in /Admin?

Be careful, though—entries in robots.txt may point to directories that, if accessed, set off alarms or may even lock you out of their website entirely. Indeed, attempting to access some of these directories may violate the law in certain jurisdictions.



The Wayback Machine (archive.org)

Many people do not realize it, but much of the internet has been archived on The Wayback Machine. You can see exactly what many sites looked like at any point in time.

1. Simply open a browser and go to http://www.archive.org.
2. In the search box, enter a URL (website address).
3. A sort of calendar shows up. Click on any year back to 1996.
4. Dates on which the site was archived are shaded in blue. Click on one of those dates.
5. That site's exact web page from that date in history will load in your browser.

By comparing pages, you can identify mergers, introductions of new product lines, when projects and products were rolled out, and more. The point here is this: If you have sensitive information on your website, by all means, get it removed. But know that it will still be available via the Wayback Machine. Also remember that your competitor is in the same boat.

You should also know that hackers and penetration testers use the Wayback Machine. If at any point the HTML code on your site contained username/password combinations, they may have been archived. Ensure those passwords have been changed.

Note that any site that requires authentication cannot be archived, but many sites are (such as the SANS website you see above).

http://y2u.be/fHhNWAKw0bY

Dangers of Social Engineering

- The most lucrative attack category, if done correctly
  - Spear phishing is the most lucrative specific attack in this category
- Targets the "weakest link" in security (people)
- May lead to defeating all security mechanisms:
  - Either because attackers gain information on how to defeat them
  - Or because attackers bypass them, receiving the data they need directly from the user

Prevention:

- **User awareness training!**
- **It is far from a perfect solution**
- **But it is the only one**

Dangers of Social Engineering

Social engineering is the most lucrative attack category ever invented. If done well, it will always work. This is because the attacker targets the "weak link" in security: Specifically, you and me. The human being. If the attacker understands human nature well enough and manipulates the victim in the right way, the victim actually becomes happy to help the attacker.

One of the dangers of social engineering is that it can defeat any security measure. Sometimes, it does so because the attacker learns what they need to know to defeat the measure. More commonly, social engineering renders the security measure moot because the victim simply gives the attacker the information they are after.

Now for the bad news. There is no effective defense against social engineering. About the only thing you can do is good awareness training, then more awareness training, and then more and more and more. Even after all that training, a determined and skilled social engineer can succeed.

An excellent video showing examples of social engineering is available here:

http://y2u.be/fHhNWAKw0bY

Categories of Social Engineering

Direct – You hear my voice

- Phone calls (Vishing)
- In-person discussions

Indirect – You cannot hear my voice

- Phishing scams / Spear phishing
  - Whaling: Spear fishing the big fish (CEO)

SANS SEC301 | Intro to Cyber Security 66

Categories of Social Engineering

There are many and varied ways to do social engineering. Generally, though, they fall into two broad categories: Direct and indirect.

1. **Direct social engineering** involves the phone call or in-person meeting. The risk to the social engineer is higher with the in-person meeting, but sometimes the chance of success is higher.

2. **Indirect social engineering** is most commonly done through phishing scams on email. Indirect can also involve pop-ups on websites and other technological ploys to trick an unsuspecting user.

Spear phishing is the most common and most successful specific attack today. For that reason, we take a closer look at spear phishing later in this section.

How It Works

- Often, the attacker assumes a position of trust
- Usually includes "pretexting":
  - Pretext = "A reason given in justification that is not the real reason":
    - This is the help desk, a coworker, the security team, and so on
    - This is your bank, credit card company, PayPal, and so on
- And then causes the victim to ***want*** to take action:
  - And we *need* this information to:
    - Fix your account, do our job: Keep you or them out of trouble
    - Give you money and more

How It Works

Every social engineering attack is different. That is part of why they are so difficult to defend against. We can make some general statements about them, though.

In many cases, the attacker assumes a position of trust and employs pretexting. Examples include: "This is the help desk and your account is broken so I need …" None of which is true of course, but "the help desk" is a position of trust. Your account being broken is a reason given in justification that is not the real reason, which is the definition of pretexting.

These two combined can be a powerful combination when done well. In fact, the most successful social engineer will make the victim *want* to help them. The victim is even happy to do so, thinking they have done exactly the right thing.

This is the most common and most lucrative single attack in the world today!

Spear Phishing

- Highly targeted phishing messages
- Take a scenario:
  - Not Very Nice Person (NVNP) searches you via Google, Facebook, etc.
  - The NVNP learns you work for XYX Corp. in accounting
  - The NVNP sends you an email "From: The Desk of The CEO"
  - The CEO informs you in the email they about to close a massive deal!
  - Transfer $25,000,000 to account XYZ as soon as possible
  - You do so – but the email did not *actually* come from the CEO at all
  - This specific attack has grown by over 350% in the last two years

Spear Phishing

Spear phishing is, by some accounts, the most common and most successful attack today. It is simply a highly targeted phishing email. Typically, the attacker finds out about an interest of the victim through a variety of means (often including social media).

The scenario plays out something like that on the slide. If the targeting is done well, it has a high chance of success. It does not have to target work interests either. If I find out you have an intense interest in classic cars or any other topic, that could be the opening I need.

Social Engineering and Spear Phishing

Social Engineering

- The most common and most lucrative **attack category**
- Used for centuries

Spear Phishing

- The most common and most lucrative **specific attack**
- Used for decades

- Spear phishing is a form of social engineering
  - And accounts for *billions of dollars* per year in personal and corporate losses

Social Engineering and Spear Phishing

This point is commonly misunderstood, so we wanted to give a bit more-detailed explanation between the category of attack versus the specific attack.

Social engineering is the most common and most lucrative attack category and has been for centuries.

Spear Phishing is the most common and most lucrative specific attack and has been for decades.

Spear Phishing is a form of social engineering, and that is part of what continues to drive social engineering as the most common category of attack.

Phishing Stats (1)

- Q2 2017 phishing volume: 47% higher than Q1.
  - It doubled in the financial industry (largest volume ever observed)
- "Secure Phish" emails rose from 1% to 13%
  - The phishing email URL points to an HTTPS site with a valid certificate
- Cloud storage sites will be phished more than financial sites
  - In part due to email addresses being used as usernames
- Over 30,000 Phish Kits are now available
  - Software to create phishing emails
  - More than a third use anti-detection techniques

Two-thirds of all malware infections come in via phishing or spam email.

Phishing Stats (1)

Phishing continues to increase in frequency. Not only does phishing often lead to stolen accounts, but as we will see in the malware module, it leads to two-thirds of all malware infections.

We also see an increase in sophistication of the phishing campaign. For example, the so-called "secure phish" rose from 1% in 2015 to 13% in 2016 and is expected to continue to increase. This is when the URL in the phishing email point to an HTTPS site with a legitimate certificate, making the phishing email appear legitimate as well. Also, there are now over 30,000 "phish kits" available on the internet, many of them free. This is software to craft your phishing emails for you. Over a third of them have anti-detection techniques build in.

There will be an increase in phishing cloud storage sites in conjunction with Ransomware attacks. They will start holding your cloud files for ransom in the future.

The statistics on this page are from phishlabs.com.

Phishing Stats (2)

- Phishing gives results—and gives them quickly!
  - 25% of link clicks happen within 10 minutes
  - 50% in the first hour
  - 90% in the first 24 hours

Thursdays are the most common phishing days.

Gives Business Email Compromise transfers time to go through before someone notices on Monday.

- Five most commonly targeted credentials:
  - Apple account, Microsoft account, Google Drive, USAA, PayPal (77.9% of total)
- Overall, users click on 1 in 20 phishing emails

Phishing Stats (2)

Phishing is such a popular attack vector in that it is successful and quick. As you can see in the slide above, 25% of link clicks happen within 10 minutes of the phishing campaign starting (the median average is 1 hour).

It is interesting to note that financial institutions, while still targeted, are no longer the most targeted. Instead, file sharing sites such as Google Drive, Dropbox, and so on are at the top of the target list. Actually, the most targeted is the Apple account, but attacks on Google Drive return a much higher click rate.

Still today, users click on an average of 1 in 20 phishing emails. Which lures are most successful depends on the scale of the attack. Smaller campaigns (less than 20,000 emails) get a 78% click rate with the "Local postal service" lure. In large-scale campaigns, Google Drive, Adobe accounts, Microsoft accounts, and Dropbox lead the way in click rates (from around 15% down to 2%).

Proofpoint 2017: The Human Factor Report
https://www.proofpoint.com/sites/default/files/pfpt-en-us-human-factor-report-2017.pdf

Vishing

- Phishing via telephone:
  - Example from the San Antonio, TX, Police Department website
  - You receive a call from the county courthouse
  - You missed your jury duty: There is a bench warrant for your arrest
  - Oh! You didn't get the summons? Oh My!
  - We can take care of this: We need your name, SSN, address, and credit card number (for the processing fe e)

HINT: When a warrant is issued for your arrest, they do NOT call ahead.

Vishing

Another form of social engineering that is gaining in popularity is sometimes referred to as *vishing*. It is essentially phishing via telephone. One common vishing scenario that is making its way around the country is listed on the slide.

Another is that you get a call at 3 a.m. after checking into a hotel room. The "girl at the front desk" says there is a problem with your credit card. You either have to give them new credit card information or leave the hotel immediately with the police officers she has waiting with her at the front desk.

Many people have fallen for both of these scams over the last few years.

Social Engineering: Physical

- The techniques can also defeat physical controls:
  - Following someone through a secure door:
    - You see this called both "piggybacking" and "tailgating"
  - Masquerade as a service technician
  - Or a UPS man, or a pizza delivery person

- Shoulder surfing (watching people type their password) can also fall into this category
- Dumpster diving:
  - Dumpster diving is not social engineering; it is a social engineer's gold mine
  - Instead, it provides information to the social engineer

Social Engineering: Physical

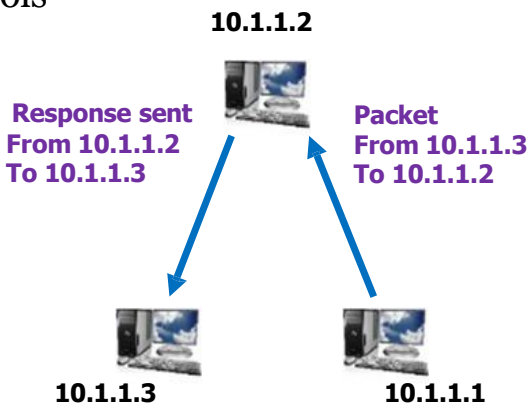
Social engineering will also often defeat physical security. "Tailgating" through a secure door is often extremely easy to do, especially if you appear to belong. Masquerading as service technicians, UPS delivery people, or pizza delivery people, and the list continues.

This often goes back to something we mentioned earlier: Dressing the part. A person in a brown uniform and boxes in their hands is rarely challenged. Plus, people often hold the door open for the busy delivery person.

Dumpster diving is not social engineering; it is a social engineer's gold mine. Successful dumpster diving often yields information valuable to the social engineer. Think about the value of the company phone directory. In his younger days, Keven Mitnick had the name, position, and office phone number of almost all PacBell managers memorized. If someone were to call you and say, "Hi, I work for John Smith, director of marketing. You can call him at 123-7895 to verify that. He wanted me to find out …" You check the company phone book and find that the information provided is indeed accurate.

Spoofing

- Falsifying information with the intent to deceive
- No built-in integrity checks in protocols
- Typical examples:
  - IP address spoofing
  - ARP cache poisoning
  - Email address falsification
  - And many more



Spoofing

Spoofing (as applied to networking and communications) refers to the practice of falsifying information to gain an advantage. In reviewing the characteristics of some of the protocols used in IPv4 (for example, IP, TCP, UDP, ARP, and ICMP), we see that there are no built-in integrity checks within the protocols.

Typical examples of spoofing can include the following:

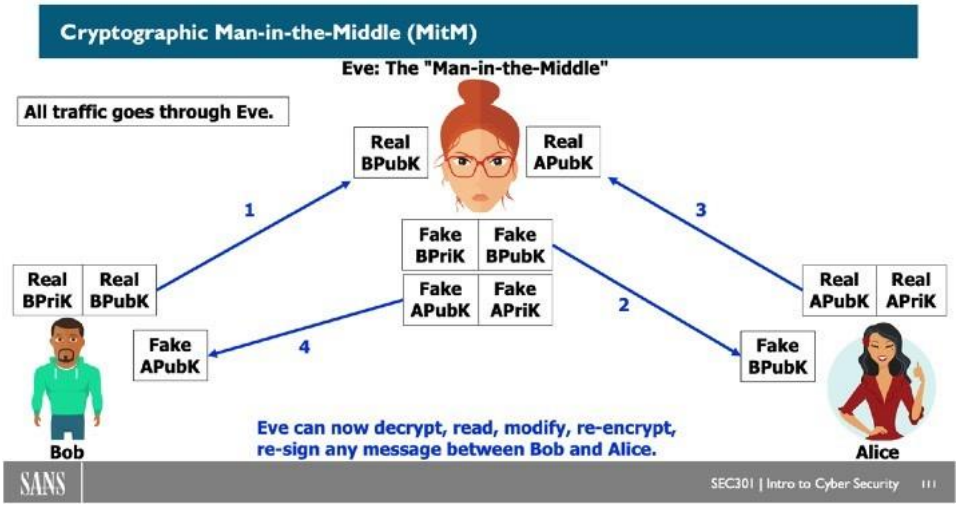
- **IP address spoofing:** A number of tools can be used to craft packets that have a spoofed source address. This is one of the key aspects of an attack such as a SYN flood.
- **ARP cache poisoning:** When an attacker sends unsolicited ARP Reply packets to place incorrect information in an ARP Cache (also called ARP Spoofing).
- **Email address falsification:** It's fairly easy to modify the From: field to make the message appear to have come from someone other than the sender.

The list represents but a few of the many ways information can be falsified with the intent of deceiving.

MitM defense = IPSec VPN Tunnels

The Man-in-the-Middle (MitM)

- A slide from crypto gives an excellent example of Man-in-the-Middle or MitM.
- This happens anytime the attacker has all data packets going through them – They can manipulate the traffic.
- At that point, the only limitation to their capabilities:
  1. Their imagination
  2. Their knowledge



The Man-in-the-Middle (MitM)

Man-in-the-Middle attacks are a favorite ploy of attackers. The condition exists anytime the attacker has all data packets flowing through them (or a point that they control, such as a computer). MitM attacks require eavesdropping on and controlling all communication traffic between two parties. Attackers love MitM because it is an extremely powerful and insidious capability.

Once an attacker establishes a MitM, their capability is limited only by their imagination and their knowledge. If they can think up something malicious and know how to do it, they can do it.

How does an attacker become a Man-in-the-Middle? There are many ways discussed elsewhere in this course, including rogue access points and ARP cache poisoning. There are many other ways as well. For example, if I can take control of a router, I am a Man-in-the-Middle for all traffic flowing through that device. If you think about it, your Internet Service Provider is a Man-in-the-Middle since all of your Internet traffic flows through them (sure they are fine people, but have they been hacked?).

Author's Note: You will occasionally run across the term Monkey-in-the-Middle instead.

While some feel the term Man-in-the-Middle is not the most Politically Correct terminology, it is the industry standard term and will therefore be used throughout this course to avoid confusion

ARP Cache Poisoning (1)

- A method to become a Man-in-the-Middle (MitM)
  - Variety of tools available:
    - ARPToxin, ARPSpyX, ARPMiTM, and Ettercap (the best)

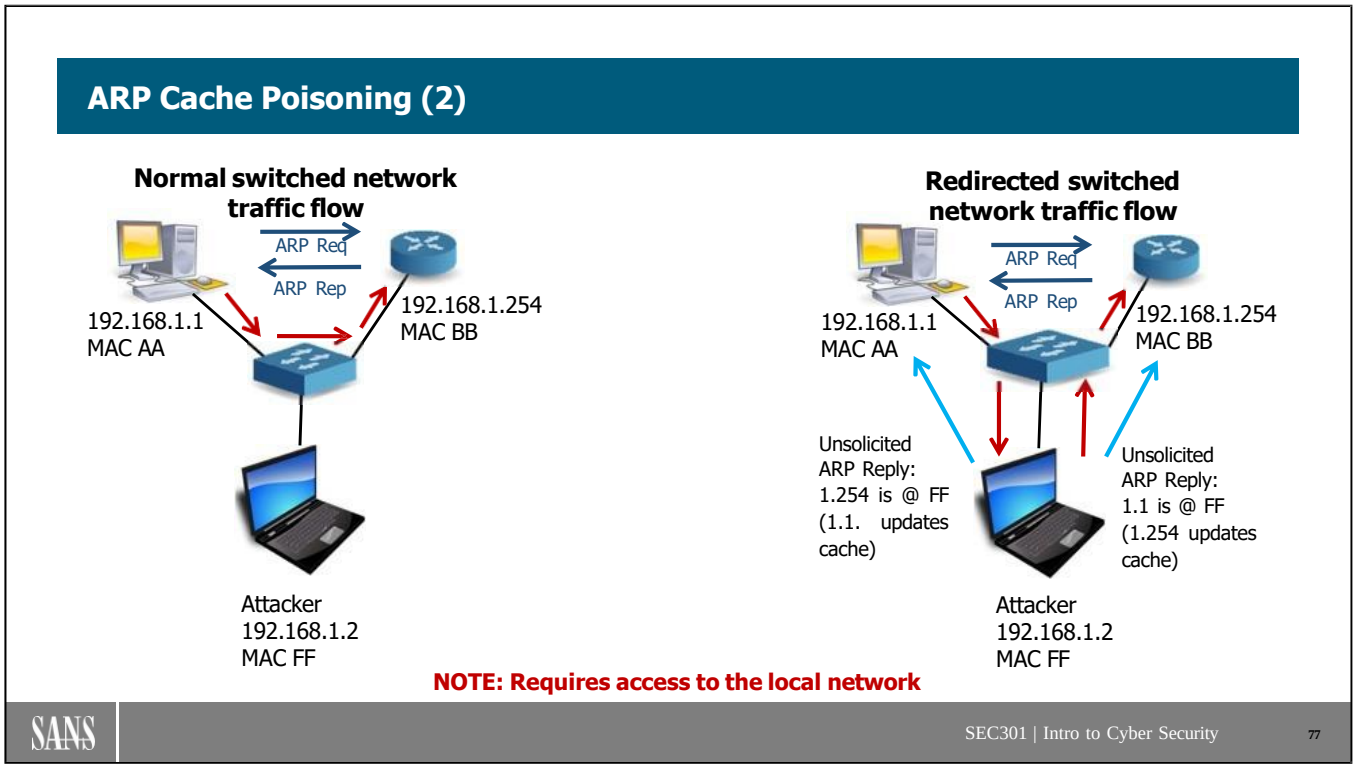
- Send unsolicited ARP replies:
  - Erroneously gives attacker's MAC address as matching the victim's IP addresses
  - Tricks systems into sending their traffic through attacker's machine

Remember: Traffic routes to the IP but physically sends to the MAC.

ARP Cache Poisoning (1)

Now that we understand ARP, we can understand how it can be attacked. Remember that every attack takes some thing or some things that exist for perfectly valid reasons and misuses them in invalid, malicious ways: Always. This attack is a great illustration of that point. It utilizes the "unsolicited ARP reply" which has a valid purpose but misuses it to create a Man-in-the-Middle (MitM) situation. In other words, it redirects all the victim's network traffic through the attacker's computer. When all the traffic flows through the attacker's system, they can manipulate that traffic in any way they desire.

This is an attack that makes more sense when seen graphically, so the next slide contains the illustration.



ARP Cache Poisoning (2)

In the diagram on the left, we see a normal switched network operation. The client PC (192.168.1.1) sends an ARP request to the default gateway (192.168.1.254) and receives a reply. The client PC updates its ARP table and knows that 192.168.1.254 is found at MAC address BB. If traffic is flowing in both directions, the gateway also has its MAC table updated, showing that 192.168.1.1 is at MAC address AA. The traffic flows from the client to the gateway through the switch, exactly as we have been describing. (Do note that the slide abbreviates the MAC addresses in the interest of space. They are normally 6 bytes, instead of the single byte length depicted here.)

In the diagram on the right, we see how an attacker can manipulate the process. The client PC and default gateway have each exchanged ARP requests and replies, so they have each other's IP address and MAC address combinations in their ARP caches.

The attacker at the bottom of the diagram sends an unsolicited ARP reply to the client PC, saying that IP address 192.168.1.254 is at MAC address FF (the MAC of the attacker's computer). The PC updates its ARP cache with this new information. Likewise, the attacker sends an unsolicited ARP reply to the gateway, saying that 192.168.1.1 is found at MAC address FF (again, the MAC of the attacker's computer). The gateway updates its ARP cache with the new information.

When the client PC needs to send a packet outside the network, it creates an Ethernet header containing a destination MAC address of FF. The switch does exactly as it is supposed to do and forwards the packet to that MAC address. The attacker runs software such as Ettercap, which removes the original Ethernet header and replaces it with a new Ethernet header containing a destination MAC address of BB (the gateway) and forwards the packet.

When a response packet comes back into the local network, it arrives at the gateway. That router checks its ARP cache and sees that it does have an entry for 192.168.1.1, which says that system's MAC address is FF. It creates a hardware header containing that destination MAC address, which the switch forwards to the attacker. The attacker's software replaces the Ethernet (or hardware) header with a new one, this time with a destination hardware MAC address of AA (the client PC).

The attacker is now a MitM. All the client PCs (the victim's) traffic flows through the attacker's computer. At that point, there are few limits on what the attacker can do to the victim. At the absolute minimum, the attacker can see all the traffic to and from the victim. The attacker can choose not to forward traffic, creating a Denial-of-Service (DoS), or edit the traffic to change its meaning, or … pretty much anything else the attacker can think of doing. The limit here is the attacker's imagination.

Do note that ARP traffic is limited to the local network, so the ARP cache poisoning attack is also limited to the local network only. In other words, the victim, the gateway, and the attacker all have to be connected to the same switch. They all have to be on the same network.

The lion does not go look for food; she just waits by the watering hole…

Watering Hole Attack

Real-world example…

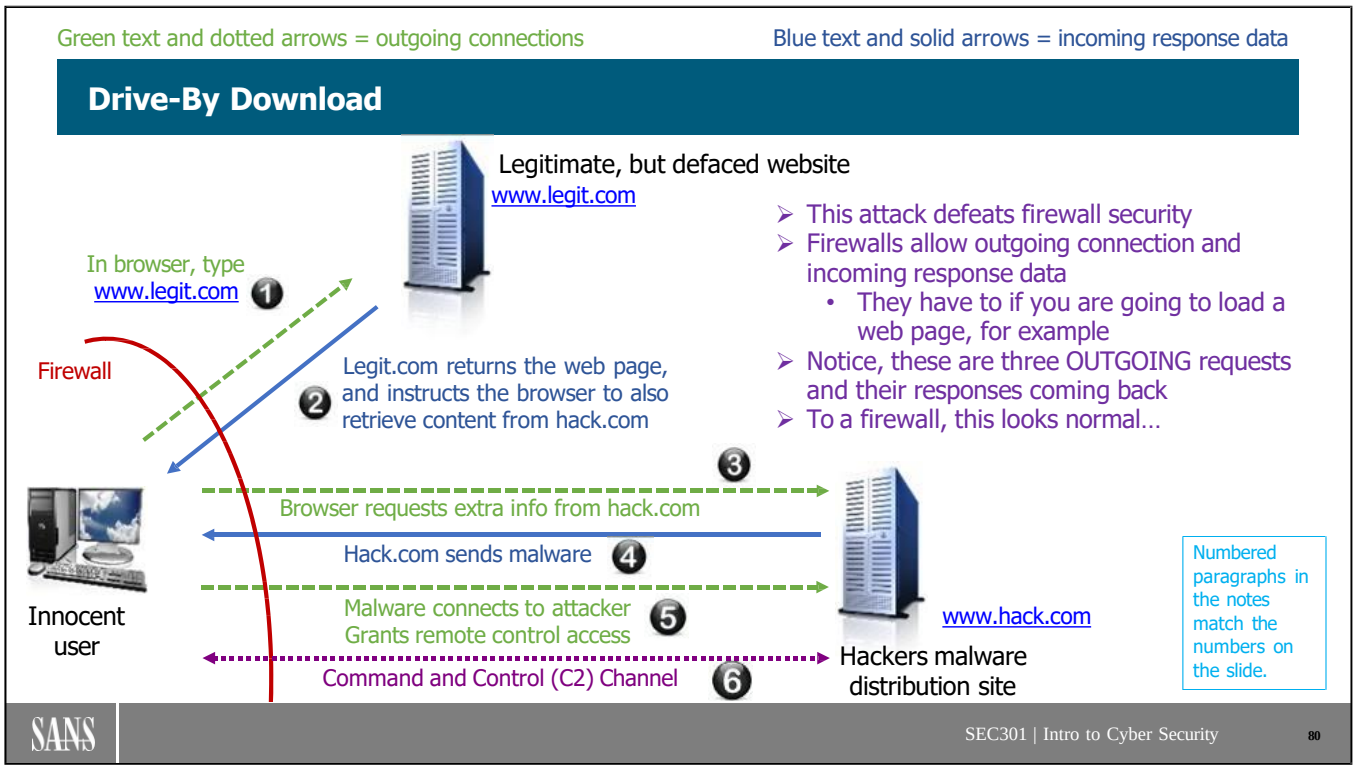
- Attacker learned that executives had lunch at Italian restaurant
  - Info gained from Facebook
- Attacker broke into the restaurant's website
  - Replaced their legitimate PDF menu with a Trojan version
- Executive assistant downloaded the Trojan menu
  - Sent it to the executives
- As each executive opened the menu it installed malware
  - Malware allowed attackers to take remote control of the executive's computer

Watering Hole Attack

There is an attack growing in frequency referred to as a "watering hole attack." These attacks are especially prevalent when the target company does an excellent job of security.

The attacker first researches the target organization using the typical methods of Facebook, Twitter, Google, and others. The attacker learns via research that employees of the target frequent a particular website that is outside the organization's control and therefore not secured by the target organization. The attacker breaks into the external website and plants malware. When the target organization's employees visit the site, their computers become infected. The infection gives the attackers remote control of the employee's computers. The attacker just became an "external insider."

An excellent watering hole at many companies is their job search site. This is the site that prospective employees go to to find positions they might be hired for. It is also the site current employees go to to find out about positions they might get promoted to. Meaning that sooner or later, everyone in the company will visit that site.



Drive-By Download

Another widespread type of attack is called the "Drive-By Download." Essentially, firewalls improved significantly. If you have a modern well-configured firewall, it is remarkably difficult to hack your way through it. Attackers had to change their tactics to continue being successful. Hence, the Drive-By Download, or sometimes referred to as a type of "application level attack", was born.

Before we get to the details of the attack, there is something you have to understand before the attack will make sense. If your computer is behind a firewall and you surf the web, then the firewall MUST allow your computer to send a request for the web page and MUST allow the web server to return that page. In other words, the firewall must allow outgoing requests and allow their responses back in. Also, as you will see in the upcoming web security section, it is completely common for your computer to connect to many different locations on the internet each time you load a webpage. The firewall has to allow all of that communication as well.

The attack begins when an attacker defaces a legitimate website. In days gone by, when someone defaced a site, they changed the words and pictures in an attempt to embarrass the site owner. While that type of attack still happens, it is less common than it once was. Today, attackers are careful not to change the look and feel of the site. Instead, they plant malicious code on the site. When a visitor to the website downloads the webpage, the malicious code will execute on their local computer. There are many possibilities for an attacker once that is in place. Drive-By Downloads are just one favorite possibility.

1. The user types in the URL of a legitimate but defaced website. The browser connects to that web server.

2. The web server downloads the requested webpage. A part of that page is the malicious code placed by the attacker during the defacement. That code indicates to the browser that to load additional components of the webpage, it must connect to another server (in this case, one owned by the attacker).

3. The browser follows the instructions of the downloaded code and connects to the attacker's server. The browser asks for the additional elements needed to create the webpage—not knowing what those elements genuinely are.

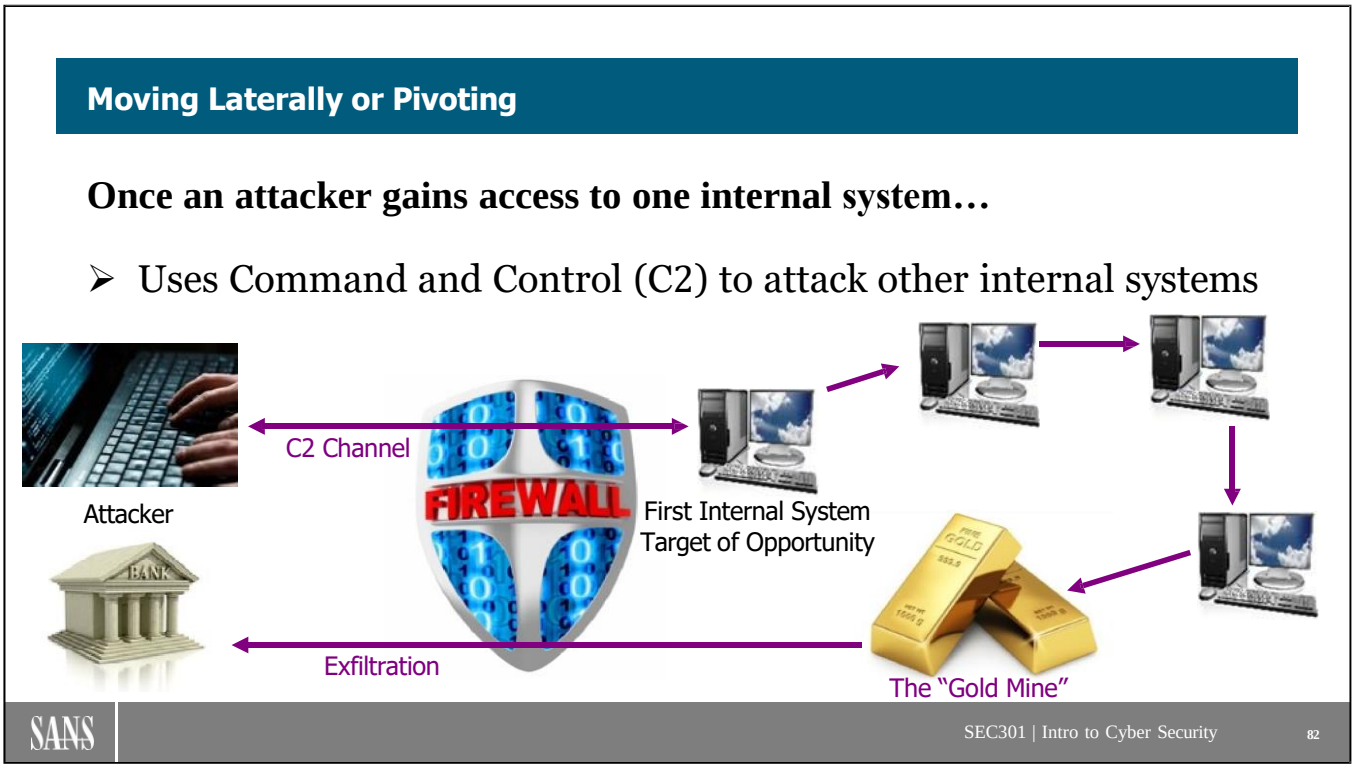
4. The attacker's server downloads malware to the unsuspecting user's computer. The browser executes the code received from the attacker's site, installing the malware.

5. The malware establishes a connection to the attacker and grants them full remote control access to the user's computer.

6. The attacker now has what we call a “Command and Control channel ” or a “C2 channel”. Via the C2 channel, the attacker is able to control the compromised system and instruct it to launch attacks against other systems on its own network.

Because all of the connections are initiated in an outgoing direction (out of the network), the firewall allows them. The instructions and malware from the attacker are in response to requests from the internal user, so the firewall also allows those.

NOTE: As we will learn in the web security section of this course, browsers being directed to download elements of a webpage from multiple internet servers is extremely common. In fact, when you load a typical internet webpage, you will typically connect to anywhere from five to as many as one hundred or more servers.



Moving Laterally or Pivoting

In a report from Carbon Black (reference below), 60% of attacks involve moving laterally or pivoting. It is an easy concept, once you understand what it means.

Most of the time, the initial system compromised by an attacker does not contain the information they are looking for. It was simply a target of opportunity. It was either compromised because it was visible from the internet (a public access system such as a web server or mail server), or it was compromised via a drive-by download, a watering hole attack, or something similar.

Once the attacker has access to that initial computer, other internal systems on that network are now visible. The attacker begins methodically working their way through machines, compromising one after another. In other words, they move laterally through your network – or they pivot from one machine to another.

Each time a system is compromised, the attacker looks to see what they might have just gained access to. Eventually, the attacker exploits the system that contains the "gold mine" of information the attacker was after to begin with. At that point, data exfiltration begins.

Reference:

https://www.carbonblack.com/wp-content/uploads/2021/01/carbon-black-global-threat-report-year-of-the-next-gen-cyberattack-012419.pdf

Island Hopping

- Half of cyberattacks today use the victim primarily for "island hopping"
- This is essentially the same as moving laterally
  - But lateral movement happens inside one organization's network
  - Island hopping occurs between two or more organizations' networks
- Reconnaissance reveals your business partner is PDQ, Inc.
  - They have poorly patched systems the attacker compromises
  - The attacker takes advantage of the trust configured between networks to move to your corporate HQ network

Island Hopping

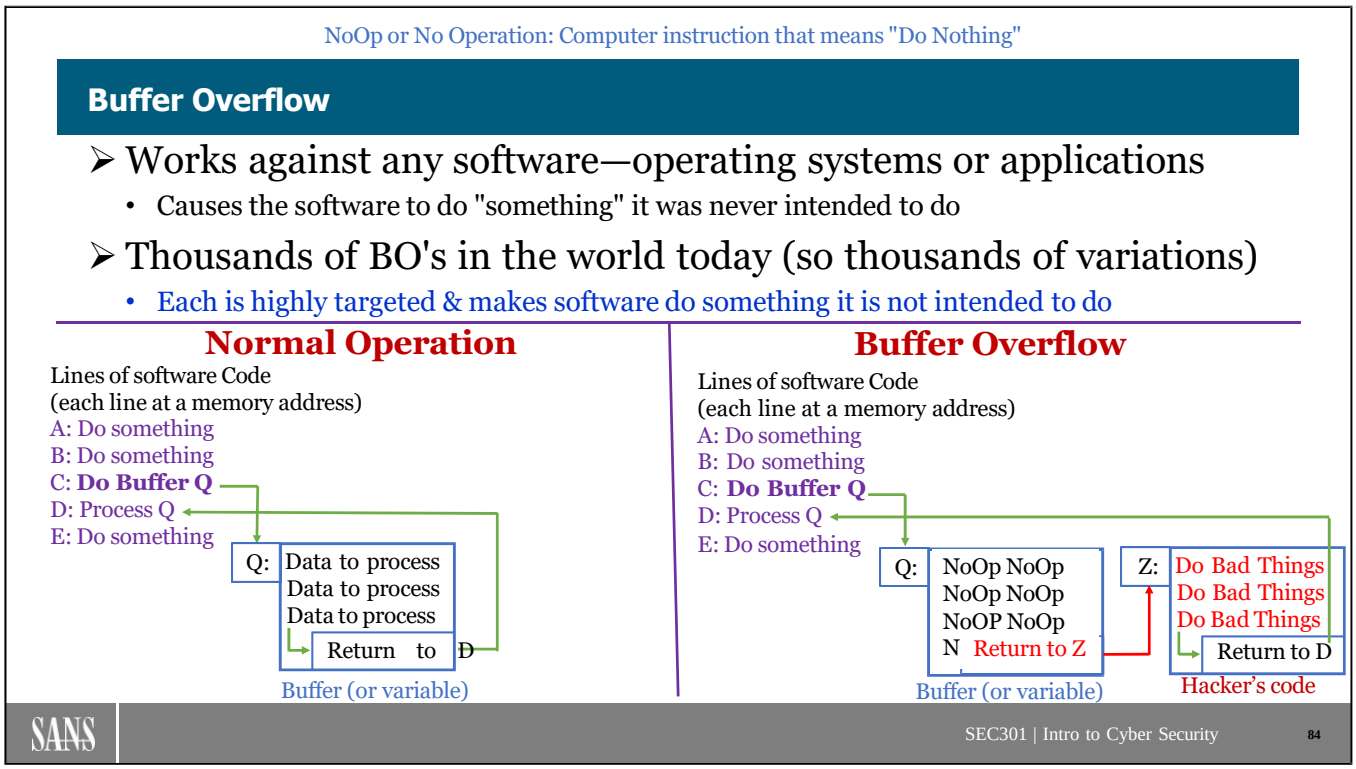
According to the same Carbon Black report referenced on the last slide, "Moving Laterally or Pivoting", about half of cyberattacks today use the victim primarily for "island hopping". This is extremely similar to moving laterally. The difference is the lateral movement happens within a single LAN, for example at corporate headquarters. Island hopping occurs between two or more networks.

For example,

- The attacker cannot find anything to exploit on your corporate headquarters LAN
- Via the first phase of an attack, reconnaissance, they discover you have a business partner
- Scanning that company's network shows unpatched systems
- The attacker compromises one of their systems and moves laterally through their network
- Eventually, the attacker discovers a system on the business partner's network with a trust relationship to a computer on your network
- They then "island hop" from the partner's network to your network
  - Much like an attacker moving within your network, but between two networks

Reference:

https://www.carbonblack.com/wp-content/uploads/2021/01/carbon-black-global-threat-report-year-of-the-next-gen-cyberattack-012419.pdf



Buffer Overflow

Another attack we have been dealing with for many years is called a Buffer Overflow (or often just, BO's). It is possible on any type of software, whether that be an operating system or some sort of application. There are literally thousands of buffer overflow exploits "in the wild", meaning there are also thousands of variations on how they work. This slide depicts the general functionality of buffer overflow exploits in a greatly simplified manner.

All buffer overflows have three things in common:

- They are complex
- They are highly targeted (one that works against version 1.1 of a program may not work against version 1.2 for example)
- They all make a piece of software do something it was never intended to do

To understand BO's, you first have to have a general understanding of how software works when no attack is in progress. First, each line of software code is found at a specific memory address. Memory addresses are pretty long, but in the slide, we will truncate them to A, B, C, and so on. Also, all software must have buffers or variables. These typically hold input from a user that the software will process.

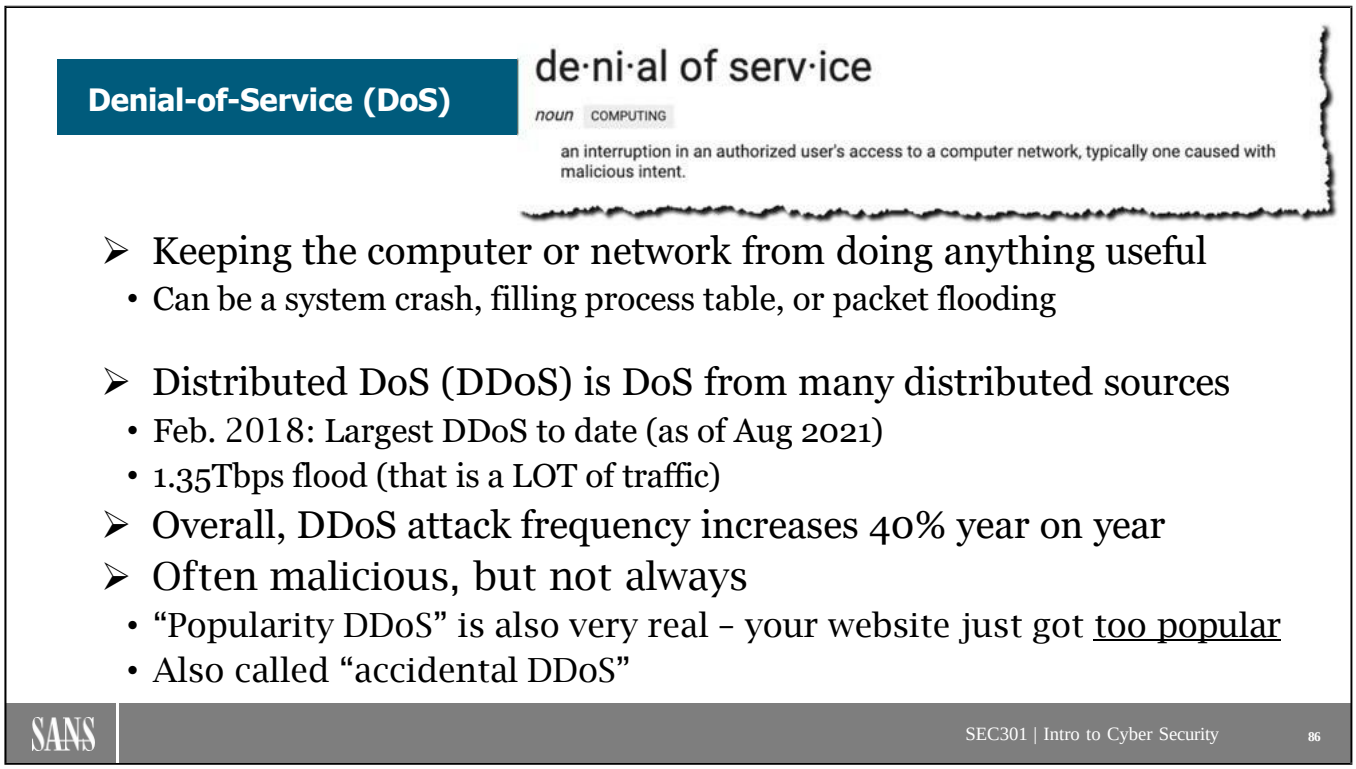
Normal Operation:

On the left side of the slide, you see that the software instruction at memory address C says to process the buffer at memory address Q. The software processes the data and then sees a "return pointer" telling the software to return to the code at Memory address D to process that data and continue. This is all completely normal operation.

Buffer Overflow:

On the right side of the slide, you see the abnormal operation that happens when a buffer overflow is used. Everything begins the same with the line of code at address C processing the information at memory address Q. However, the attacker has filled that buffer full of garbage. (This "garbage" is often a "NoOp sled"—in other words, a number of NoOps in a string. A NoOp is a perfectly valid computer instruction that means, "Do Nothing".) The NoOp sled overwrites the return pointer and replaces it with a new return pointer telling the software, instead of returning to address D, proceed to memory address Z. That is the memory address where we find the hacker code saying to do some sort of bad things. Note that when the attacker overwrote the original return pointer of D, they also copied it and placed it at the end of their malicious code. Now their "Do Bad Things" code executes, then sees return pointer D. This causes the software to return back to the original code and continue processing.

Since the hacker's code also executed, the software was made to do things it was never intended to do. What sort of things? Well, if there are thousands of buffer overflow exploits, then there are also thousands of possibilities—each one is different. As an example, perhaps the hacker code created a new administrator level account with a password the attacker knows, so the attacker can now log into the system with administrator-level privileges. There are many, many other possibilities that the "do bad things" code might have done.



Denial-of-Service (DoS)

Denial-of-service, or DoS, is one of the most common attacks in use today. It works just like it sounds: It denies useful service to a system or network. DoS attacks aim at preventing a computer or network from performing its normal duties. It can take the form of crashing a computer, but more often, it takes the form of flooding the network or computer with millions of information or service requests. The victim computer quickly is overwhelmed and can't handle the load. When this happens, service is denied to legitimate users because they can't seem to get the server's attention. DoS attacks don't need to come from the network, either. A malicious (or just badly programmed) application can begin to spawn new processes over and over until the resources of the machine are exhausted. The approach is different, but the effect is the same: An unusable or crashed system.

DoS attacks are appealing to attackers for a number of reasons. First, they are extremely simple to do. The wide variety of methods for performing a DoS attack is not that difficult to learn or perform; we've seen several examples so far. Second, depending on how you perform the DoS, all you are doing is preventing legitimate traffic from getting to the server. You do not necessarily have to crash the machine or ruin any of the server's resources.

The attacker mentality says that a DoS is no more harmful than driving slowly on the highway or taking your time at the drive-through line at the bank. Tell that to Amazon, where a DDoS attack against the www.amazon.com web site would have cost them $443,132 per minute.

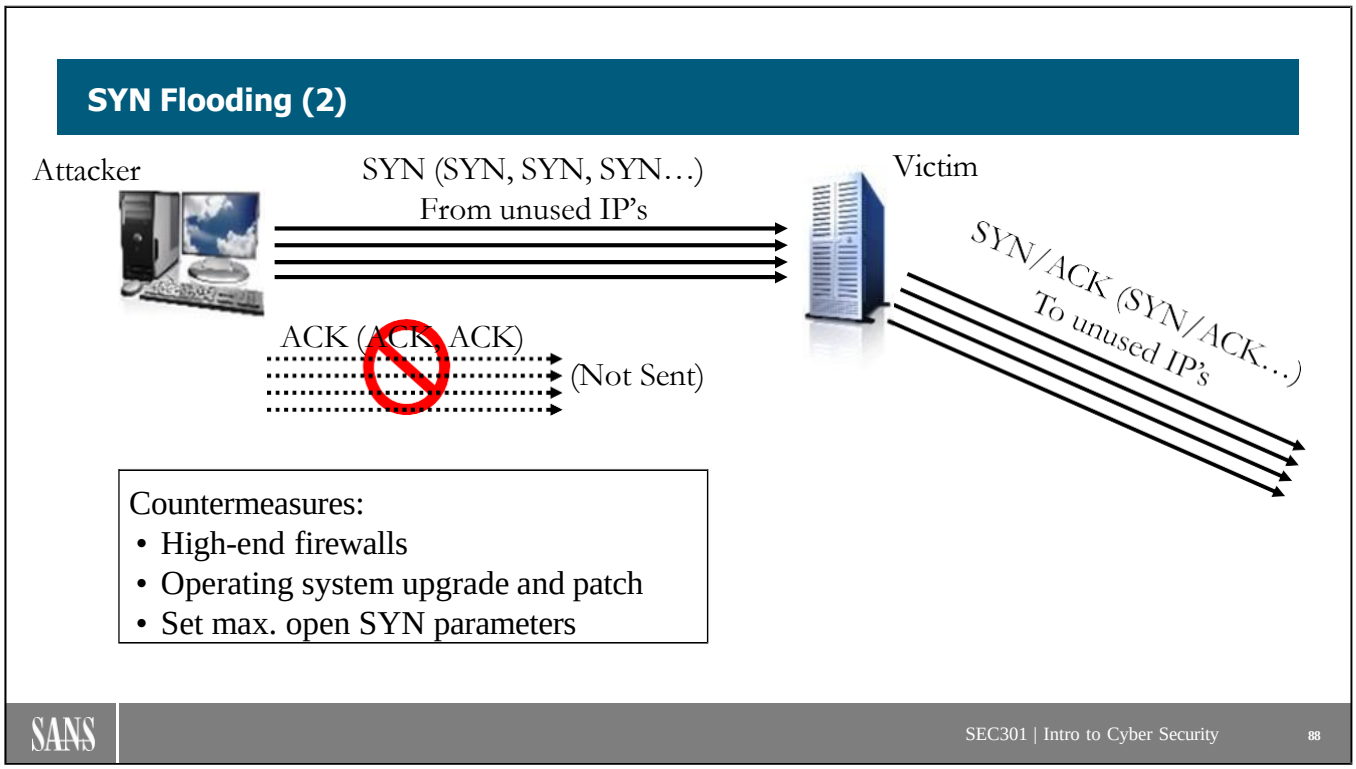
SYN Flooding (1)

- This attack exploits the way TCP connections are made
- Each established connection requires resources to track
- Attacker sends many SYNs but never completes handshake (no final ACK)
- Attacker also spoofs the source address
- Victim uses up all its resources tracking bogus connections

SYN Flooding (1)

Another common attack exploits the three-way handshake that TCP/IP computers use to establish a TCP session. While the three-way handshake is in progress, the server needs some way to keep track of the fact that there is a pending TCP connection. To do this, the server has a "backlog queue" of some number of slots. For example, some Windows versions default to 400 slots in the backlog queue. Note that each open port typically has its own queue.

The SYN Flood attack takes advantage of this and, as you might guess, floods the backlog queue. Exactly how this looks is on the diagram on the following page …



SYN Flooding (2)

This diagram shows how SYN floods actually work in practice. The attacker sends a huge number of SYN packets to the victim. Each of these packets come from unassigned IP addresses (in other words, IP addresses not assigned to any computer in the world). The victim server sends the SYN/ACK to the unused IP address. Because it is an unassigned IP address, no computer ever receives it. Therefore, the third step of the handshake never happens.

Unfortunately, this is a difficult attack to mitigate. There is a "solution" called SYN-Cookies that makes this attack impossible. Unfortunately, SYN-Cookies are so computationally expensive, it is actually easier to DoS a system by crashing it than it is to perform the SYN Flood attack.

High-end firewalls often have the ability to proxy the three-way handshake, which prevents this attack. Unfortunately, those firewalls tend to be quite expensive and out of reach for smaller companies. For companies without the budget for the high-end firewall, the only solution is often to wait the attack out. They will usually leave you alone in an hour or two.

Real-World SYN-Flood Example: Spring 2018

- 12-year-old "developer" put attack code on YouTube channel
- Coordinated with others via the online gaming service "STEAM" and via IRC (Internet Relay Chat) channels
- Generated over 65Mpps (65 million packets per second)
  - Each was a SYN Flood packet
- When a single IP did not gain enough results
  - Started sending traffic to 254 IP addresses simultaneously

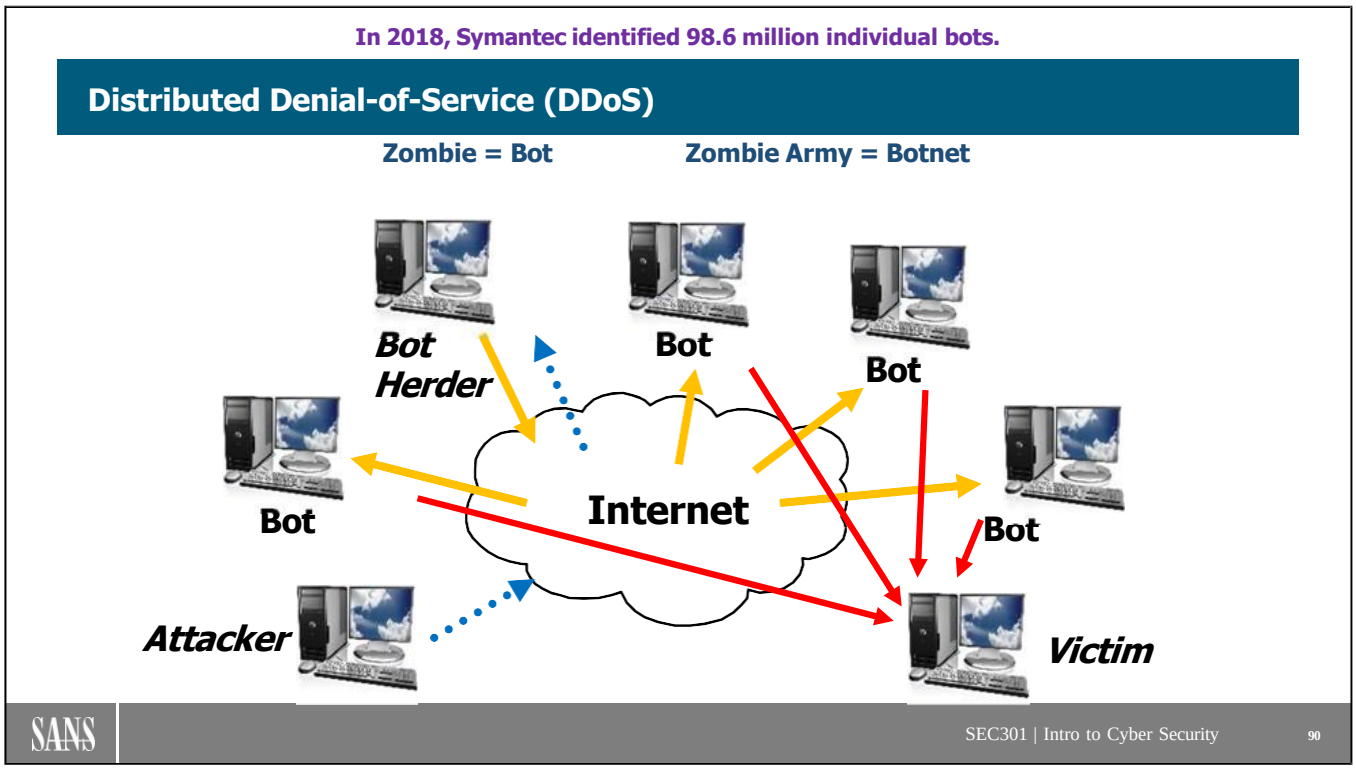
Real-World Example – Spring 2018

An example of a real-world Distributed Denial of Service (DDoS) attack that utilized SYN Flooding occurred in the Spring of 2018. In this case, a 12-year-old "developer" created a tool and shared it via his YouTube channel. Coordination for the attack came through the chat rooms of the online gaming service STEAM, as well as Internet Relay Chat (IRC) rooms. The members of this group managed to create over 65 million SYN Flood packets per second (65Mpps). When that attack against a single IP address was not effective enough, the attackers switched to attacking an entire /24 subnet (meaning they were now sending that traffic to 254 IP addresses).

Note: In this type of attack, knowing the total bandwidth is important (in this case, the bandwidth was 170Gbps—170 gigabits per second—170 billion bits per second). However, often the packets per second measurement is just as important and sometimes more so. Some firewalls mitigate the SYN Flood attack by buffering the pending connections. 65Mpps means the firewall had to buffer 65 million new pending connections per second. It is entirely possible to overwhelm the firewall this way.

The author remembers dealing with SYN Flood attacks in the late 1990s. They are still very much a reality today.

Source: Akamai State Of The Internet, Summer 2018 report.



Distributed Denial-of-Service (DDoS)

Classic network DoS attacks occur when a single system floods your system or network with packets. You can stop the attack by instructing your routers or firewalls not to accept packets from that system. However, a different breed of DoS attack makes this type of simple protection all but useless; the Distributed Denial-of-Service, or DDoS. In DDoS attacks, the attack does not come from a single system or network; it comes from a wide distribution of computers from all over the internet, sometimes seemingly at random. DDoS attacks are more complicated to set up from an attacker's point of view, but the effects can be more devastating.

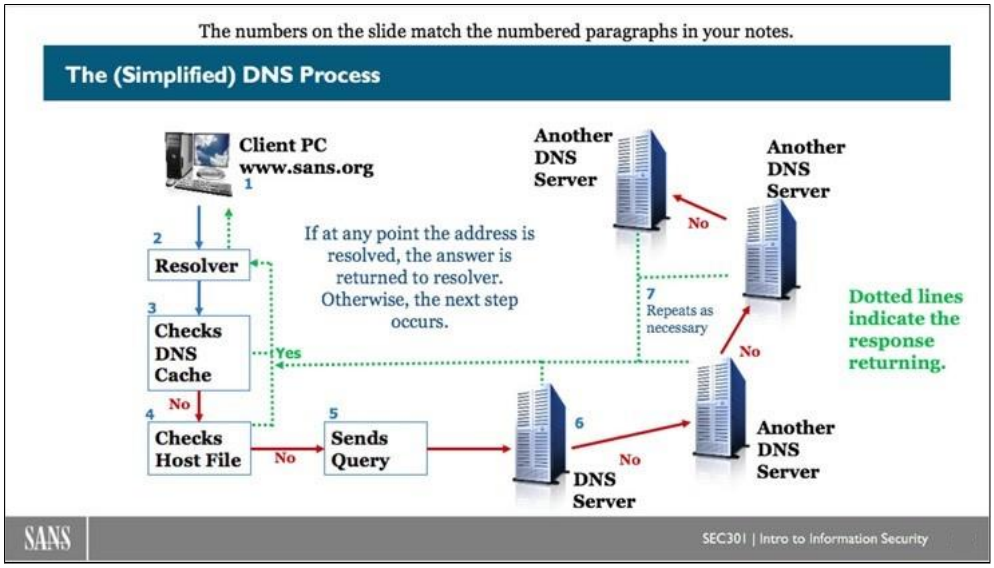
A typical DDoS attack has a number of roles and components. On the roles side is the attacker, the victim, and a number of "innocent" third parties called *bots* that play an unwilling role in the attack. The attacker breaks into each of the bots (either manually or, more likely, using an automated tool, a worm, or spyware) and plants a program that can perform a DoS attack against the victim. There can be hundreds, thousands, or even millions of bots in a single botnet. One or more of the bots are tagged as the *bot herder*. It is the bot herder that sends the attack commands on behalf of the attacker.

When the attacker is ready to launch the attack, he contacts the bot herder and tells it who the real victim is, how long the attack should last, and any other information the bots need. The bot herder then relays that information to the bots, and off they go. What the victim sees is a DDoS attack from many different sites all coming at once.

What makes DDoS attacks so unique and powerful is that they use the diversity of the internet to amplify the attack. The attack seems to be coming from everywhere at once, and because TCP/IP connections have no authentication, there is no way to tell the real origin of the attack.

Note: You may also run into bots being called *zombies*, bot herders called *zombie masters*, and botnets being called *zombie armies*. The zombie terminology was mostly replaced by bot some time ago, but you occasionally still see that terminology in articles and books. Just know the terms are interchangeable.

Domain Attacks (DNS): Reminder on DNS



Domain Attacks (DNS): Reminder on DNS

On the slide above, you see a screenshot from earlier in the class. This is simply a reminder of the basic DNS process. We need this process firmly in mind when we discuss DNS Cache poisoning on the next slide.

Domain Attacks (DNS)

- Allows an attacker to control traffic destined for an internet domain
- Methods:
  - DNS Cache Poisoning (DNS Spoofing)
  - Domain Hijacking (Social Engineering)
- Preventions:
  - Well-configured DNS servers
  - Maintain current contact information
  - Use reputable registrars and implement their security settings!

Domain Attacks (DNS)

The *Domain Name System (DNS)* is critical to the smooth operation and usability of the internet, yet it has no built-in security mechanisms. There is no authentication of either the user, the requesting computer, or the DNS server. And there is no verification that the machine name or IP address the DNS server gives as a reply to a query is, in fact, correct. When a service such as DNS becomes that important and has no built-in security checks or controls, it is ripe for exploitation by evildoers.

Attacks against DNS involve attempts to control traffic destined for a domain on the internet. Although there are several ways to disrupt traffic, we look at two in particular: DNS Cache Poisoning and Domain Hijacking. The two attacks are completely different, but they can have a similar effect: The attacker controls the destination of the packets.

Cache Poisoning

In a *DNS Cache Poisoning attack,* the attacker wants to direct browsers attempting to reach www.victim.com to their server www.attacker.com. The attacker creates a false authoritative DNS record in the attacker.com name server, which maps the name www.victim.com to the IP address of www.attacker.com. Next, they query www.victim.com, asking the victim's DNS server to get DNS records for the attacker.com domain. Those records include the false entry for www.victim.com. Assuming that the victim's DNS server does not have any protections against DNS poisoning, their DNS server now contains a bad entry for their web server, which redirects any queries for www.victim.com to the www.attacker.com website.

Domain Hijacking

The second form of DNS hijacking involves no greater technical skill than the ability to use email or a fax machine. Many domain registrars do little to verify the authority of those who request changes to their domain information. If an attacker can send a convincing-looking email or fax to the appropriate DNS registrar asking to change the IP information for victim.com to now point to attacker.com's systems, many registrars blindly implement the request without much (if any) verification. Some of the larger, more established registrars now perform stricter authentication of DNS change requests using such methods as mail header checking, passwords, or encrypted and signed mail, but there are still a surprising number that do nothing.

Why would an attacker want to hijack a domain? The attacker could put up a bogus web server such as www.xyz.com and advertise that XYZ Corp was giving away millions of dollars' worth of free merchandise or that XYZ Corp was announcing massive layoffs in the coming months. Because users have no way of distinguishing false information from real information (after all, they typed **www.xyz.com** into their browser), this type of activity can have serious consequences for the victim of
a domain hijacking attack.

There are some things your organization can do to help minimize attacks against your domain. The first is to ensure that your DNS servers don't accept any information that isn't relevant to the query being made. You should also keep your account contact information up-to-date and keep track of the expiration dates of your domain. Many domain hijackers simply wait for domain names to expire and then register them for themselves in the hopes of selling them back to the original company. By keeping your contact info updated and not missing the expiration deadlines, you can prevent this from happening. The next thing you can do is to place a registrar lock on your domain. This can help prevent it from being transferred, modified, or deleted by a third party. Finally, you should use only established, well-known registrars for your critical domain name business. Use a vendor that has been around for a while and has good security and authentication mechanisms in place for handling name change requests.

Keystroke Capture (1)

- Hardware or software versions:
  - Hardware costs from $20 to $200
  - Software costs from free to hundreds
- Physical inspection is the only way to detect hardware logger
- All can capture millions of keystrokes
- Software can now do screen captures and such
- Can be done for legal purposes by admins (get it in writing)
- Can be done maliciously

Keystroke Capture (1)

Keystroke capture does exactly what it sounds like. It captures every keystroke the user types on a keyboard (and in some cases, even more).

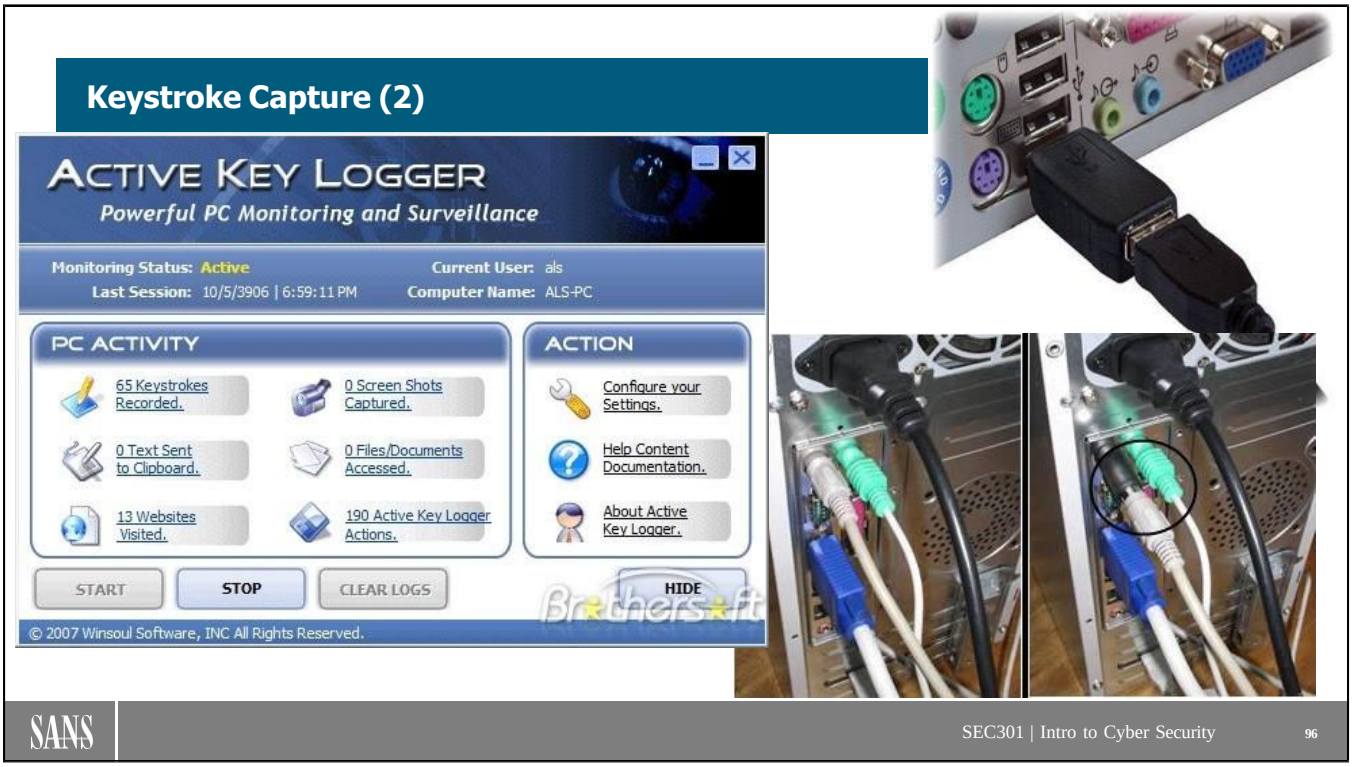
This is a double-edged sword. These techniques can be used by attackers to capture keystrokes including username/password combinations, and, of course, the actual data.

It is also used by many companies to monitor employee activity. Per one report from ABC News, 78% of the Fortune 500 companies capture all employee keystrokes.

There are external devices you plug the keyboard in to. (You see them above and more pictures are on the next slide.) These cost $20 to $200 and can capture millions of keystrokes. They store the keystrokes using exactly the same technology as a USB thumb drive.

There is also software that can be installed on the system. Quite often, the software will capture keystrokes, but also screen captures of whatever is currently displayed on the screen when a mouse is clicked, for example.

Companies regularly use commercial software to monitor employee activity via keystroke capture. They can also purchase hardware such as keyboards and laptops with the capability built in.



Keystroke Capture (2)

Here, you see a screen capture of one of the freeware keystroke capture software utilities. Notice that you can configure the software to do screen captures. You can also configure it to send an email back to you periodically with everything it is capturing.

You also see pictures of the hardware versions plugged into a computer. These will often go undetected because we don't normally crawl under our desks to look at the back of the computer. Of course, it is also true that many users would simply assume the device was legitimate if they did see it.

Do be aware that using these without proper authorization can get you into trouble. In March 2014, federal wiretap charges were filed against a woman who put this software on her husband's computer. She thought he might be having an affair. (He was.) There have been other similar cases.

Module 13: Malware and Anti-malware

- Types of Malware
  - Virus/Worm/Trojan/Logic Bomb/Ransomware
- Antivirus
- Personal Firewalls

COURSE ROADMAP

- Module 11: Wireless Security & IoT
  - Lab 4.1: Wireless Access Point Configuration
- Module 12: Network Attacks
- **Module 13: Malware and Anti-malware**
  - Lab 4.2: Anti-malware Scanning

Module 13: Malware and Anti-malware

This page intentionally left blank.

How Much Malware Is There?

- How much malware is there?
- Depends on who you ask:
  - Per one report:
    - 1990: 1,300 pieces of malware existed
    - 2000: 50,000 pieces of malware existed
    - 2010: 200 million total malware in the world
  - Per a different report:
    - By the end of 2013, there were 145 million
    - 30 million (20%) created in 2013 (82,000 per day)
  - 2018: Nearly 2 million PER DAY unique malware variants detected (Symantec)
    - Over 23 per second…
- Regardless, the problem is large and rapidly growing bigger

How Much Malware Is There?

How much malware is there in the world? It seems to be anybody's guess. For example, there are two reports mentioned here. (We *could* bring in many more to really cloud the waters, but we'll try to keep it simple and still illustrate the point.)

The first report places the total number of malware in the world by the end of 2010 at 200 million. The second report puts that number at 145 million by the end of 2013. So how many are there really? It is difficult to give solid numbers on this. Each company counts malware differently. One company may include spyware in their numbers, yet another doesn't.

The point remains: This problem is getting worse. We need to understand the issues and terminology to try and combat a growing problem both at home and at work.

References

https://www.helpnetsecurity.com/2011/03/14/40th-anniversary-of-the-computer-virus/
http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Annual-Report-PandaLabs-2013.pdf or http://tinyurl.com/zy57cwa
Symantec 2018 Internet Security Threat Report: https://www.symantec.com/security-center/threat-report

Footnote: The first reference above has a really good summary of important historical malware: How we got to where we are. It is worth reading when you have time.

Propagation Techniques

- Email: The most common method of malware infection
  - Per Symantec: For the year 2017, 1 in 412 email messages had malware in the message
  - Spam accounts for 54.6% of all email and a lot of the infected emails
- Email attachments accounted for 92.4% of all malware in 2017 (Verizon 2018 DBIR)
- Mac malware rose 80% in 2017 per Symantec
  - Beware – that is misleading. Most were actually targeting cross-platform JavaScript and MS Office Macros. Mac targeted malware in 2017 = 12

Propagation Techniques

Email is by far the most common propagation technique for malware. In fact, according to Symantec, in 2017 if you took 412 email messages at random, one of them will contain malware. This is actually an improvement over 2016 when the rate was 1 in 131, 1 in 220 for the year 2015 and 1 in 244 in 2014. Part of this equation is the continued growth of SPAM, which now accounts for 54.6% of all email worldwide in 2017. A significant percentage of that SPAM contains malware. (Source: 2018 Symantec Internet Security Threat Report (ISTR))

According to the 2018 Verizon Data Breach Incident Report, 92.4% of all malware came from malicious email attachments. This means that we cannot forget the other infection vectors (e.g., the world wide web), but email should undoubtedly be a priority focus.

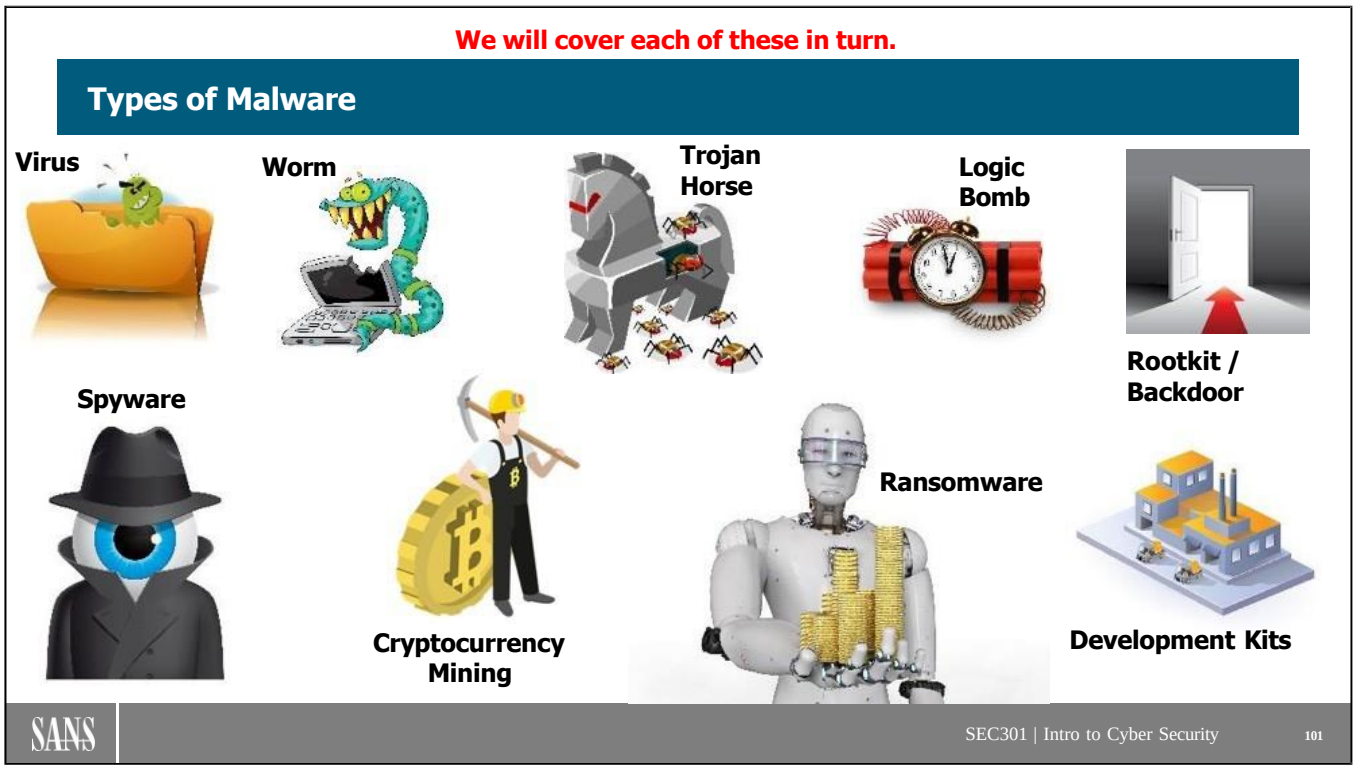
Malware Realities

- Definitions are fine for study purposes:
  - But with 1 million new variants per day ...
  - Malware does not always fit into a nice, neat category
  - A virus might also be a worm, and a trojan might also be a virus
- Historically, malware was about dirty tricks—not anymore:
  - Depending on whose numbers you use, today ...
  - 75% to 90% of malware has a monetary goal
  - Today, a lot of the "dirty trick" malware has a geopolitical motivation
    - E.g., shutting down a nation's power grid

Malware Realities

In the following pages, we give you cut-and-dried definitions of malware terms. For example, you see definitive definitions for the terms virus, worm, trojan, and logic bomb. Knowing these definitions is important, in part because they help you understand how malware works and spreads. However, keep in mind that malware rarely sticks to these definitions. A virus may also have the traits of a worm or trojan horse, worms often also have the traits of the trojan horse, and so on.

Also, understanding the big picture with malware requires understanding the motivations of the malware author. Not that many years ago, malware was mostly about dirty tricks and proving that something was possible. Today, depending on which company's numbers you choose to look at, somewhere between 75% and 90% of malware has a monetary goal. It is now all about the money. The malware author is after your credit card numbers, online banking information, and such.



Types of Malware

This slide depicts some of the more common types of malware that we will cover. It would be nice if this were the entire list of types of malware, but unfortunately, there are others.

We will use the graphics above to help you keep track of which type we are discussing.

Virus

- Virus:
  - Software that, to survive and propagate, must insert itself into other executable code:
    - When you execute Word, you unknowingly execute the virus
    - The virus becomes memory-resident and infects other executables
- Often said to be "parasitic in nature"
  - It relies on other software to propagate

Virus

Virus: Defined as any piece of software that, "to survive and propagate, must insert itself into other executable code." For example, if Microsoft's Word.exe is infected and you run that program, you unknowingly execute the virus code as well. The virus typically becomes memory-resident and remains in RAM even after you close Microsoft Word. Hours later, you execute some other piece of software and the virus inserts itself into that executable at that time.

Because of this reliance on other software, viruses are often referred to as "parasitic in nature."

Worm (or Network Worm)

- Worm:
  - Self-standing, self-executing software:
    - Traverses your network looking for vulnerable systems
    - When it finds one, it infects it and then uses that as a platform to move on
- Usually, worms only know how to take advantage of one or two vulnerabilities
  - And almost always target desktop operating systems

Worm (or Network Worm)

Worm: By contrast, a worm is self-standing software that is self-propagating. Much like a network vulnerability scanner, it scans through your network, looking for a system that has a vulnerability it knows how to take advantage of. When it finds "Windows 2008, patch level 2," for example, it then exploits a vulnerability that it is aware of in that specific OS and patch level. Most worms know how to take advantage of one or two things, occasionally three at most. There are a few exceptions to that, though.

Trojan Horse

- Trojan Horse
  - Software with a:
    - Known desired function
    - And an unknown, undesired function:
    - A fake login screen logs you in and sends credentials to attacker
    - Screensaver installation also puts redirectors in the browser
- This is the most common infection vector
  - A PDF document causes an infection when you open it
    - The PDF is the known desired function
    - The malware infection is the unknown, undesired function

Per Symantec, you can buy an Android-based banking Trojan on the dark net for $200

Trojan Horse

Trojan horse: Any piece of software that has a "known desired function, as well as an unknown undesired function" is defined as a Trojan Horse. According to a Panda Security report referenced earlier, Trojans accounted for 78.97% of all malware in 2013. A common example: You download a free screensaver. When you install the screensaver, you also install malware that tracks your internet surfing activity. We will see other examples as we proceed through the materials.

Logic Bomb

- Malware that waits for a preconfigured event or date before executing (or detonating)
- Event-based logic bombs are more common:
  - Example: Snippet of code that says: "If my name disappears from the employee database, delete the employee database."
  - Several real-world examples (links in the notes)
  - Also, a popular topic in fiction (books, movies, and TV)

Logic Bomb

Any piece of malware that "waits for a preconfigured event or date" before executing is defined as a logic bomb. Of course, with logic bombs, they are said to "detonate" instead of execute.

An old but famous example of this kind of malware comes from 1991 (meaning, these are not new). The Michelangelo virus would execute only on March 6, which is Michelangelo's birthday. There was no other reference to the famous artist in the malware. The Michelangelo virus also illustrates the point from earlier that malware can fall into multiple categories. This virus spreads by infecting the boot sector of floppy disks and hard drives, which falls within the definition of virus. (Boot sectors are executable.) It is also a logic bomb in that it executes only on a preconfigured date.

Other examples include: The programmer who put the trigger into the employee management software that said, "If my name is removed from the employee database, delete the employee database." A disgruntled network administrator who placed a logic bomb that would have formatted every hard drive on the Fannie-Mae network at 1 minute after midnight, 2010. Also, a logic bomb triggered to go off at exactly 1400 hours on March 20, 2013, wiping the hard drives of three banks and two media companies in South Korea.

References

http://www.wired.com/threatlevel/2009/01/fannie/
http://www.wired.com/2013/03/logic-bomb-south-korea-attack/
http://computer.howstuffworks.com/logic-bomb.htm

Rootkits

- Software that allows a hacker to get back into a compromised system, control its functions, etc.; all without being detected:
  - Hacker's files, processes, etc. do not show up, even to the admin
  - Almost always provide the attacker with easy backdoor access
- Examples:
  - Knark for Linux/UNIX: Very elegant
  - NetBus for Windows (PC Anywhere with a bad attitude)
- Tend to be difficult to detect and remove
- Sony music CDs even installed a rootkit at one time (Extended Copy Protection)
  - Two years later, they did it again with USB thumb drives

Rootkits

Rootkits come in many variations as well. There are file-level, user-level, and kernel-level rootkits. Each works and behaves a little differently. However, there tend to be some similarities among rootkits:

- They almost always insert a backdoor on the system to allow the attacker easy access.
- They commonly hide the attacker's files, system processes, and so on from the administrator.
- They tend to actively "fight" against removal.

From there, variations abound. Some, such as NetBus that we see on the next slide, provide for remote control of a computer. Think of something such as PC Anywhere with a bad attitude—and legitimate users cannot see what the attacker is doing with NetBus the way they can with PC Anywhere.

They can also come from unexpected places. In 2005, it was discovered that several Sony music CDs had a rootkit. If you put them into your PC, they would infect you. Sony could use the backdoor to see if you had illegal music. More information, including the list of CDs, is at these links.

References

https://www.wired.com/2005/11/real-story-of-the-rogue-rootkit/
https://www.eff.org/deeplinks/2005/11/are-you-infected-sony-bmgs-rootkit

Rootkits: Example – NetBus

Rootkits: Example – NetBus

These screenshots show the NetBus rootkit that attackers can install on Microsoft Windows. (This can be the malicious payload of the free screensaver, for example, so yes, NetBus is also a trojan.) Notice on the left side, it has "lamer tools," like opening the CD-ROM drawer, switching the mouse buttons, and such. But on the right, you see much worse things such as spy functions to record audio and video (if there is a camera on the system).

This can be extremely nasty. In 1999, this tool was used by an unknown person or persons to put 3,500 child pornography images on the PC of a law professor at Lund University. He was acquitted of all charges in 2004; it was proven definitively that it was a remote attacker using NetBus. However, by the time he was cleared, he had lost his job, his name had been published in news reports, and he had to flee the country.

Yes, these can turn nasty indeed.

Spyware

- Records computer activity (browsing, keystrokes ...)
- Can be very damning
  - Keystroke capture can record online banking login, for example

- Historical – used for targeted advertising
  - Your surfing activity is sold to advertisers, and so on
    - E.g., if you frequent web pages about classic cars, you will start seeing more advertisements for classic cars
    - As you will see in the Browsing section, they have a more efficient means of doing this
    - Advertising spyware has now become rare...

Spyware

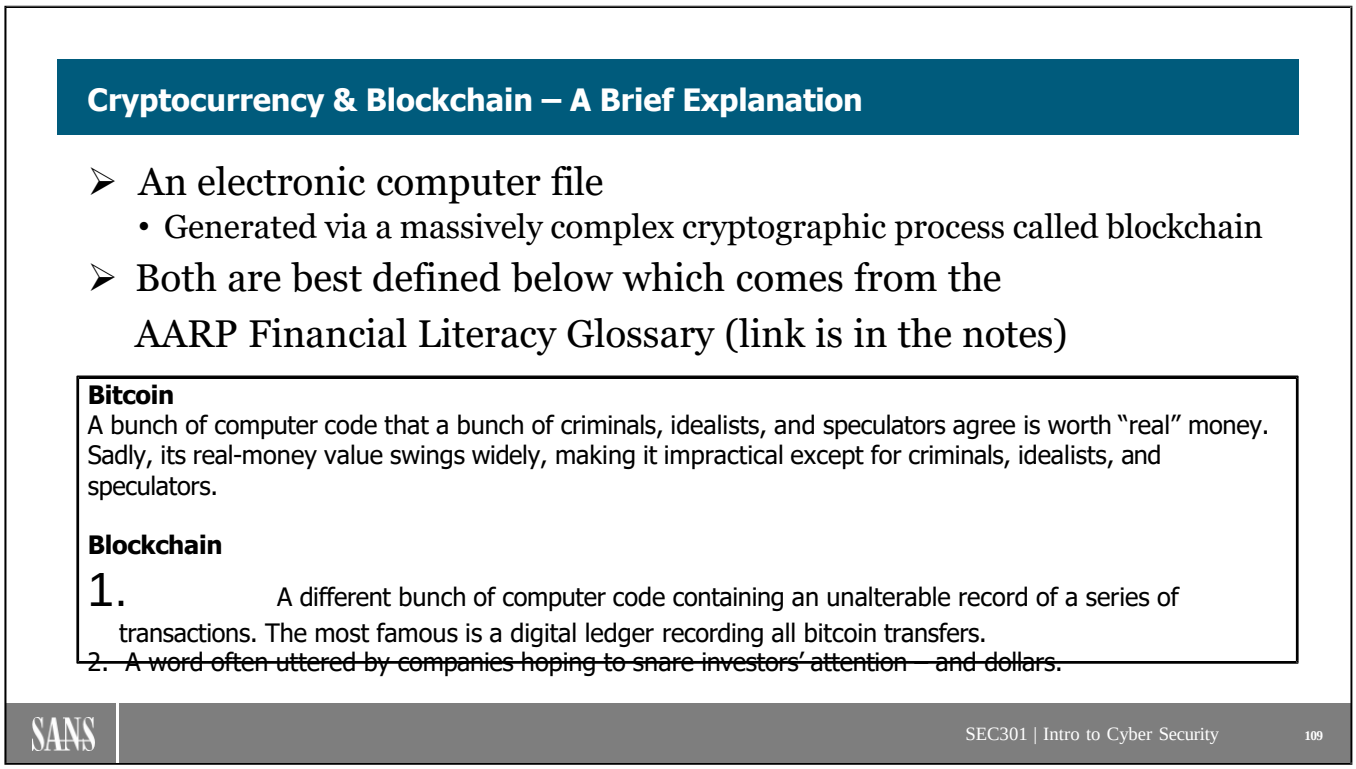
Even if you have an active and effective antivirus program in your environment, chances are you still have a problem with spyware. *Spyware* is the latest twist on the age-old game of getting information from users' systems without the users knowing about it.

The exact activities tracked varies, but typical uses include logging keystrokes, recording web-browsing habits, gathering information about installed software, and obtaining personal information about the user. What does the spyware do with all this information? Most spyware apps send it to some unseen central server for use by the spyware creator. From there, the creator can (in the best case) use the data to target marketing information to the user or (in the worst case) use the information against the user in some way.

Unfortunately, a lot of antivirus software either does not look for spyware at all or does so poorly. You have to run a separate anti-spyware utility. There are a number of utilities that do well at finding and eliminating spyware on your system. Perhaps the best known is Spybot Search & Destroy, available from Safer-Networking.[1] The program's operation is automatic, and the results are comprehensive. Not only does Spybot find classic "spyware," it also looks for tracking cookies, system files, and history lists that may be used to track your activities and your information. If it finds a potential problem, the user can click the listing to see a detailed description of the program along with the potential it has to compromise your system. The price is right (it's free, although donations are requested) and it (or a program like it) should be considered as vital as antivirus software for an internet-active system.

Reference

[1] http://www.safer-networking.org/



Cryptocurrency & Blockchain – A Brief Explanation

If you pay attention to the news, in particular tech news or investing news, then you have certainly heard of cryptocurrency. It is an electronic computer file generated by an extremely complex cryptographic process called "blockchain". It basically has value, because someone says it has value. But that value is not backed by any government the way traditional currency is.

The best simple explanation of both, that the author has seen, comes from the AARP (American Association of Retired Persons) Financial Literacy Glossary at the link below. Any attempt to explain the technical details behind these terms would take hours, if not days

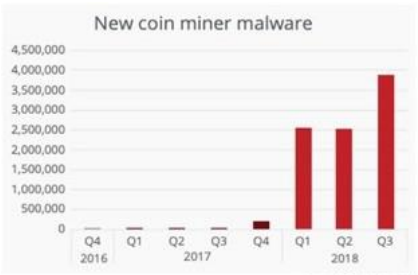
Reference

https://www.aarp.org/money/investing/info-2018/financial-literacy-glossary-terms.html

See the link in the notes for the cost to mine a Bitcoin in your country.

Cryptocurrency Mining – Cryptojacking

- Fastest rising category of malware
  - 4,000% increase in 2018 (but started at almost zero)
  - Infected systems are used to create cryptocurrency
  - Huge cost-savings for the miner – they use your electricity
    - In the U.S., it costs about $4,758 in electricity to create one bitcoin—but it may happen over many months
      - The processing power needed is extreme
    - Globally, the electrical consumption of all cryptocurrency mining is equal that of the Czech Republic—a country of 10.6 million people



Cryptocurrency Mining – Cryptojacking

McAfee reports that Cryptojacking malware (or coin miner malware) increased 4,000% in 2018. True, as the chart in the slide shows, it began at almost zero, so a 4,000% increase is not as massive as it appears at first glance. Still, this is a very significant increase and a category of malware we need to pay attention to.

Some feel this is a victimless crime. After all, the attacker is only using your computer's power to create currency. At most you might see a slowdown of your computer. Right? Wrong! You will also see an increase in your electric bill. Based on the Marketwatch report referenced below, given the average electricity cost in the U.S., it costs about $4,758 in electricity to mine one bitcoin. The report details costs in several different countries.

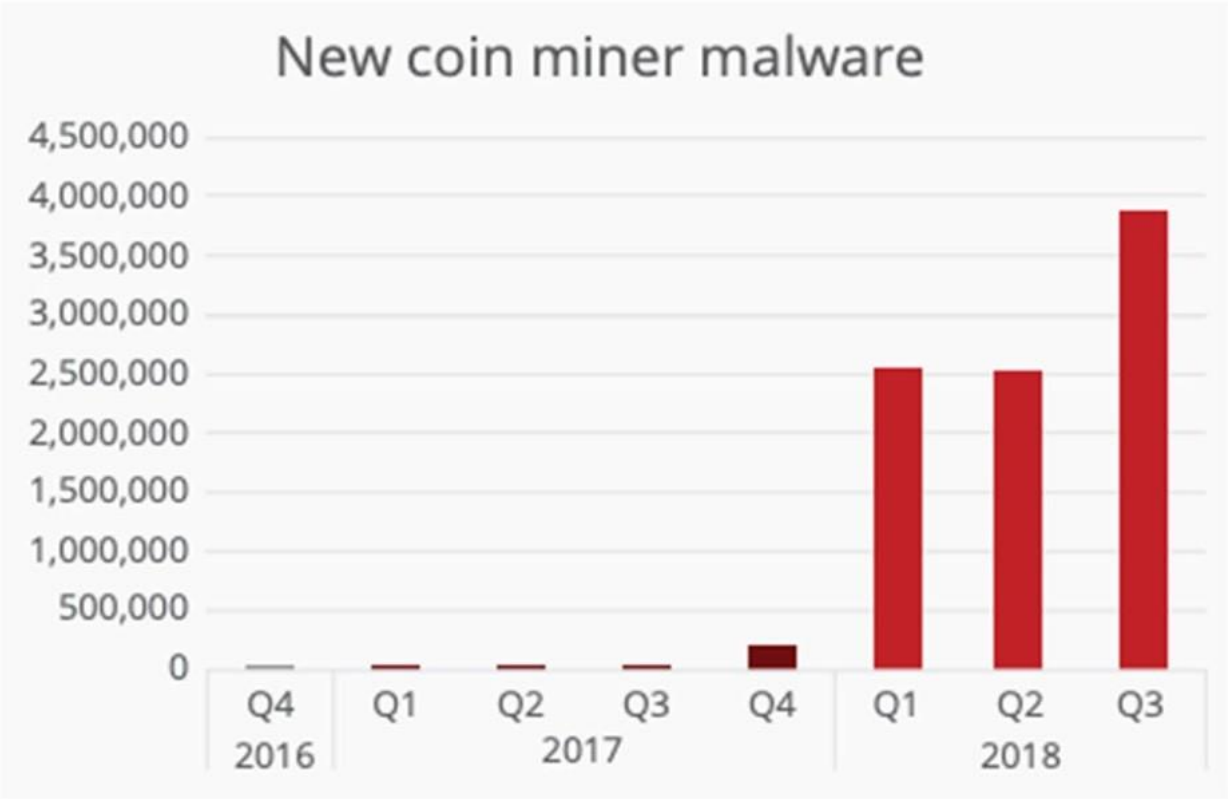
Note that if you have Cryptojacking malware on your system at home, the creation of the cryptocurrency may happen over many months, so you don't notice an immediate spike in your electric bill. However, you do pay the price over time.

Sources

https://www.marketwatch.com/story/heres-how-much-it-costs-to-mine-a-single-bitcoin-in-your-country-2018-03-06

https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf

Per McAfee – the 2018 growth in Cryptojacking malware:



Source: McAfee Labs, 2018.

Frequency of this attack dropped significantly in late 2017 & throughout 2018. Cryptojacking took over…

Ransomware

- Makes the data on a computer unavailable until ransom is paid
  - Most commonly encrypts files
    - Will usually follow a network share to encrypt the files there as well
  - Some use other methods of blocking access
  - Ransom is paid using electronic currency: Bitcoin is common
    - An untraceable digital currency not controlled by any government
    - There is a LOT of debate about paying ransom
  - Ransomware authors consider themselves businessmen
    - Offer exceptional technical support
  - Some now re-extort after ransom is paid

Ransomware

Ransomware is a category of malware that makes a computer unavailable for use until a ransom is paid. Most ransomware works by encrypting the files on your computer. When you pay the ransom, the ransomware author provides the decryption key and instructions for recovering your files. Less common, some ransomware uses alternative methods of making your files inaccessible.

Note that most of the variants that utilize encryption will follow a network share. Meaning that if you have a folder of files shared across the network, those files will be encrypted as well.

Almost without exception, ransom is paid in the form of Bitcoin. This is an untraceable digital currency that is not controlled by any government. The price of Bitcoin fluctuates more rapidly than the stock market.

Interestingly enough, the authors of ransomware consider themselves to be "an honest businessman." (Yes, that is a direct quote from one of the ransomware authors.) They offer exceptional support to their victims. They will walk a victim through the process of obtaining and uploading the Bitcoin to them. They have even been known to accept lower amounts if they can tell the victim is trying to work with them but cannot obtain the required amount of Bitcoin. In at least one case, a ransomware author used one of his victims as a reference, as in: "Call this man; he will tell you that I am an honest businessman who stands behind his word."

Ransomware Defense

- Careful surfing habits help
  - But will not fully protect you
- Versioning Backups!
  - Retains each saved version of files
  - Even if the encrypted file is backed up ...
  - The prior unencrypted version is still available

Ransomware Defense

The screenshot above is specific to "Wana Decrypt0r" (better known as WannaCry) in 2017, but it is indicative of a typical ransomware screen. It informs the victim that their files have been encrypted and of the amount of money it will cost them to obtain the decryption key. Notice that it also includes a countdown timer to let you know how much time you have to make payment. Toward the bottom, it includes instructions for obtaining the Bitcoin. Also, notice there are helpful links to click including "About Bitcoin", "How to buy Bitcoin", and of course, "Contact Us" in case you need assistance. It is sad, but ransomware authors provide some of the best technical support in the IT industry.

Safe surfing practices can help you avoid ransomware, but they will not completely protect you. Some infections occur when someone visits a completely legitimate web page, but the page has either been defaced with code to cause infection or displays a banner ad that infects them.

The best current defense is to have backups that support "versioning." This means that each time you save a file, that version is backed up and available for recovery. In the case of ransomware, the encrypted version of your files may back up, but the prior unencrypted version will still be available for recovery.

Malware Development Kits (Factories)

- Software you can purchase
  - Point-and-click creation of Malware
- Ransomware is the current leader here
  - A ransomware development kit sells on the darknet for $10 to $1,800
    - The more you spend, the better it is of course
- Some now operate on a royalty basis
  - For example, the factory creator gets 10% of proceeds

Malware Development Kits (Factories)

People will make money any way they can. Sometimes, malware authors make their money by writing the malware itself. Sometimes they create software that will create the malware for others and sell it as a product. The authors of malware creation software call them Development Kits, or more commonly, "Factories."

There are now many of these on the market, most sold on the dark web. Most of the malware factories for sale create ransomware for the simple reason that ransomware is the "hot market" today. The price for these factories varies greatly, but even the best are less than $2,000—a tiny fraction of what someone stands to gain in ransom payments.

It is interesting that some of the factories available on the darknet now work on a royalty basis. For example, the factory creator might get 10% of the ransom. The same smart business practices that work for legitimate businesses unfortunately also work in illegal businesses as well.

Other Malware Terms

- Polymorphic malware:
  - Virus designed to self-modify to fool antivirus software
  - Most antivirus software looks for a signature, unique string in the virus code
  - Polymorphic viruses attempt to modify their unique strings
- Retrovirus:
  - A virus that actively attacks/disables antivirus software (and personal firewalls sometimes)
  - Often also blocks access to most/all antivirus sites:
    - Can be extremely difficult to get rid of
- Multipartite:
  - Simply a virus that spreads through multiple mechanisms
  - Often said "multiple infection vectors"

Other Malware Terms

There are a few other malware terms that you may run into and will want to have familiarity with.

Polymorphic malware is designed to self-modify via a variety of mechanisms. By doing so, they attempt to fool antivirus software into not detecting them.

Retrovirus: In biology, a retrovirus is a virus that attacks the human immune system. In computing, a retrovirus actively attacks our antivirus and other endpoint security software, trying to disable it.

Multipartite: This is a fancy way of saying "malware that can infect you in more than one way." In other words, a virus that is both a file infector and a boot sector infector is multipartite.

Anti-malware (Antivirus)

- The first thing installed on a new computer:
  - Windows / Mac / Android / Any Computer Today!
- Two general categories of detection:
  - Signature: The software has a database of strings unique to each virus—it scans executables looking for those strings
  - Heuristics: Watches for virus-like behavior:
    - That is, something trying to write to a boot sector

- Most antivirus now includes antispyware capability:
  - They scan for all types of malware

Anti-malware (Antivirus)

After the operating system, this is likely the single most important piece of software installed on a computer today. And we do mean any computer, whether it is running Windows, Mac, Apple, Android, or any other operating system.

Anti-malware most commonly scans for more than just viruses (hence, we are not using the term antivirus as much). Most of the packages, especially those at the forefront of the marketplace, are scanning for viruses, worms, trojans, spyware, adware, and all other categories of malware.

Signature: Almost all of them utilize a signature analysis engine. Every virus has some unique string (called a signature) somewhere in its code. The "signature database" contains those unique strings for the malware currently making the rounds. When you do a virus scan, your anti-malware package goes through the executables on your system, looking to see if it can find one of those strings. If it does, you have that virus.

Of course, as we have already discussed, there are millions of new malware released every day, and each of them has a new signature. This is why we have to keep our signature databases up-to-date. When the author first installed antivirus software in the late 1980s, he received the signature updates once a quarter on a 5 ¼-inch floppy disk. Today, his antivirus software updates the signatures every 3 minutes by default.

Heuristics: The second common method for looking for malware is called heuristics. This method does not rely on a signature database. Instead, it watches for malware-like activity. A perfect example: There are few times when your computer writes to the boot sector of the hard drive. Specifically, it does that when:

- You format the hard drive
- You repartition the hard drive
- You run a checkdisk command to check the drive for errors
- A boot sector virus writes to the boot sector of the drive, infecting your computer

To write to the boot sector of the drive, software must use a particular system call. Heuristic anti-malware monitors that system call. If anything attempts to use it, it blocks its use until you approve it. The idea being, if you are not doing one of the first three operations listed above, you would not give approval. Of course, this does rely on the knowledge of the user.

Heuristics is not a new idea. It does have the advantage of possibly blocking malware that is not in your signature database. But it is far from perfect. Go back to the fact that there are tens of thousands of new malware coming out every day. Each of them behaves a little differently. Exactly which behavior should your endpoint security software watch for?

Windows Defender

- Free - Built-in and enabled by default
- Gets good, but not great, rankings in *recent* anti-virus comparisons (beware of the old reviews when it was new)
- Supports the Microsoft Antimalware Scan Interface (AMSI), which allows it to scan "fileless" malware that only exists in memory, such as malicious PowerShell code
- Don't have to worry much about future OS updates breaking it
- Has optional integration with some of Microsoft's cloud services, such as Advanced Threat Protection (ATP)

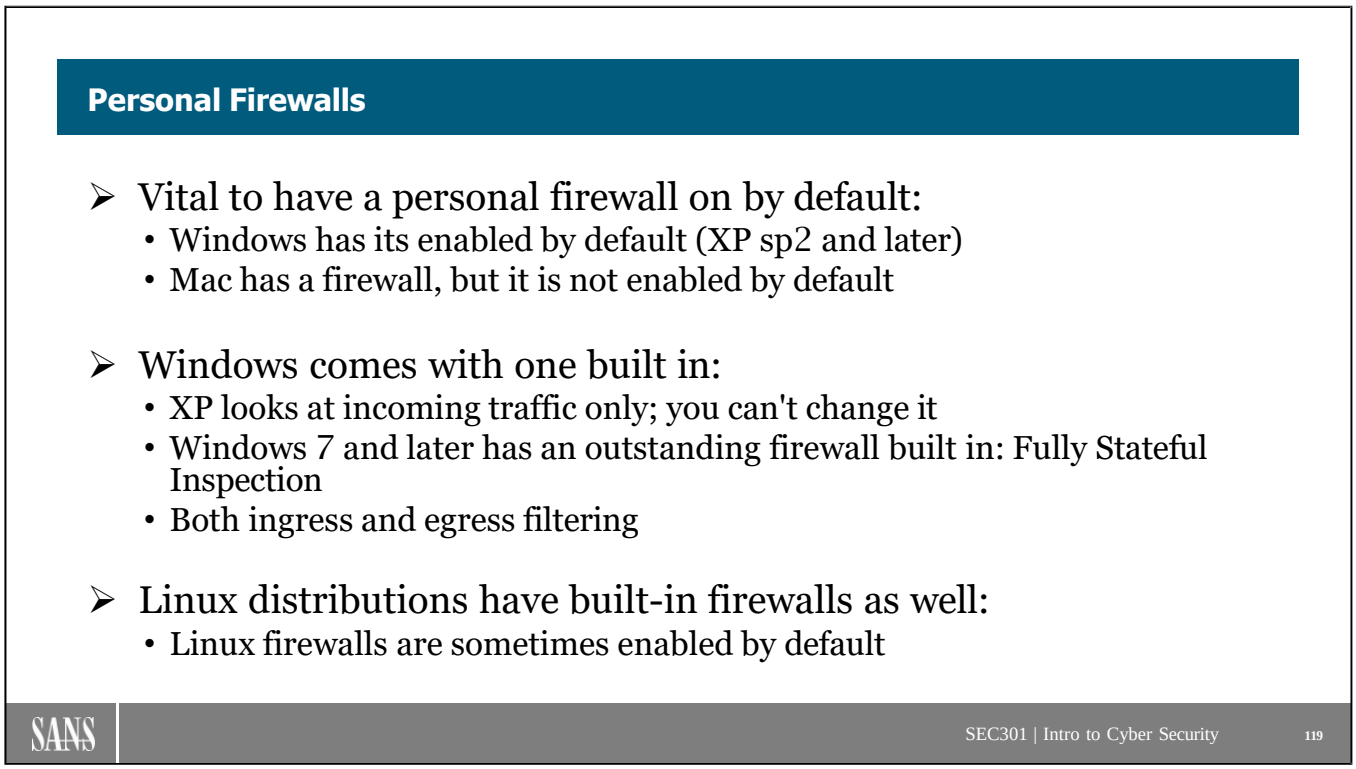
Windows Defender

In the past, Microsoft has tried to integrate anti-virus into Windows on a number of occasions. That effort has always failed spectacularly.

Recently with Windows 10, they introduced Windows Defender and it is actually pretty decent. The best news is that it is free (once you pay for Windows) and installed and enabled by default. When you look at reviews of Windows Defender, early reviews were pretty dismal. Lately, the reviews have improved dramatically. Pretty much, each review of a newer version is better than the last.

An important feature of Windows Defender is that it supports the “Microsoft Antimalware Scan Interface (AMSI). Among other things, this allows it to scan for malware that is only in RAM and not on the drive. This way, it can find more malware, such as malicious PowerShell code (which is on the rise). A lot of malware scanners do not do this.

Because it is a Microsoft included service to the Operating System, there is minimal concern that future updates will break Windows Defender – that is not the case with some other Antimalware products. Also, it provides some (and growing) integration with Microsoft Cloud Services such as Advanced Threat Protection (ATP).



Personal Firewalls

Another vital piece of software is the personal firewall. You should NEVER connect a computer to the internet unless the personal firewall is turned on. It takes as little as 3 to 5 minutes for an unprotected system on the internet to be compromised.

The Windows firewall has been enabled by default since it added the feature in Windows XP service pack 2. The XP firewall looks only at traffic into the PC, not traffic leaving it. The Windows 7 (and later) firewall is actually an outstanding protection feature. It is fully stateful inspection (a term we explain fully at another point in the course). When you tell that firewall that you are connected to a public location such as a coffee shop, your computer pretty much becomes a black hole. The *only* things your system responds to are ARP packets.

Mac also has a good firewall built in. Unfortunately, it is not enabled by default. It is simple enough to enable, but you have to know to do so.

All Linux operating systems have IPTables, which can be used as a personal firewall. Many Linux distributions turn that firewall on by default, and some do not. Even for those that have it on automatically, the default configuration can vary widely.

Lab Time

- LAB 4.2: Anti-malware Scanning

- Objectives:
  - Use the Malwarebytes tool to scan for malware
  - Safely remove malware using Malwarebytes
  - Whitelist non-malware PUPs using Malwarebytes
    - PUP = Potentially Unwanted Program
  - Estimated completion time: 30 minutes

This page intentionally left blank.

SEC301.4 | Introduction to Cyber Security

SANS

Wireless Security, Network Attacks, & Malware

End Day 4

This page intentionally left blank.

Questions & Answers

This page intentionally left blank.

Appendix

Review Questions

This page intentionally left blank.

Answers

SANS

Wireless Security Review Question

This page intentionally left blank.

- What is the encryption algorithm used in WPA2?
  A. RC4
  B. AES
  C. Diffie-Hellman
  D. Triple DES

- What is the single most important thing you can do to improve Wi-Fi security?
  A. Upgrade to WPA2
  B. Upgrade to WPA2
  C. Upgrade to WPA2
  D. Upgrade to WPA2

This page intentionally left blank.

Review Questions (2)

- Why does antenna / transmitter strength matter in Wi-Fi?
  A. You will interfere with your neighbor's signal.
  B. Stronger antennas allow for stronger encryption keys.
  C. Antenna strength is a static value; it does not matter.
  D. Wi-Fi signals travel and can be intercepted outside your facility.

- What is the most common Bluetooth class and range?
  A. Class 1: 10 meters
  B. Class 2: 1 meter
  C. Class 3: 100 meters
  D. Class 1: 100 meters
  E. Class 2: 10 meters

This page intentionally left blank.

Review Questions (3)

- In Bluetooth, what does SSP stand for?
  A. Super Simple Pairing
  B. Seriously Secure Pairing
  C. Secure Simple Pairing
  D. SSP is not a Bluetooth acronym

- Which encryption algorithm is used in SSP?
  A. Triple DES
  B. AES
  C. RC4
  D. MD5
  E. Diffie-Hellman

This page intentionally left blank.

- What is the most recent Wi-Fi standard released in January 2014?
  A. 802.11g
  B. 802.1i
  C. 802.11ac
  D. 802.11.n

- What is the current widely deployed encryption specification for Wi-Fi?
  A. WEP
  B. WPA
  C. WPAN
  D. WPA2

This page intentionally left blank.

- If both Bluetooth devices have a screen to display a 6-digit number and can accept a yes/no response, which Association Model should you use?
  A. Passkey Entry
  B. Numeric Comparison
  C. Out of Band (OOB)
  D. Just Works

- What is the key exchange mechanism used by Secure Simple Pairing?
  A. Advanced Encryption Standard (AES)
  B. Advanced Encryption Standard Diffie-Hellman (AESDH)
  C. Elliptic Curve Diffie-Hellman (ECDH)
  D. These do not use a secure key exchange mechanism

This page intentionally left blank.

Answers

SANS

Network Attacks Review Question

This page intentionally left blank.

- What are the five phases of an attack?
  A. Covering Tracks, Reconnaissance, Scanning, Gaining Access, Maintaining Access
  B. Covering Tracks, Maintaining Access, Gaining Access, Scanning, Reconnaissance
  C. Scanning, Reconnaissance, Gaining Access, Maintaining Access, Covering Tracks
  D. Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks
  E. Phishing, Access, Exfiltration, Public Posting, 6 o'clock news

- Which is the most common category of attack?
  A. Phishing
  B. Spear phishing
  C. Social engineering
  D. Ransomware

This page intentionally left blank.

- What is the URL of the Wayback Machine?
  A. http://www.wayback.com
  B. http://www.wayback.org
  C. http://www.archive.org
  D. http://www.sans.org/wayback

Where would you find the Google Dorks?
A. The Google Hacking Database
B. The Google Dorks Database
C. The Googleist tip sheet
D. The Google What's???

This page intentionally left blank.

- Is Spear Phishing an example of direct or indirect social engineering?
  A. Indirect
  B. Neither
  C. Direct
  D. Both

What does "A reason given in justification that is not the real reason" define?
A. Pretexting
B. Lying
C. Manipulation
D. Obfuscating

This page intentionally left blank.

- Hiding the real source IP address is commonly referred to as
  A. IP Hiding
  B. IP Spoofing
  C. That is not possible
  D. ARP Spoofing

- What does the acronym MitM stand for?
  A. Man-in-the-Middle
  B. Mission-Impossible-the-Movie
  C. Missing Threat Management
  D. Modern TCP Management

This page intentionally left blank.

- What is an attack against the availability of a system called?
  A. System Availability Denial (SAD)
  B. Availability attack
  C. Denial-of-Service (DoS)
  D. It has no formal name (IHNFN)

- Which is an attack that exploits the TCP three-way handshake?
  A. SYN Flood
  B. Handshake Flood
  C. DoS
  D. Zombie Flood

This page intentionally left blank.

- What are two names for the computers commonly used in Distributed Denial-of-Service attacks? (choose two)
  - A. Zombot
  - B. Zombie
  - C. Bot
  - D. DDoSer
- What are two names for the collection of machines commonly used in DDoS attacks? (choose two)
  - A. SYN Army
  - B. Zombie Army
  - C. DDoS Team
  - D. Botnet

This page intentionally left blank.

Answers

SANS

Malware and Anti-malware Review Question

This page intentionally left blank.

Review Questions (1)

- What is malware that is parasitic in nature called?
  A. Virus
  B. Worm
  C. Trojan
  D. Logic Bomb

- What is malware that is self-standing and self-propagating in nature called?
  A. Virus
  B. Worm
  C. Trojan
  D. Logic Bomb

This page intentionally left blank.

Malware and Anti-malware

Review Questions (2)

- What is malware that waits for a preconfigured event or date to execute called?
  - A. Virus
  - B. Worm
  - C. Trojan
  - D. Logic Bomb
- What is malware that has a known desired function as well as an unknown undesired function called?
  - A. Virus
  - B. Worm
  - C. Trojan
  - D. Logic Bomb

This page intentionally left blank.

- What is the most common reason malware is created today?
  A. To make money for the author
  B. To prove that a virus can spread in a particular way
  C. To destroy all of your data
  D. Just because they can!

- What is malware that must insert itself into other executable code?
  A. Logic Bomb
  B. Trojan Horse
  C. Worm
  D. Virus

This page intentionally left blank.

Review Questions (4)

- In computing, what does the term *retrovirus* describe?
  A. Malware that attacks security software (antivirus, firewall, etc.)
  B. Malware that is self-modifying
  C. That is a nonsense term
  D. Malware that infects via multiple infection vectors

- What does the term *multipartite* describe?
  A. Malware that is self-modifying
  B. A trojan horse that is also a virus and a worm
  C. Malware that infects via multiple infection vectors
  D. A virus that divides itself into multiple parts to avoid detection

This page intentionally left blank.

Review Questions (5)

- What does the term *polymorphic* describe?
  A. A logic bomb with multiple triggers
  B. Malware that self-modifies to avoid detection
  C. A worm that can infect multiple types of systems
  D. A virus that attacks both Windows and Mac operating systems

- Which of the following is most common?
  A. Logic Bomb
  B. Trojan Horse
  C. Worm
  D. Virus

This page intentionally left blank.

Review Questions (6)

- What is malware that monitors and reports your online activity called?
  A. Rootkit
  B. Spyware
  C. Adware
  D. Virus

- What is malware that usually provides a backdoor and hides the attacker's activities from administrators called?
  A. Rootkit
  B. Spyware
  C. Adware
  D. Virus

This page intentionally left blank.

Review Questions (7)

- What is malware called that requires you to pay a fee to recover your data?
  A. Fee-Based Recovery malware
  B. Ransomware
  C. Ransom malware
  D. Monetary malware

- When anti-malware watches for malware-like activity, what is it called?
  A. Signature Analysis
  B. Heuristics
  C. Multipartite Analysis
  D. No anti-malware does this

This page intentionally left blank.

- Signature analysis works by
  A. Looking for a particular string unique to a piece of malware
  B. Watching virus-like activity
  C. Analyzing the data portion of a packet for maliciousness
  D. Analyzing the behavior of an application to see if it is behaving oddly

- What is the default configuration of the Mac Firewall?
  A. Blocks all incoming and outgoing traffic
  B. There is no firewall on Mac—it is not needed
  C. Disabled
  D. Enabled for limited traffic filtering

This page intentionally left blank.

Appendix

Answers to Review Questions

This page intentionally left blank.

Answers

SANS

Wireless Security
Review Question Answers

This page intentionally left blank.

- What is the encryption algorithm used in WPA2?
  A. RC4
  B. AES
  C. Diffie-Hellman
  D. Triple DES

- What is the single most important thing you can do to improve Wi-Fi security?
  A. Upgrade to WPA2
  B. Upgrade to WPA2
  C. Upgrade to WPA2
  D. Upgrade to WPA2

This page intentionally left blank.

- Why does antenna / transmitter strength matter in Wi-Fi?
  A. You will interfere with your neighbor's signal.
  B. Stronger antennas allow for stronger encryption keys.
  C. Antenna strength is a static value; it does not matter.
  D. Wi-Fi signals travel and can be intercepted outside your facility.

- What is the most common Bluetooth class and range?
  A. Class 1: 10 meters
  B. Class 2: 1 meter
  C. Class 3: 100 meters
  D. Class 1: 100 meters
  E. Class 2: 10 meters

This page intentionally left blank.

- In Bluetooth, what does SSP stand for?
  A. Super Simple Pairing
  B. Seriously Secure Pairing
  C. Secure Simple Pairing
  D. SSP is not a Bluetooth acronym

- Which encryption algorithm is used in SSP?
  A. Triple DES
  B. AES
  C. RC4
  D. MD5
  E. Diffie-Hellman

This page intentionally left blank.

- What is the most recent Wi-Fi standard released in January 2014?
  A. 802.11g
  B. 802.1i
  C. 802.11ac
  D. 802.11.n

- What is the current encryption specification for Wi-Fi?
  A. WEP
  B. WPA
  C. WPAN
  D. WPA2

This page intentionally left blank.

- If both Bluetooth devices have a screen to display a 6-digit number and can accept a yes/no response, which Association Model should you use?
  - A. Passkey Entry
  - **B. Numeric Comparison**
  - C. Out of Band (OOB)
  - D. Just Works

- What is the key exchange mechanism used by Secure Simple Paring?
  - A. Advanced Encryption Standard (AES)
  - B. Advanced Encryption Standard Diffie-Hellman (AESDH)
  - **C. Elliptic Curve Diffie-Hellman (ECDH)**
  - D. These do not use a secure key exchange mechanism

This page intentionally left blank.

Answers

Network Attacks vs. Security Topologies Review Question Answers

This page intentionally left blank.

- What are the five phases of an attack?
  A. Covering Tracks, Reconnaissance, Scanning, Gaining Access, Maintaining Access
  B. Covering Tracks, Maintaining Access, Gaining Access, Scanning, Reconnaissance
  C. Scanning, Reconnaissance, Gaining Access, Maintaining Access, Covering Tracks
  D. Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks
  E. Phishing, Access, Exfiltration, Public Posting, 6 o'clock news

- Which is the most common category of attack?
  A. Phishing
  B. Spear phishing
  C. Social engineering
  D. Ransomware

This page intentionally left blank.

- What is the URL of the Wayback Machine?
  - A. http://www.wayback.com
  - B. http://www.wayback.org
  - **C. http://www.archive.org**
  - D. http://www.sans.org/wayback

Where would you find the Google Dorks?

- **A. The Google Hacking Database**
- B. The Google Dorks Database
- C. The Googleist tip sheet
- D. The Google What's???

This page intentionally left blank.

- Is Spear Phishing an example of direct or indirect social engineering?
  - **A. Indirect**
  - B. Neither
  - C. Direct
  - D. Both

What does "A reason given in justification that is not the real reason" define?

- **A. Pretexting**
- B. Lying
- C. Manipulation
- D. Obfuscating

This page intentionally left blank.

- Hiding the real source IP address is commonly referred to as
  - A. IP Hiding
  - **B. IP Spoofing**
  - C. That is not possible
  - D. ARP Spoofing

- What does the acronym MitM stand for?
  - **A. Man-in-the-Middle**
  - B. Mission-Impossible-the-Movie
  - C. Missing Threat Management
  - D. Modern TCP Management

This page intentionally left blank.

- What is an attack against the availability of a system called?
  A. System Availability Denial (SAD)
  B. Availability attack
  C. Denial-of-Service (DoS)
  D. It has no formal name (IHNFN)

- Which is an attack that exploits the TCP three-way handshake?
  A. SYN Flood
  B. Handshake Flood
  C. DoS
  D. Zombie Flood

This page intentionally left blank.

Network Attacks

Review Questions (6)

- What are two names for the computers commonly used in Distributed Denial-of-Service attacks? (choose two)
  - A. Zombot
  - **B. Zombie**
  - **C. Bot**
  - D. DDoSer
- What are two names for the collection of machines commonly used in DDoS attacks? (choose two)
  - A. SYN Army
  - **B. Zombie Army**
  - C. DDoS Team
  - **D. Botnet**

This page intentionally left blank.

Answers

SANS

Malware and Anti-malware Review Question Answers

This page intentionally left blank.

Malware and Anti-malware

Review Questions (1)

- What is malware that is parasitic in nature called?
  - **A. Virus**
  - B. Worm
  - C. Trojan
  - D. Logic Bomb
- What is malware that is self-standing and self-propagating in nature called?
  - A. Virus
  - **B. Worm**
  - C. Trojan
  - D. Logic Bomb

This page intentionally left blank.

Review Questions (2)

- What is malware that waits for a preconfigured event or date to execute called?
  - A. Virus
  - B. Worm
  - C. Trojan
  - **D. Logic Bomb**

- What is malware that has a known desired function as well as an unknown undesired function called?
  - A. Virus
  - B. Worm
  - **C. Trojan**
  - D. Logic Bomb

This page intentionally left blank.

- What is the most common reason malware is created today?
  - **A. To make money for the author**
  - B. To prove that a virus can spread in a particular way
  - C. To destroy all of your data
  - D. Just because they can!

- What is malware that must insert itself into other executable code?
  - A. Logic Bomb
  - B. Trojan Horse
  - C. Worm
  - **D. Virus**

This page intentionally left blank.

Review Questions (4)

- In computing, what does the term *retrovirus* describe?
  - **A. Malware that attacks security software (antivirus, firewall, etc.)**
  - B. Malware that is self-modifying
  - C. That is a nonsense term
  - D. Malware that infects via multiple infection vectors

- What does the term *multipartite* describe?
  - A. Malware that is self-modifying
  - B. A trojan horse that is also a virus and a worm
  - **C. Malware that infects via multiple infection vectors**
  - D. A virus that divides itself into multiple parts to avoid detection

This page intentionally left blank.

- What does the term *polymorphic* describe?
  - A. A logic bomb with multiple triggers
  - **B. Malware that self-modifies to avoid detection**
  - C. A worm that can infect multiple types of systems
  - D. A virus that attacks both Windows and Mac operating systems

- Which of the following is most common?
  - A. Logic Bomb
  - **B. Trojan Horse**
  - C. Worm
  - D. Virus

This page intentionally left blank.

- What is malware that monitors and reports your online activity called?
  - A. Rootkit
  - **B. Spyware**
  - C. Adware
  - D. Virus

- What is malware that usually provides a backdoor and hides the attacker's activities from administrators called?
  - **A. Rootkit**
  - B. Spyware
  - C. Adware
  - D. Virus

This page intentionally left blank.

Malware and Anti-malware

Review Questions (7)

- What is malware called that requires you to pay a fee to recover your data?
  A. Fee-Based Recovery malware
  B. Ransomware
  C. Ransom malware
  D. Monetary malware

- When anti-malware watches for malware-like activity, what is it called?
  A. Signature Analysis
  B. Heuristics
  C. Multipartite Analysis
  D. No anti-malware does this

This page intentionally left blank.

Review Questions (9)

- Signature analysis works by
  - **A. <u>Looking for a particular string unique to a piece of malware</u>**
  - B. Watching virus-like activity
  - C. Analyzing the data portion of a packet for maliciousness
  - D. Analyzing the behavior of an application to see if it is behaving oddly
- What is the default configuration of the Mac Firewall?
  - A. Blocks all incoming and outgoing traffic
  - B. There is no firewall on Mac—it is not needed
  - **C. <u>Disabled</u>**
  - D. Enabled for limited traffic filtering

This page intentionally left blank.

Many of the slide graphics in this course are provided through a royalty-free license with PresentationPro. http://www.presentationpro.com/