Professor Messer

Professor Messer's

CompTIA SECURITY+

SY0-601

Course Notes

James "Professor" Messer

Professor Messer's SY0-601 CompTIA Security+ Course Notes

James "Professor" Messer

http://www.ProfessorMesser.com

Professor Messer's SY0-601 CompTIA Security+ Course Notes
Written by James "Professor" Messer

http://www.ProfessorMesser.com

First Edition: November 2020
This is version 1.02

Trademark Acknowledgments

Warning and Disclaimer
This book is designed to provide information about the CompTIA SY0-601 Security+ certification exam. However, there may be typographical and/or content errors. Therefore, this book should serve only as a general guide and not as the ultimate source of subject information. The author shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have incurred, directly or indirectly, by the information contained in this book.

Contents

Introduction

Information technology security is a significant concern for every IT specialist. Our systems are under constant attack, and the next generation of security professionals will be at the forefront of keeping our critical information safe.

CompTIA's Security+ exam tests you on the specifics of network security, vulnerabilities and threats, cryptography, and much more. I've created these Course Notes to help you through the details that you need to know for the exam. Best of luck with your studies!

- Professor Messer

The CompTIA Security+ certification

To earn the Security+ certification, you must pass a single SY0-601 certification exam. The exam is 90 minutes in duration and includes both multiple choice questions and performance-based questions. Performance-based questions can include fill-in-the-blank, matching, sorting, and simulated operational environments. You will need to be very familiar with the exam topics to have the best possible exam results.

Here's the breakdown of each technology section and the percentage of each topic on the SY0-601 exam:

Section 1.0 - Attacks, Threats, and Vulnerabilities - 24%
Section 2.0 - Architecture and Design - 21%
Section 3.0 - Implementation - 25%
Section 4.0 - Operations and Incident Response - 16%
Section 5.0 - Governance, Risk, and Compliance - 14%

CompTIA provides a detailed set of exam objectives that provide a list of everything you need to know before you take your exam. You can find a link to the exam objectives here:

https://professormesser.com/objectives/

How to use this book

Once you're comfortable with all of the sections in the official CompTIA SY0-601 exam objectives, you can use these notes as a consolidated summary of the most important topics. These Course Notes follow the same format and numbering scheme as the exam objectives, so it should be easy to cross reference these notes with the Professor Messer video series and all of your other study materials. The CompTIA Security+ video training series can be found on the Professor Messer website at https://ProfessorMesser.com.


Professor
Messer

Professor Messer's

CompTIA Security+

SY0-601 Course Notes

http://www.ProfessorMesser.com

1.1 - Phishing

Phishing

- Social engineering with a touch of spoofing
  - Often delivered by email, text, etc.
  - Very remarkable when well done
- Don't be fooled
  - Check the URL
- Usually there's something not quite right
  - Spelling, fonts, graphics

Tricks and misdirection

- How are they so successful?
  - Digital slight of hand - it fools the best of us
- Typosquatting
  - A type of URL hijacking - https://professormessor.com
  - Prepending: https://pprofessormesser.com
- Pretexting
  - Lying to get information
  - Attacker is a character in a situation they create
  - Hi, we're calling from Visa regarding an automated payment to your utility service…

Pharming

- Redirect a legit website to a bogus site
  - Poisoned DNS server or client vulnerabilities
- Combine pharming with phishing
  - Pharming - Harvest large groups of people
  - Phishing - Collect access credentials
- Difficult for anti-malware software to stop
  - Everything appears legitimate to the user

Phishing with different bait

- Vishing (Voice phishing) is done over the phone or voicemail
  - Caller ID spoofing is common
  - Fake security checks or bank updates
- Smishing (SMS phishing) is done by text message
  - Spoofing is a problem here as well
  - Forwards links or asks for personal information
- Variations on a theme
  - The fake check scam, phone verification code scam,
  - Boss/CEO scam, advance-fee scam
  - Some great summaries on https://reddit.com/r/Scams

Finding the best spot to phish

- Reconnaissance
  - Gather information on the victim
- Background information
  - Lead generation sites
  - LinkedIn, Twitter, Facebook, Instagram
  - Corporate web site
- Attacker builds a believable pretext
  - Where you work
  - Where you bank
  - Recent financial transactions
  - Family and friends

Spear phishing

- Targeted phishing with inside information
  - Makes the attack more believable
- Spear phishing the CEO is "whaling"
  - Targeted phishing with the possibility of a large catch
  - The CFO (Chief Financial Officer) is commonly speared
- These executives have direct access to the corporate bank account
  - The attackers would love to have those credentials

1.1 - Impersonation

The pretext

- Before the attack, the trap is set
  - There's an actor and a story
- "Hello sir, my name is Wendy and I'm from Microsoft Windows. This is an urgent check up call for your computer as we have found several problems with it."
- Voice mail: "This is an enforcement action executed by the US Treasury intending your serious attention."
- "Congratulations on your excellent payment history! You now qualify for 0% interest rates on all of your credit card accounts."

Impersonation

- Attackers pretend to be someone they aren't
  - Halloween for the fraudsters
- Use some of those details from reconnaissance
  - You can trust me, I'm with your help desk
- Attack the victim as someone higher in rank
  - Office of the Vice President for Scamming
- Throw tons of technical details around
  - Catastrophic feedback due to the depolarization of the differential magnetometer
- Be a buddy
  - How about those Cubs?

1.1 - Impersonation (continued)

Eliciting information
- Extracting information from the victim
  - The victim doesn't even realize this is happening
  - Hacking the human
- Often seen with vishing (Voice Phishing)
  - Can be easier to get this information over the phone
- These are well-documented psychological techniques
  - They can't just ask, "So, what's your password?"

Identity fraud
- Your identity can be used by others
  - Keep your personal information safe!
- Credit card fraud
  - Open an account in your name, or use your credit card information
- Bank fraud
  - Attacker gains access to your account or opens a new account
- Loan fraud
  - Your information is used for a loan or lease
- Government benefits fraud
  - Attacker obtains benefits on your behalf

Protect against impersonation
- Never volunteer information
  - My password is 12345
- Don't disclose personal details
  - The bad guys are tricky
- Always verify before revealing info
  - Call back, verify through 3rd parties
- Verification should be encouraged
  - Especially if your organization owns valuable information

1.1 - Dumpster Diving

Dumpster diving
- Mobile garbage bin
  - United States brand name "Dumpster"
  - Similar to a rubbish skip
- Important information thrown out with the trash
  - Thanks for bagging your garbage for me!
- Gather details that can be used for a different attack
  - Impersonate names, use phone numbers
- Timing is important
  - Just after end of month, end of quarter
  - Based on pickup schedule

Is it legal to dive in a dumpster?
- I am not a lawyer.
  - In the United States, it's legal
  - Unless there's a local restriction
- If it's in the trash, it's open season
  - Nobody owns it
- Dumpsters on private property or "No Trespassing" signs may be restricted
  - You can't break the law to get to the rubbish
- Questions? Talk to a legal professional.

Protect your rubbish
- Secure your garbage
  - Fence and a lock
- Shred your documents
  - This will only go so far
  - Governments burn the good stuff
- Go look at your trash
  - What's in there?

1.1 - Shoulder Surfing

Shoulder surfing
- You have access to important information
  - Many people want to see
  - Curiosity, industrial espionage, competitive advantage
- This is surprisingly easy
  - Airports / Flights
  - Hallway-facing monitors
  - Coffee shops
- Surf from afar
  - Binoculars / Telescopes
  - Easy in the big city
  - Webcam monitoring

- **Preventing shoulder surfing**
- Control your input
  - Be aware of your surroundings
- Use privacy filters
  - It's amazing how well they work
- Keep your monitor out of sight
  - Away from windows and hallways
- Don't sit in front of me on your flight
  - I can't help myself

1.1 - Hoaxes

Computer hoaxes

- A threat that doesn't actually exist
  - But they seem like they COULD be real
- Still often consume lots of resources
  - Forwarded email messages, printed memorandums, wasted time
- Often an email
  - Or Facebook wall post, or tweet, or...
- Some hoaxes will take your money
  - But not through electronic means
- A hoax about a virus can waste as much time as a regular virus

De-hoaxing

- It's the Internet. Believe no one.
  - Consider the source
- Cross reference
  - http://www.hoax-slayer.net
  - http://www.snopes.com
- Spam filters can help
  - There are so many other ways...
- If it sounds too good to be true...
  - So many sad stories

1.1 - Watering Hole Attacks

Watering Hole Attack

- What if your network was really secure?
  - You didn't even plug in that USB key from the parking lot
- The attackers can't get in
  - Not responding to phishing emails
  - Not opening any email attachments
- Have the mountain come to you
  - Go where the mountain hangs out
  - The watering hole
  - This requires a bit of research

Executing the watering hole attack

- Determine which website the victim group uses
  - Educated guess - Local coffee or sandwich shop
  - Industry-related sites
- Infect one of these third-party sites
  - Site vulnerability
  - Email attachments
- Infect all visitors
  - But you're just looking for specific victims
  - Now you're in!

Because that's where the money is

- January 2017
- Polish Financial Supervision Authority, National Banking and Stock Commission of Mexico, State-owned bank in Uruguay
  - The watering hole was sufficiently poisoned
- Visiting the site would download malicious JavaScript files
  - But only to IP addresses matching banks and other financial institutions
- Did the attack work?
  - We still don't know

Watching the watering hole

- Defense-in-depth
  - Layered defense
  - It's never one thing
- Firewalls and IPS
  - Stop the network traffic before things get bad
- Anti-virus / Anti-malware signature updates
  - The Polish Financial Supervision Authority attack code was recognized and stopped by generic signatures in Symantec's anti-virus software

1.1 - Spam

Spam

- Unsolicited messages
  - Email, forums, etc.
  - Spam over Instant Messaging (SPIM)
- Various content
  - Commercial advertising
  - Non-commercial proselytizing
  - Phishing attempts
- Significant technology issue
  - Security concerns
  - Resource utilization
  - Storage costs
  - Managing the spam

Mail gateways

- Unsolicited email
  - Stop it at the gateway before it reaches the user
  - On-site or cloud-based

Identifying spam

- Allowed list
  - Only receive email from trusted senders
- SMTP standards checking
  - Block anything that doesn't follow RFC standards
- rDNS - Reverse DNS
  - Block email where the sender's domain doesn't match the IP address
- Tarpitting
  - Intentionally slow down the server conversation
- Recipient filtering
  - Block all email not addressed to a valid recipient email address

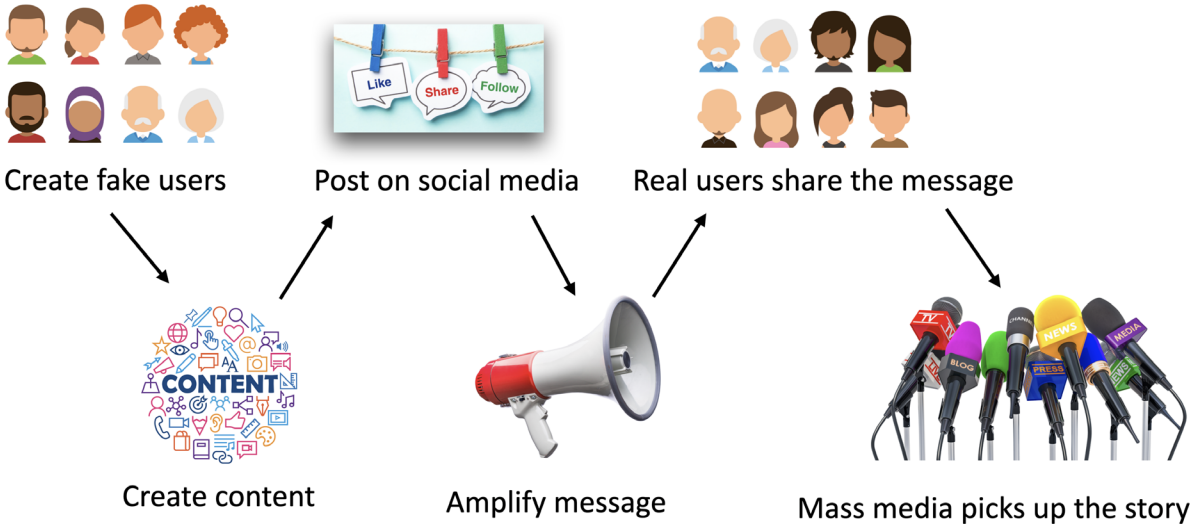
1.1 - Influence Campaigns

Hacking public opinion

- Influence campaigns
  - Sway public opinion on political and social issues
- Nation-state actors
  - Divide, distract, and persuade
- Advertising is an option
  - Buy a voice for your opinion
- Enabled through Social media
  - Creating, sharing, liking
  - Amplification

Hybrid warfare

- Military strategy
  - A broad description of the techniques
  - Wage war non-traditionally
- Not a new concept
  - The Internet adds new methods
- Cyberwarfare
  - Attack an entity with technology
- Influence with a military spin
  - Influencing foreign elections
  - "Fake news"



1.1 - Other Social Engineering Attacks

Tailgating

- Use an authorized person to gain unauthorized access to a building
  - Not an accident
- Johnny Long / No Tech Hacking
  - Blend in with clothing
  - 3rd-party with a legitimate reason
  - Temporarily take up smoking
  - I still prefer bringing doughnuts
- Once inside, there's little to stop you
  - Most security stops at the border

Watching for tailgating

- Policy for visitors
  - You should be able to identify anyone
- One scan, one person
  - A matter of policy or mechanically required
- Mantrap / Airlock
  - You don't have a choice
- Don't be afraid to ask
  - Who are you and why are you here?

Invoice scams

- Starts with a bit of spear phishing
  - Attacker knows who pays the bills
- Attacker sends a fake invoice
  - Domain renewal, toner cartridges, etc.
  - From: address is a spoofed version of the CEO
- Accounting pays the invoice
  - It was from the CEO, after all
- Might also include a link to pay
  - Now the attacker has payment details

Credential harvesting

- Also called password harvesting
  - Attackers collect login credentials
- There are a lot of stored credentials on your computer
  - The attacker would like those
  - Chrome, Firefox, Outlook, Windows Credential Manager, etc.
- User receives an email with a malicious Microsoft Word doc
  - Opening the document runs a macro
  - The macro downloads credential-harvesting malware
- User has no idea
  - Everything happens in the background

1.1 - Principles of Social Engineering

Effective social engineering

- Constantly changing
  - You never know what they'll use next
- May involve multiple people
  - And multiple organizations
  - There are ties connecting many organizations
- May be in person or electronic
  - Phone calls from aggressive "customers"
  - Emailed funeral notifications of a friend or associate

Social engineering principles

- Authority
  - The social engineer is in charge
  - I'm calling from the help desk/office of the CEO/police
- Intimidation
  - There will be bad things if you don't help
  - If you don't help me, the payroll checks won't be processed
- Consensus / Social proof
  - Convince based on what's normally expected
  - Your co-worker Jill did this for me last week
- Scarcity
  - The situation will not be this way for long
  - Must make the change before time expires
- Urgency
  - Works alongside scarcity
  - Act quickly, don't think
- Familiarity / Liking
  - Someone you know, we have common friends
- Trust
  - Someone who is safe
  - I'm from IT, and I'm here to help

How I Lost My $50,000 Twitter Username

- Naoki Hiroshima - @N
  - https://professormesser.link/twittername
- Attacker calls PayPal and uses social engineering to get the last four digits of the credit card on file
- Attacker calls GoDaddy and tells them he lost the card, so he can't properly validate. But he has the last four, does that help?
  - GoDaddy let the bad guy guess the first two digits of the card
  - He was allowed to keep guessing until he got it right
  - Social engineering done really, really well

How to steal a $50,000 Twitter name

- Attacker is now in control of every domain name
  - And there were some good ones
- Attacker extorts a swap
  - Domain control for @N
  - Owner agrees
- Twitter reviewed the case for a month
  - Eventually restored access to @N
- How I Lost My $50,000 Twitter Username
  - https://professormesser.link/twittername

1.2 - An Overview of Malware

Malware

- Malicious software
  - These can be very bad
- Gather information
  - Keystrokes
- Participate in a group
  - Controlled over the 'net
- Show you advertising
  - Big money
- Viruses and worms
  - Encrypt your data
  - Ruin your day

Malware Types and Methods

- Viruses
- Crypto-malware
- Ransomware
- Worms
- Trojan Horse
- Rootkit
- Keylogger
- Adware/Spyware
- Botnet

How you get malware

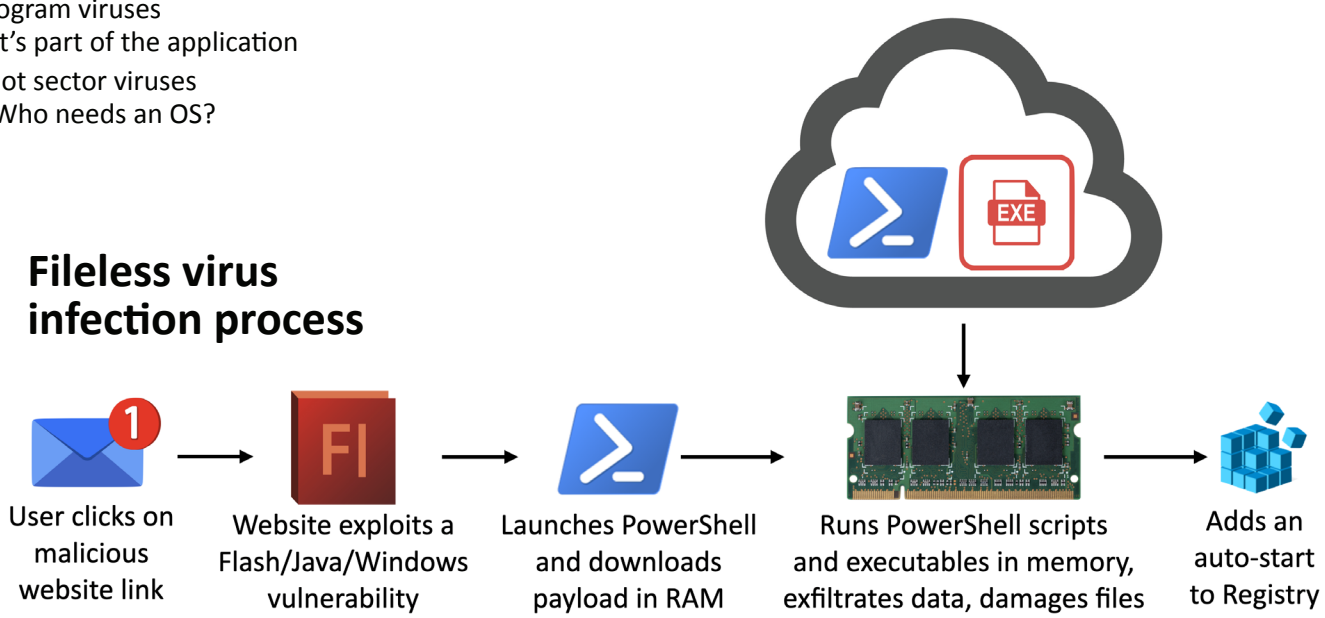
- These all work together
  - A worm takes advantage of a vulnerability
  - Installs malware that includes a remote access backdoor
  - Bot may be installed later
- Your computer must run a program
  - Email link - Don't click links
  - Web page pop-up
  - Drive-by download
  - Worm
- Your computer is vulnerable
  - Operating system - Keep your OS updated!
  - Applications - Check with the publisher

1.2 - Viruses and Worms

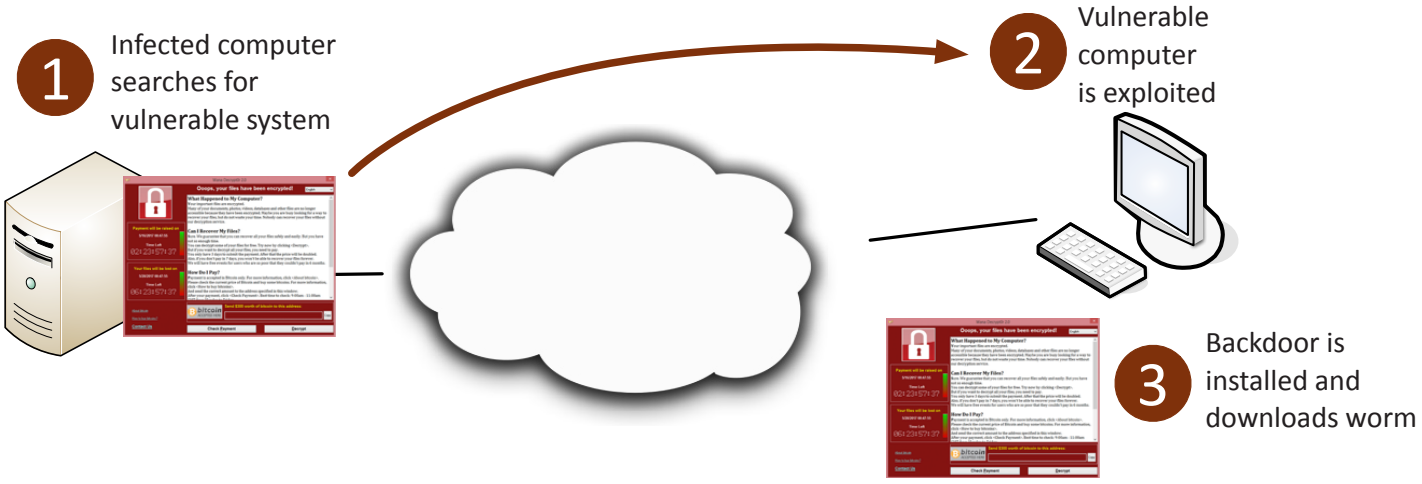
Virus
- Malware that can reproduce itself
  - It needs you to execute a program
- Reproduces through file systems or the network
  - Just running a program can spread a virus
- May or may not cause problems
  - Some viruses are invisible, some are annoying
- Anti-virus is very common
  - Thousands of new viruses every week
  - Is your signature file updated?

Virus types
- Program viruses
  - It's part of the application
- Boot sector viruses
  - Who needs an OS?
- Script viruses
  - Operating system and browser-based
- Macro viruses
  - Common in Microsoft Office

Fileless virus
- A stealth attack
  - Does a good job of avoiding anti-virus detection
- Operates in memory
  - But never installed in a file or application



Worms
- Malware that self-replicates
  - Doesn't need you to do anything
  - Uses the network as a transmission medium
  - Self-propagates and spreads quickly
- Worms are pretty bad things
  - Can take over many systems very quickly
- Firewalls and IDS/IPS can mitigate many worm infestations
  - Doesn't help much once the worm gets inside



1.2 - Ransomware and Crypto-malware

Your data is valuable
- Personal data
  - Family pictures and videos
  - Important documents
- Organization data
  - Planning documents
  - Employee personally identifiable information (PII)
  - Financial information
  - Company private data
- How much is it worth?
  - There's a number

Ransomware
- The attackers want your money
  - They'll take your computer in the meantime
- May be a fake ransom
  - Locks your computer "by the police"
- The ransom may be avoided
  - A security professional may be able to remove these kinds of malware

Crypto-malware
- A newer generation of ransomware
  - Your data is unavailable until you provide cash
- Malware encrypts your data files
  - Pictures, documents, music, movies, etc.
  - Your OS remains available
  - They want you running, but not working
- You must pay the bad guys to obtain the decryption key
  - Untraceable payment system
  - An unfortunate use of public-key cryptography

Protecting against ransomware
- Always have a backup
  - An offline backup, ideally
- Keep your operating system up to date
  - Patch those vulnerabilities
- Keep your applications up to date
  - Security patches
- Keep your anti-virus/anti-malware signatures up to date
  - New attacks every hour
- Keep everything up to date

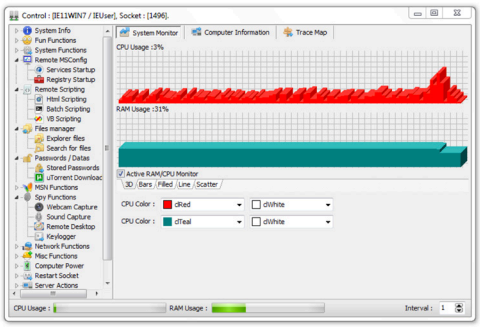
1.2 - Trojans and RATs

Trojan horse
- Used by the Greeks to capture
  - Troy from the Trojans
  - A digital wooden horse
- Software that pretends to be something else
  - So it can conquer your computer
  - Doesn't really care much about replicating
- Circumvents your existing security
  - Anti-virus may catch it when it runs
  - The better Trojans are built to avoid and disable AV
- Once it's inside it has free reign
  - And it may open the gates for other programs

Potentially Unwanted Program (PUP)
- Identified by anti-virus/anti-malware
  - Potentially undesirable software
  - Often installed along with other software
- Overly aggressive browser toolbar
- A backup utility that displays ads
- Browser search engine hijacker

Backdoors
- Why go through normal authentication methods?
  - Just walk in the back door
- Often placed on your computer through malware
  - Some malware software can take advantage of backdoors created by other malware
- Some software includes a backdoor (oops)
  - Old Linux kernel included a backdoor
  - Bad software can have a backdoor as part of the app

Remote Access Trojans (RATs)
- Remote Administration Tool
  - The ultimate backdoor
  - Administrative control of a device
- Malware installs the server/service/host
  - Attacker connects with the client software
- Control a device
  - Key logging
  - Screen recording /screenshots
  - Copy files
  - Embed more malware



Protecting against Trojans and RATs
- Don't run unknown software
  - Consider the consequences
- Keep anti-virus/anti-malware signatures updated
  - There are always new attacks
- Always have a backup
  - You may need to quickly recover

1.2 - Rootkits

Rootkits

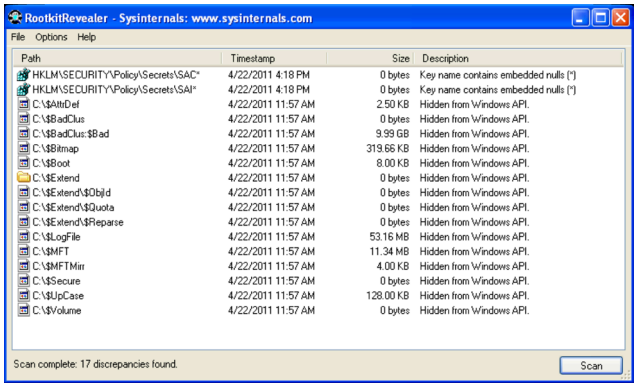
- Originally a Unix technique
  - The "root" in rootkit
- Modifies core system files
  - Part of the kernel
- Can be invisible to the operating system
  - Won't see it in Task Manager
- Also invisible to traditional anti-virus utilities
  - If you can't see it, you can't stop it

Kernel drivers

- Zeus/Zbot malware
  - Famous for cleaning out bank accounts
- Now combined with Necurs rootkit
  - Necurs is a kernel-level driver
- Necurs makes sure you can't delete Zbot
  - Access denied
- Trying to stop the Windows process?
  - Error terminating process: Access denied

Finding and removing rootkits

- Look for the unusual
  - Anti-malware scans
- Use a remover specific to the rootkit
  - Usually built after the rootkit is discovered
- Secure boot with UEFI
  - Security in the BIOS



1.2 - Spyware

Adware

- Your computer is one big advertisement
  - Pop-ups with pop-ups
- May cause performance issues
  - Especially over the network
- Installed accidentally
  - May be included with other software
- Be careful of software that claims to remove adware
  - Especially if you learned about it from a pop-up

Spyware

- Malware that spies on you
  - Advertising, identity theft, affiliate fraud
- Can trick you into installing
  - Peer to peer, fake security software
- Browser monitoring
  - Capture surfing habits
- Keyloggers - Capture every keystroke
  - Send it back to the mother ship

Why is there so much adware and spyware?

- Money
  - Your eyeballs are incredibly valuable
- Money
  - Your computer time and bandwidth is incredibly valuable
- Money
  - Your bank account is incredibly valuable
  - Yes, even your bank account

Protecting against adware/spyware

- Maintain your anti-virus / anti-malware
  - Always have the latest signatures
- Always know what you're installing
  - And watch your options during the installation
- Where's your backup?
  - You might need it someday
  - Cleaning adware isn't easy
- Run some scans - Malwarebytes

1.2 - Bots and Botnets

Bots (Robots)

- Once your machine is infected, it becomes a bot
  - You may not even know
- How does it get on your computer?
  - Trojan Horse (I just saw a funny video of you! Click here.) or...
  - You run a program or click an ad you THOUGHT was legit, but...
  - OS or application vulnerability
- A day in the life of a bot
  - Sit around. Check in with the Command and Control (C&C) server. Wait for instructions.

Botnets

- A group of bots working together
  - Nothing good can come from this
- Distributed Denial of service (DDoS)
  - The power of many
- Relay spam, proxy network traffic, distributed computing tasks
- Botnets are for sale
  - Rent time from the botnet owner
  - Not a long-term business proposition

1.2 - Bots and Botnets (continued)

Stopping the bot

- Prevent the initial infection
  - OS and application patches
  - Anti-virus/anti-malware and updated signatures
- Identify an existing infection
  - On-demand scans, network monitoring
- Prevent command and control (C&C)
  - Block at the firewall
  - Identify at the workstation with a host-based firewall or host-based IPS

1.2 - Logic Bombs

Logic Bomb

- Waits for a predefined event
  - Often left by someone with grudge
- Time bomb
  - Time or date
- User event
  - Logic bomb
- Difficult to identify
  - Difficult to recover if it goes off

Real-world logic bombs

- March 19, 2013, South Korea
  - Email with malicious attachment sent to
  - South Korean organizations
  - Posed as a bank email
  - Trojan installs malware
- March 20, 2013, 2 p.m. local time
  - Malware time-based logic-bomb activates
  - Storage and master boot record deleted, system reboots
  - Boot device not found.
  - Please install an operating system on your hard disk.
- December 17, 2016, 11:53 p.m.
  - Kiev, Ukraine, high-voltage substation
  - Logic bomb begins disabling electrical circuits
  - Malware mapped out the control network
  - Began disabling power at a predetermined time
  - Customized for SCADA networks (Supervisory Control and Data Acquisition)

Preventing a logic bomb

- Difficult to recognize
  - Each is unique
  - No predefined signatures
- Process and procedures
  - Formal change control
- Electronic monitoring
  - Alert on changes
  - Host-based intrusion detection, Tripwire, etc.
- Constant auditing
  - An administrator can circumvent existing systems

1.2 - Password Attacks

Plaintext / unencrypted passwords

- Some applications store passwords “in the clear”
  - No encryption. You can read the stored password.
  - This is rare, thankfully
- Do not store passwords as plaintext
  - Anyone with access to the password file or database has every credential
- What to do if your application saves passwords as plaintext:
  - Get a better application

Hashing a password

- Hashes represent data as a fixed-length string of text
  - A message digest, or “fingerprint”
- Will not have a collision (hopefully)
  - Different inputs will not have the same hash
- One-way trip
  - Impossible to recover the original message from the digest
  - A common way to store passwords

The password file

- Different across operating systems and applications
  - Different hash algorithms

Linux Account Hashes

```
Jumper Bay:1001::42e2f19c31c9ff73cb97eb1b26c10f54:::
Carter:1007::cf4eb977a6859c76efd21f5094ecf77d:::
Jackson:1008::e1f757d9cdc06690509e04b5446317d2:::
O’Neill:1009::78a8c423faedd2f002c6aef69a0ac1af:::
Teal’c:1010::bf84666c81974686e50d300bc36aea01:::
```

1.2 - Password Attacks (continued)

Spraying attack
- Try to login with an incorrect password
  - Eventually you're locked out
- There are some common passwords
  - https://en.wikipedia.org/wiki/List_of_the_most_common_passwords
- Attack an account with the top three (or more) passwords
  - If they don't work, move to the next account
  - No lockouts, no alarms, no alerts

Brute force
- Try every possible password combination until the a hash is matched
- This might take some time
  - A strong hashing algorithm slows things down
- Brute force attacks - Online
  - Keep trying the login process
  - Very slow
  - Most accounts will lockout after a number of failed attempts
- Brute force the hash - Offline
  - Obtain the list of users and hashes
  - Calculate a password hash, compare it to a stored hash
  - Large computational resource requirement

Dictionary attacks
- Use a dictionary to find common words
  - Passwords are created by humans
- Many common wordlists available on the 'net
  - Some are customized by language or line of work
- The password crackers can substitute letters
  - p&ssw0rd
- This takes time
  - Distributed cracking and GPU cracking is common
- Discover passwords for common words
  - This won't discover random character passwords

Rainbow tables
- An optimized, pre-built set of hashes
  - Saves time and storage space
  - Doesn't need to contain every hash
  - Contains pre-calculated hash chains
- Remarkable speed increase
  - Especially with longer password lengths
- Need different tables for different hashing methods
  - Windows is different than MySQL

Adding some salt
- Salt
  - Random data added to a password when hashing
- Every user gets their own random salt
  - The salt is commonly stored with the password
- Rainbow tables won't work with salted hashes
  - Additional random value added to the original password
- This slows things down the brute force process
  - It doesn't completely stop the reverse engineering
- Each user gets a different random hash
  - The same password creates a different hash

When the hashes get out
- January 2019 - Collection #1
  - A collection of email addresses and passwords
  - 12,000+ files and 87 GB of data
- 1,160,253,228 unique emails and passwords
  - A compilation of data breach results
- 772,904,991 unique usernames
  - That's about 773 million people
- 21,222,975 unique passwords
  - You really need a password manager
- https://haveibeenpwned.com/

1.2 - Physical Attacks

Malicious USB cable
- It looks like a normal USB cable
  - It has additional electronics inside
- Operating system identifies it as a HID
  - Human Interface Device
  - It looks like you've connected a keyboard or mouse
  - A keyboard doesn't need extra rights or permissions
- Once connected, the cable takes over
  - Downloads and installs malicious software
- Don't just plug in any USB cable
  - Always use trusted hardware

Malicious flash drive
- Free USB flash drive!
  - Plug it in and see what's on it
  - That's a bad idea
- Older operating systems would automatically run files
  - This has now been disabled or removed by default
- Could still act as a HID (Human Interface Device) / Keyboard
  - Start a command prompt and type anything without your intervention
- Attackers can load malware in documents
  - PDF files, spreadsheets
- Can be configured as a boot device
  - Infect the computer after a reboot
- Acts as an Ethernet adapter
  - Redirects or modifies Internet traffic requests
  - Acts as a wireless gateway for other devices
- Never connect an untrusted USB device

1.2 - Physical attacks (continued)

Skimming

- Stealing credit card information, usually during a normal transaction
  - Copy data from the magnetic stripe:
  - Card number, expiration date, card holder's name
- ATM skimming
  - Includes a small camera to also watch for your PIN
- Attackers use the card information for other financial transactions
  - Fraud is the responsibility of the seller
- Always check before using card readers

Card cloning

- Get card details from a skimmer
  - The clone needs an original
- Create a duplicate of a card
  - Looks and feels like the original
  - Often includes the printed CVC (Card Validation Code)
- Can only be used with magnetic stripe cards
  - The chip can't be cloned
- Cloned gift cards are common
  - A magnetic stripe technology

1.2 - Adversarial Artificial Intelligence

Machine learning

- Our computers are getting smarter
  - They identify patterns in data and improve their predictions
- This requires a lot of training data
  - Face recognition requires analyzing a lot of faces
  - Driving a car requires a lot of road time
- In use every day
  - Stop spam
  - Recommend products from an online retailer
  - What movie would you like to see? This one.
  - Prevent car accidents

Poisoning the training data

- Confuse the artificial intelligence (AI)
  - Attackers send modified training data that causes the AI to behave incorrectly
- Microsoft AI chatter bot named Tay
- (Thinking About You)
  - Joins Twitter on March 23, 2016
  - Designed to learn by interacting with Twitter users
  - Microsoft didn't program in anti-offensive behavior
  - Tay quickly became racist, sexist, and inappropriate

Evasion attacks

- The AI is only as good as the training
  - Attackers find the holes and limitations
- An AI that knows what spam looks like can be fooled by a different approach
  - Change the number of good and bad words in the message
- An AI that uses real-world information can release confidential information
  - Trained with data that includes social security numbers
  - AI can be fooled into revealing those numbers

Securing the learning algorithms

- Check the training data
  - Cross check and verify
- Constantly retrain with new data
  - More data
  - Better data
- Train the AI with possible poisoning
  - What would the attacker try to do?

1.2 - Supply Chain Attacks

Supply chain

- The chain contains many moving parts
  - Raw materials, suppliers, manufacturers, distributors, customers, consumers
- Attackers can infect any step along the way
  - Infect different parts of the chain without suspicion
  - People trust their suppliers
- One exploit can infect the entire chain
  - There's a lot at stake

Supply chain security

- Target Corp. breach - November 2013
  - 40 million credit cards stolen
- Heating and AC firm in Pennsylvania was infected
  - Malware delivered in an email
  - VPN credentials for HVAC techs was stolen
- HVAC vendor was the supplier
  - Attackers used a wide-open Target network to infect every cash register at 1,800 stores
- Do these technicians look like an IT security issue?

Supply chain security

- Can you trust your new server/router/switch/firewall/software?
  - Supply chain cybersecurity
- Use a small supplier base
  - Tighter control of vendors
- Strict controls over policies and procedures
  - Ensure proper security is in place
- Security should be part of the overall design
  - There's a limit to trust

1.2 - Cloud-based vs. On-Premises Attacks

Attacks can happen anywhere

- Two categories for IT security
  - The on-premises data is more secure!
  - The cloud-based data is more secure!
- Cloud-based security is centralized and costs less
  - No dedicated hardware, no data center to secure
  - A third-party handles everything
- On-premises puts the security burden on the client
  - Data center security and infrastructure costs
- Attackers want your data
  - They don't care where it is

On-premises security

- Customize your security posture
  - Full control when everything is in-house
- On-site IT team can manage security better
  - The local team can ensure everything is secure
  - A local team can be expensive and difficult to staff
- Local team maintains uptime and availability
  - System checks can occur at any time
  - No phone call for support
- Security changes can take time
  - New equipment, configurations, and additional costs

Security in the cloud

- Data is in a secure environment
  - No physical access to the data center
  - Third-party may have access to the data
- Cloud providers are managing large-scale security
  - Automated signature and security updates
  - Users must follow security best-practices
- Limited downtime
  - Extensive fault-tolerance and 24/7/365 monitoring
- Scalable security options
  - One-click security deployments
  - This may not be as customizable as necessary

1.2 - Cryptographic Attacks

Cryptographic attacks

- You've encrypted data and sent it to another person
  - Is it really secure? How do you know?
- The attacker doesn't have the combination (the key)
  - So they break the safe (the cryptography)
- Finding ways to undo the security
  - There are many potential cryptographic shortcomings
  - The problem is often the implementation

Birthday attack

- In a classroom of 23 students, what is the chance of two students sharing a birthday? About 50%.
  - For a class of 30, the chance is about 70%
- In the digital world, this is a hash collision
  - A hash collision is the same hash value for two different plaintexts
  - Find a collision through brute force
- The attacker will generate multiple versions of plaintext to match the hashes
  - Protect yourself with a large hash output size

Collisions

- Hash digests are supposed to be unique
  - Different input data should never create the same hash
- MD5 hash
  - Message Digest Algorithm 5
  - Published in April 1992, Collisions identified in 1996
- December 2008: Researchers created CA certificate that appeared legitimate when MD5 is checked
  - Built other certificates that appeared to be legit and issued by RapidSSL

Downgrade attack

- Instead of using perfectly good encryption, use something that's not so great
  - Force the systems to downgrade their security
- 2014 - TLS vulnerability - POODLE (Padding Oracle On Downgraded Legacy Encryption)
  - On-path attack
  - Forces clients to fall back to SSL 3.0
  - SSL 3.0 has significant cryptographic vulnerabilities
  - Because of POODLE, modern browsers won't fall back to SSL 3.0

1.3 - Privilege escalation

Privilege escalation

- Gain higher-level access to a system
  - Exploit a vulnerability - Might be a bug or design flaw
- Higher-level access means more capabilities
  - This commonly is the highest-level access
  - This is obviously a concern
- These are high-priority vulnerability patches
  - You want to get these holes closed very quickly
  - Any user can be an administrator
- Horizontal privilege escalation
  - User A can access user B resources

Mitigating privilege escalation

- Patch quickly
  - Fix the vulnerability
- Updated anti-virus/anti-malware software
  - Block known vulnerabilities
- Data Execution Prevention
  - Only data in executable areas can run
- Address space layout randomization
  - Prevent a buffer overrun at a known memory address

1.3 - Cross-site Scripting

Cross-site scripting
- XSS
  - Cascading Style Sheets (CSS) are something else entirely
- Originally called cross-site because of browser security flaws
  - Information from one site could be shared with another
- One of the most common web application development errors
  - Takes advantage of the trust a user has for a site
  - Complex and varied
- Malware that uses JavaScript - Do you allow scripts? Me too.

Non-persistent (reflected) XSS attack
- Web site allows scripts to run in user input
  - Search box is a common source
- Attacker emails a link that takes advantage of this vulnerability
  - Runs a script that sends credentials/session IDs/cookies to the attacker
- Script embedded in URL executes in the victim's browser
  - As if it came from the server
- Attacker uses credentials/session IDs/cookies to steal victim's information without their knowledge
  - Very sneaky

Persistent (stored) XSS attack
- Attacker posts a message to a social network
  - Includes the malicious payload
- It's now "persistent" - Everyone gets the payload
- No specific target - All viewers to the page
- For social networking, this can spread quickly
  - Everyone who views the message can have it posted to their page
  - Where someone else can view it and propagate it further...

Hacking a Subaru
- June 2017, Aaron Guzman
  - Security researcher
- When authenticating with Subaru, users get a token
  - This token never expires (bad!)
- A valid token allowed any service request
  - Even adding your email address to someone else's account
  - Now you have full access to someone else's car
- Web front-end included an XSS vulnerability
  - A user clicks a malicious link, and you have their token

Protecting against XSS
- Be careful when clicking untrusted links
  - Never blindly click in your email inbox. Never.
- Consider disabling JavaScript
  - Or control with an extension
  - This offers limited protection
- Keep your browser and applications updated
  - Avoid the nasty browser vulnerabilities
- Validate input
  - Don't allow users to add their own scripts to an input field

1.3 - Injection Attacks

Code injection
- Code injection
  - Adding your own information into a data stream
- Enabled because of bad programming
  - The application should properly handle input and output
- So many different data types
  - HTML, SQL, XML, LDAP, etc.

SQL injection
- SQL - Structured Query Language
  - The most common relational database management system language
- SQL Injection
  - Modifying SQL requests
  - Your application shouldn't really allow this

XML injection and LDAP injection
- XML - Extensible Markup Language
  - A set of rules for data transfer and storage
- XML injection
  - Modifying XML requests - a good application will validate
- LDAP - Lightweight Directory Access Protocol
  - Created by the telephone companies
  - Now used by almost everyone
- LDAP injection
  - Modify LDAP requests to manipulate application results

DLL injection
- Dynamic-Link Library
  - A Windows library containing code and data
  - Many applications can use this library
- Inject a DLL and have an application run a program
  - Runs as part of the target process

1.3 - Buffer Overflows

Buffer overflows

- Overwriting a buffer of memory
  - Spills over into other memory areas
- Developers need to perform bounds checking
  - The attackers spend a lot of time looking for openings
- Not a simple exploit
  - Takes time to avoid crashing things
  - Takes time to make it do what you want
- A really useful buffer overflow is repeatable
  - Which means that a system can be compromised

Variable A and B before buffer overflow

Variable Name	A								B	
Value	[null string]								1979	
Hex Value	00	00	00	00	00	00	00	00	07	BB

Overflowing variable A changes variable B

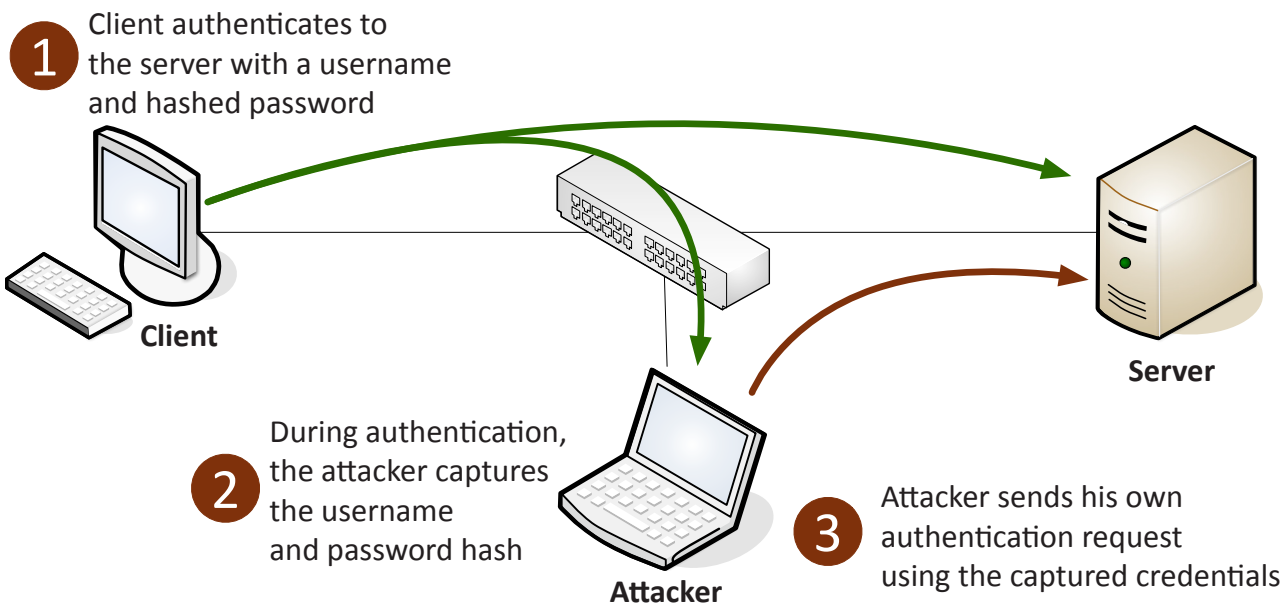
Variable Name	A								B	
Value	'e'	'x'	'c'	'e'	's'	's'	'i'	'v'	25856	
Hex Value	65	78	63	65	73	73	69	76	65	00

1.3 - Replay Attacks

Replay attack

- Useful information is transmitted over the network
  - A crafty hacker will take advantage of this
- Need access to the raw network data
  - Network tap, ARP poisoning, malware on the victim computer
- The gathered information may help the attacker
  - Replay the data to appear as someone else
- This is not an on-path attack
  - The actual replay doesn't require the original workstation
- Avoid this type of replay attack with a salt
  - Use a session ID with the password hash to create a unique authentication hash each time

Pass the Hash



Header manipulation

- Information gathering
  - Wireshark, Kismet
- Exploits
  - Cross-site scripting
- Modify headers
  - Tamper, Firesheep, Scapy
- Modify cookies
  - Cookies Manager+ (Firefox add-on)

Prevent session hijacking

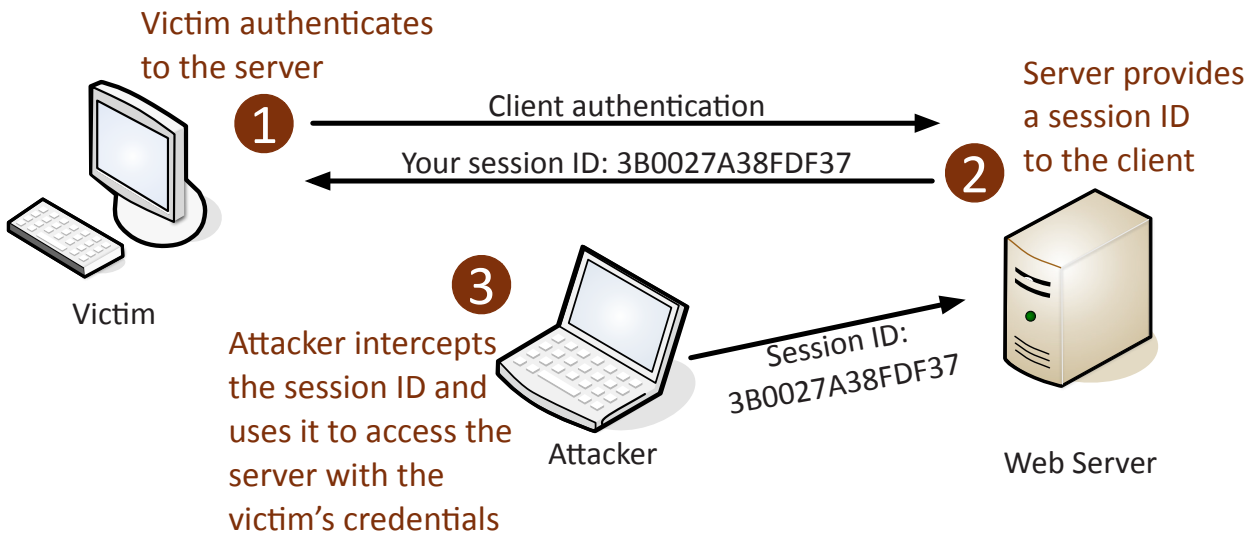
- Encrypt end-to-end
  - They can't capture your session ID if they can't see it
  - Additional load on the web server (HTTPS)
  - Firefox extension: HTTPS Everywhere, Force-TLS
  - Many sites are now HTTPS-only
- Encrypt end-to-somewhere
  - At least avoid capture over a local wireless network
  - Still in-the-clear for part of the journey
  - Personal VPN (OpenVPN, VyprVPN, etc.)

1.3 - Replay Attacks (continued)

Browser cookies and session IDs

- Cookies
  - Information stored on your computer by the browser
- Used for tracking, personalization, session management
  - Not executable, not generally a security risk
  - Unless someone gets access to them
- Could be considered be a privacy risk
  - Lots of personal data in there
- Session IDs are often stored in the cookie
  - Maintains sessions across multiple browser sessions

Session hijacking (Sidejacking)



1.3 - Request Forgeries

Cross-site requests

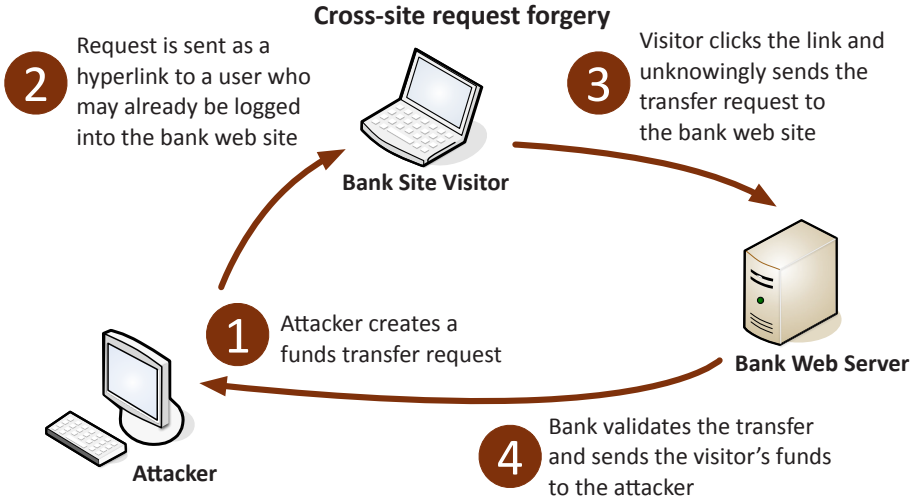
- Cross-site requests are common and legitimate
  - You visit ProfessorMesser.com
  - Your browser loads text from the ProfessorMesser.com server
  - Your browser loads a video from YouTube
  - Your browser loads pictures from Instagram
- HTML on ProfessorMesser.com directs requests from your browser
  - This is normal and expected
  - Most of these are unauthenticated requests

The client and the server

- Website pages consist of client-side code and server-side code
  - Many moving parts
- Client side
  - Renders the page on the screen
  - HTML, JavaScript
- Server side
  - Performs requests from the client - HTML, PHP
  - Transfer money from one account to another
  - Post a video on YouTube

Cross-site request forgery

- One-click attack, session riding - XSRF, CSRF (sea surf)
- Takes advantage of the trust that a web application has for the user
  - The web site trusts your browser
  - Requests are made without your consent or your knowledge
  - Attacker posts a Facebook status on your account
- Significant web application development oversight
  - The application should have anti-forgery techniques added
  - Usually a cryptographic token to prevent a forgery



1.3 - Request Forgeries (continued)

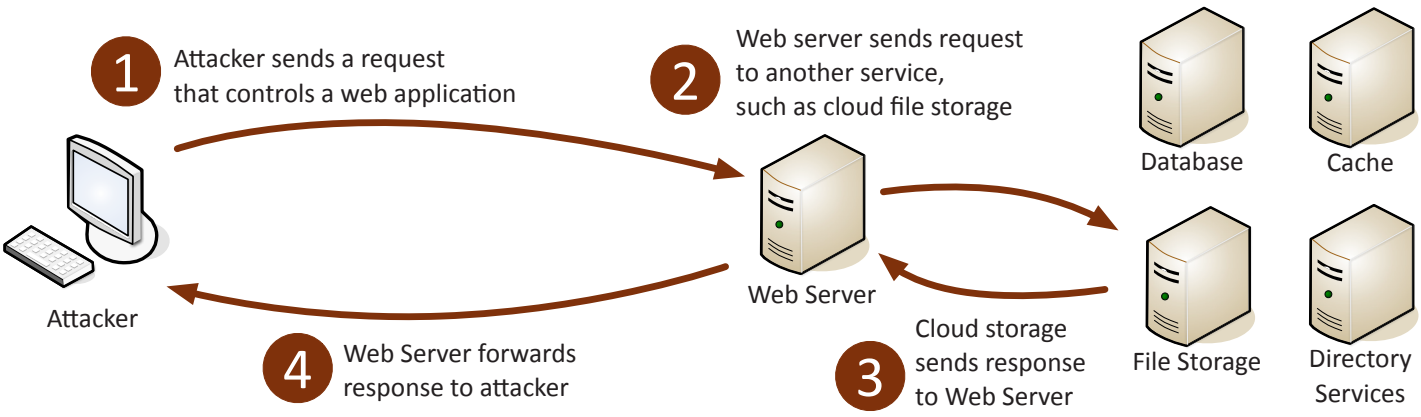
Server-side request forgery (SSRF)

- Attacker finds a vulnerable web application
  - Sends requests to a web server
  - Web server performs the request on behalf of the attacker
- Caused by bad programming
  - Never trust the user input
  - Server should validate the input and the responses
  - These are rare, but can be critical vulnerabilities

Capital One SSRF breach - March 2019

- Attacker is able to execute commands on the Capital One website
  - This is normally stopped by a WAF (Web Application Firewall)
  - The WAF was misconfigured
- Attacker obtained security credentials for the WAF role
- WAF-Role account listed the buckets on Amazon S3
- Attacker retrieved the data from the Amazon buckets
- Credit card application data from 2005 through 2019
  - 106 million names, address, phone, email, DoB
  - 140,000 Social Security numbers, 80,000 bank accounts

Server-side request forgery (SSRF)



1.3 - Driver Manipulation

Malware hide-and-go-seek

- Traditional anti-virus is very good at identifying known attacks
  - Checks the signature
  - Block anything that matches
- There are still ways to infect and hide
  - It's a constant war
  - Zero-day attacks, new attack types, etc.

Your drivers are powerful

- The interaction between the hardware and your operating system
  - They are often trusted
  - Great opportunity for security issues
- May 2016 - HP Audio Drivers
  - Conexant audio chips
  - Driver installation includes audio control software
  - Debugging feature enables a keylogger
- Hardware interactions contain sensitive information
  - Video, keyboard, mouse

Shimming

- Filling in the space between two objects
  - A middleman
- Windows includes it's own shim
  - Backwards compatibility with previous Windows versions
  - Application Compatibility Shim Cache
- Malware authors write their own shims
  - Get around security (like UAC)
- January 2015 Microsoft vulnerability
  - Elevates privilege

Refactoring

- Metamorphic malware
  - A different program each time it's downloaded
- Make it appear different each time
  - Add NOP instructions
  - Loops, pointless code strings
- Can intelligently redesign itself
  - Reorder functions
  - Modify the application flow
  - Reorder code and insert unused data types
- Difficult to match with signature-based detection
  - Use a layered approach

1.3 - SSL Stripping

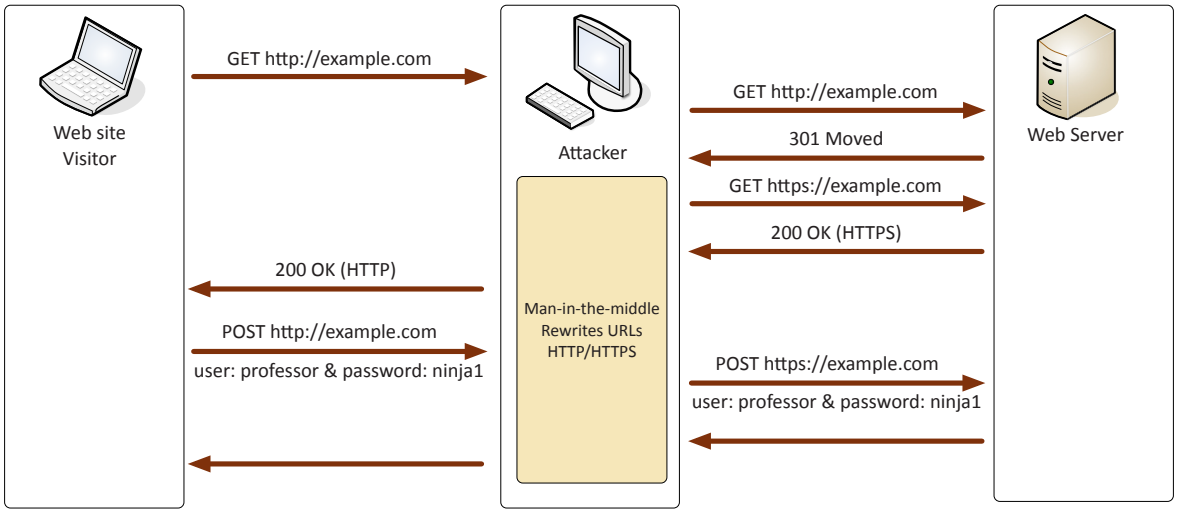
SSL stripping / HTTP downgrade

- Combines an on-path attack with a downgrade attack
  - Difficult to implement, but big returns for the attacker
- Attacker must sit in the middle of the conversation
  - Must modify data between the victim and web server
  - Proxy server, ARP spoofing, rogue Wi-Fi hotspot, etc.
- Victim does not see any significant problem
  - Except the browser page isn't encrypted
  - Strips the S away from HTTPS
- This is a client and server problem
  - Works on SSL and TLS

SSL and TLS

- SSL (Secure Sockets Layer) 2.0 - Deprecated in 2011
- SSL 3.0
  - Vulnerable to the POODLE attack
  - Deprecated in June 2015
- Transport Layer Security (TLS) 1.0
  - Upgrade to SSL 3.0, and a name change from SSL to TLS
  - Can downgrade to SSL 3.0
- TLS 1.1
  - Deprecated in January 2020 by modern browsers
- TLS 1.2 and TLS 1.3 - The latest standards

SSL stripping



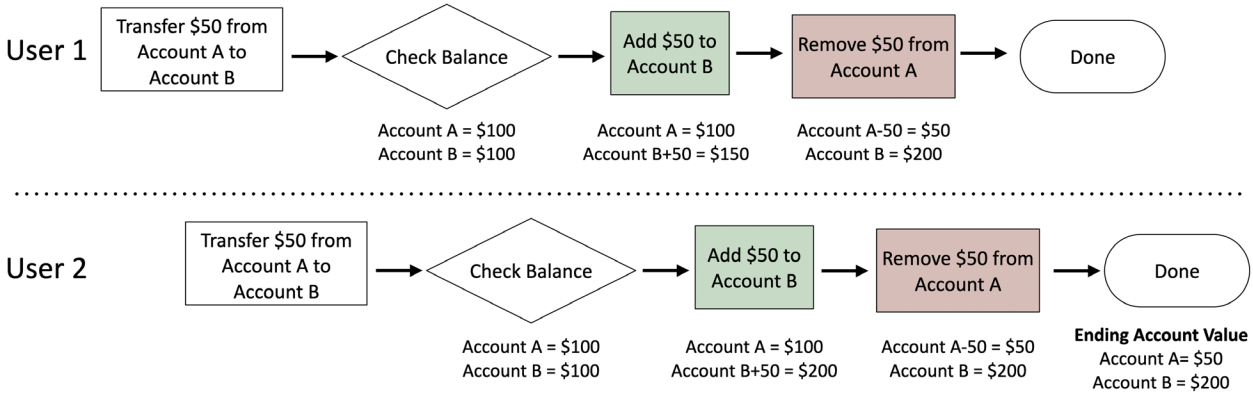
1.3 - Race Conditions

Race condition

- A programming conundrum
  - Sometimes, things happen at the same time
  - This can be bad if you've not planned for it
- Time-of-check to time-of-use attack (TOCTOU)
  - Check the system
  - When do you use the results of your last check?
  - Something might happen between the check and the use

Race conditions can cause big problems

- January 2004 - Mars rover "Spirit"
  - Reboot when a problem is identified
  - Problem is with the file system, so reboot because of the file system problem
  - Reboot loop was the result
- GE Energy - Energy Management System
  - Three power lines failed at the same time
  - Race condition delayed alerts
  - Caused the Northeast Blackout of 2003
- Therac-25 radiation therapy machine in the 1980s
  - Used software interlocks instead of hardware
  - Race condition caused 100 times the normal dose of radiation
  - Six patients injured, three deaths



1.3 - Other Application Attacks

Memory vulnerabilities

- Manipulating memory can be advantageous
  - Relatively difficult to accomplish
- Memory leak
  - Unused memory is not properly released
  - Begins to slowly grow in size
  - Eventually uses all available memory
  - System crashes
- NULL Pointer dereference
  - Programming technique that references a portion of memory
  - What happens if that reference points to nothing?
  - Application crash, debug information displayed, DoS
- Integer overflow
  - Large number into a smaller sized space
  - Where does the extra number go?
  - You shouldn't be able to manipulate memory this way

Directory traversal

- Directory traversal / path traversal
  - Read files from a web server that are outside of the website's file directory
  - Users shouldn't be able to browse the Windows folder
- Web server software vulnerability
  - Won't stop users from browsing past the web server root
- Web application code vulnerability
  - Take advantage of badly written code

Improper error handling

- Errors happen
  - And you should probably know about it
- Messages should be just informational enough
  - Avoid too much detail
  - Network information, memory dump, stack traces, database dumps
- This is an easy one to find and fix
  - A development best-practice

Improper input handling

- Many applications accept user input
  - We put data in, we get data back
- All input should be considered malicious
  - Check everything. Trust nobody.
- Allowing invalid input can be devastating
  - SQL injections, buffer overflows, denial of service, etc.
- It takes a lot of work to find input that can be used maliciously
  - But they will find it

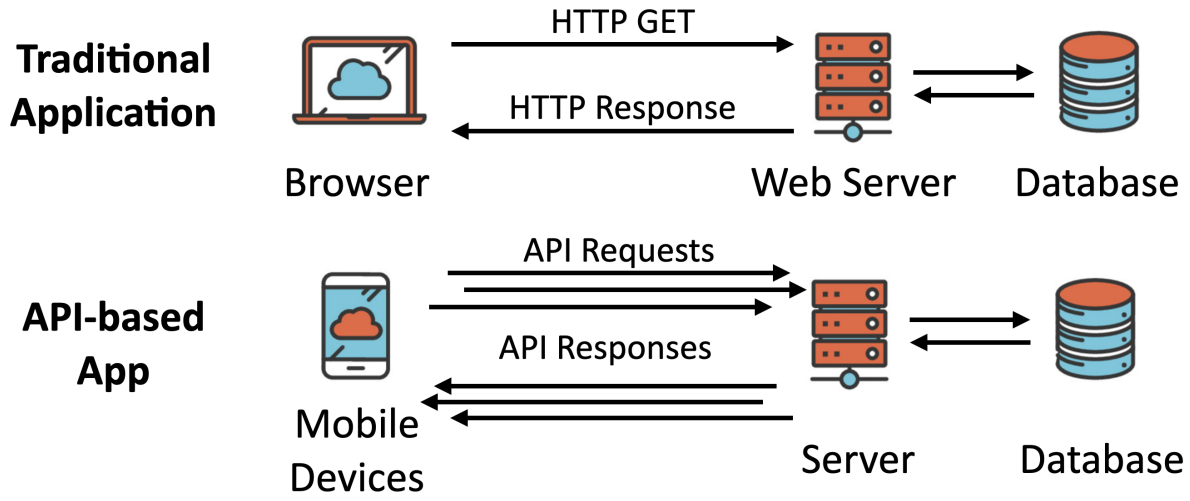
API attacks

- API - Application Programming Interface
- Attackers look for vulnerabilities in this new communication path
  - Exposing sensitive data, DoS, intercepted communication, privileged access

Resource exhaustion

- A specialized DoS (Denial of Service) attack
  - May only require one device and low bandwidths
- ZIP bomb
  - A 42 kilobyte .zip compressed file
  - Uncompresses to 4.5 petabytes (4,500 terabytes)
  - Anti-virus will identify these
- DHCP starvation
  - Attacker floods a network with IP address requests
  - MAC address changes each time
  - DHCP server eventually runs out of addresses
  - Switch configurations can rate limit DHCP requests

Traditional vs. API-based applications



1.4 - Rogue Access Points and Evil Twins

Rogue access points

- An unauthorized wireless access point
  - May be added by an employee or an attacker
  - Not necessarily malicious
  - A significant potential backdoor
- Very easy to plug in a wireless AP
  - Or enable wireless sharing in your OS
- Schedule a periodic survey
  - Walk around your building/campus
  - Use third-party tools / WiFi Pineapple
- Consider using 802.1X (Network Access Control)
  - You must authenticate, regardless of the connection type

Wireless evil twins

- Looks legitimate, but actually malicious
  - The wireless version of phishing
- Configure an access point to look like an existing network
  - Same (or similar) SSID and security settings/captive portal
- Overpower the existing access points
  - May not require the same physical location
- WiFi hotspots (and users) are easy to fool
  - And they're wide open
- You encrypt your communication, right?
  - Use HTTPS and a VPN

1.4 - Bluejacking and Bluesnarfing

Bluejacking

- Sending of unsolicited messages to another device via Bluetooth
  - No mobile carrier required!
- Typical functional distance is about 10 meters
  - More or less, depending on antenna and interference
- Bluejack with an address book object
  - Instead of contact name, write a message
  - "You are Bluejacked!"
  - "You are Bluejacked! Add to contacts?"
- Third-party software may also be used
  - Blooover, Bluesniff

Bluesnarfing

- Access a Bluetooth-enabled device and transfer data
  - Contact list, calendar, email, pictures, video, etc.
- First major security weakness in Bluetooth
  - Marcel Holtmann in September 2003 and
  - Adam Laurie in November 2003
  - This weakness was patched
- Serious security issue
  - If you know the file, you can download it without authentication

1.4 - Wireless Disassociation Attacks

It started as a normal day

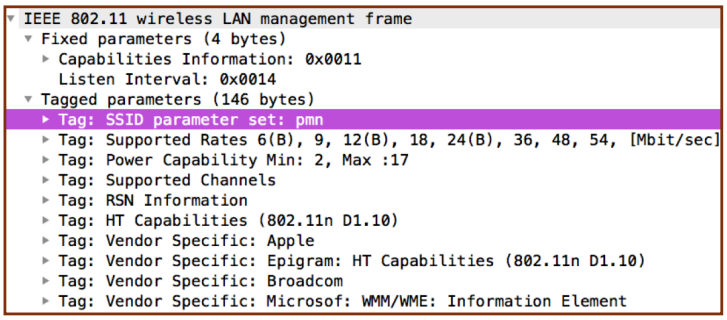
- Surfing along on your wireless network
  - And then you're not
- And then it happens again
  - And again
- You may not be able to stop it
  - There's (almost) nothing you can do
  - Time to get a long patch cable
- Wireless disassociation
  - A significant wireless denial of service (DoS) attack

802.11 management frames

- 802.11 wireless includes a number of management features
  - Frames that make everything work
  - You never see them
- Important for the operation of 802.11 wireless
  - How to find access points, manage QoS, associate/disassociate with an access point, etc.
- Original wireless standards did not add protection for management frames
  - Sent in the clear
  - No authentication or validation

Protecting against disassociation

- IEEE has already addressed the problem
  - 802.11w - July 2014
- Some of the important management frames are encrypted
  - Disassociate, deauthenticate, channel switch announcements, etc.
- Not everything is encrypted
  - Beacons, probes, authentication, association
- 802.11w is required for 802.11ac compliance
  - This will roll out going forward



1.4 - Wireless Jamming

Radio frequency (RF) jamming

- Denial of Service
  - Prevent wireless communication
- Transmit interfering wireless signals
  - Decrease the signal-to-noise ratio at the receiving device
  - The receiving device can't hear the good signal
- Sometimes it's not intentional
  - Interference, not jamming
  - Microwave oven, fluorescent lights
- Jamming is intentional
  - Someone wants your network to not work

Wireless jamming

- Many different types
  - Constant, random bits / Constant, legitimate frames
- Data sent at random times
  - Random data and legitimate frames
- Reactive jamming
  - Only when someone else tries to communicate
- Needs to be somewhere close
  - Difficult to be effective from a distance
- Time to go fox hunting
  - You'll need the right equipment to hunt down the jam
  - Directional antenna, attenuator

1.4 - RFID and NFC Attacks

RFID (Radio-frequency identification)

- It's everywhere
  - Access badges
  - Inventory/Assembly line tracking
  - Pet/Animal identification
  - Anything that needs to be tracked
- Radar technology
  - Radio energy transmitted to the tag
  - RF powers the tag, ID is transmitted back
  - Bidirectional communication
  - Some tag formats can be active/powered

RFID Attacks

- Data capture
  - View communication
  - Replay attack
- Spoof the reader - Write your own data to the tag
- Denial of service - Signal jamming
- Decrypt communication
  - Many default keys are on Google

Near field communication (NFC)

- Two-way wireless communication
  - Builds on RFID, which is mostly one-way
- Payment systems
  - Many options available
- Bootstrap for other wireless
  - NFC helps with Bluetooth pairing
- Access token, identity "card"
  - Short range with encryption support

NFC Security Concern

- Remote capture
  - It's a wireless network
  - 10 meters for active devices
- Frequency jamming
  - Denial of service
- Relay / Replay attack
  - On-path attack
- Loss of RFC device control
  - Stolen/lost phone

1.4 - Randomizing Cryptography

Cryptographic nonce

- Arbitrary number
  - Used once
  - "For the nonce" - For the time being
- A random or pseudo-random number
  - Something that can't be reasonably guessed
  - Can also be a counter
- Use a nonce during the login process
  - Server gives you a nonce
  - Calculate your password hash using the nonce
  - Each password hash sent to the host will be different, so a replay won't work

Initialization Vectors (IV)

- A type of nonce
  - Used for randomizing an encryption scheme
  - The more random the better
- Used in encryption ciphers, WEP, and some SSL implementations

Salt

- A nonce most commonly associated with password randomization
  - Make the password hash unpredictable
- Password storage should always be salted
  - Each user gets a different salt
- If the password database is breached, you can't correlate any passwords
  - Even users with the same password have different hashes stored

1.4 - On-Path Attacks

On-path network attack

- How can an attacker watch without you knowing?
  - Formerly known as man-in-the-middle
- Redirects your traffic
  - Then passes it on to the destination
  - You never know your traffic was redirected
- ARP poisoning
  - ARP has no security
  - On-path attack on the local IP subnet

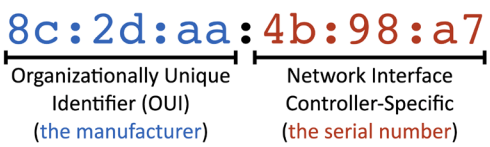
On-path browser attack

- What if the middleman was on the same computer as the victim?
  - Malware/Trojan does all of the proxy work
  - Formerly known as man-in-the-browser
- Huge advantages for the attackers
  - Relatively easy to proxy encrypted traffic
  - Everything looks normal to the victim
- The malware in your browser waits for you to login to your bank
  - And cleans you out

1.4 - MAC Flooding and Cloning

The MAC address

- Ethernet Media Access Control address
  - The "physical" address of a network adapter
  - Unique to a device
- 48 bits / 6 bytes long
  - Displayed in hexadecimal



LAN switching

- Forward or drop frames
  - Based on the destination MAC address
- Gather a constantly updating list of MAC addresses
  - Builds the list based on the source MAC address of incoming traffic
  - These age out periodically, often in 5 minutes
- Maintain a loop-free environment
  - Using Spanning Tree Protocol (STP)

Learning the MACs

- Switches examine incoming traffic
  - Makes a note of the source MAC address
- Adds unknown MAC addresses to the MAC address table
  - Sets the output interface to the received interface

MAC flooding

- The MAC table is only so big
- Attacker starts sending traffic with different source MAC addresses
  - Force out the legitimate MAC addresses
- The table fills up
  - Switch begins flooding traffic to all interfaces
- This effectively turns the switch into a hub
  - All traffic is transmitted to all interfaces
  - No interruption in traffic flows
- Attacker can easily capture all network traffic!
- Flooding can be restricted in the switch's port security settings

MAC cloning / MAC spoofing

- An attacker changes their MAC address to match the MAC address of an existing device
  - A clone / a spoof
- Circumvent filters
  - Wireless or wired MAC filters
  - Identify a valid MAC address and copy it
- Create a DoS
  - Disrupt communication to the legitimate MAC
- Easily manipulated through software
  - Usually a device driver option

1.4 - DNS Attacks

DNS poisoning

- Modify the DNS server
  - Requires some crafty hacking
- Modify the client host file
  - The host file takes precedent over DNS queries
- Send a fake response to a valid DNS request
  - Requires a redirection of the original request or the resulting response

Domain hijacking

- Get access to the domain registration, and you have control where the traffic flows
  - You don't need to touch the actual servers
  - Determines the DNS names and DNS IP addresses
- Many ways to get into the account
  - Brute force
  - Social engineer the password
  - Gain access to the email address that manages the account
  - The usual things

Domain hijacking

- Saturday, October 22, 2016, 1 PM
- Domain name registrations of 36 domains are changed
  - Brazilian bank
  - Desktop domains, mobile domains, and more
- Under hacker control for 6 hours
  - The attackers became the bank
- 5 million customers, $27 billion in assets
  - Results of the hack have not been publicly released

1.4 - DNS Attacks (continued)

URL hijacking
- Make money from your mistakes
  - There's a lot of advertising on the 'net
- Sell the badly spelled domain to the actual owner
  - Sell a mistake
- Redirect to a competitor
  - Not as common, legal issues
- Phishing site
  - Looks like the real site, please login
- Infect with a drive-by download
  - You've got malware!

Types of URL hijacking
- Typosquatting / brandjacking
  - Take advantage of poor spelling
- Outright misspelling
  - professormesser.com vs. professormessor.com
- A typing error
  - professormeser.com
- A different phrase
  - professormessers.com
- Different top-level domain
  - professormesser.org

Domain reputation
- The Internet is tracking your security posture
  - They know when things go sideways
- Email reputation
  - Suspicious activity
  - Malware originating from the IP address
- A bad reputation can cause email delivery to fail
  - Email rejection or simply dropped
- Check with the email or service provider to check the reputation
  - Follow their instructions to remediate
- Infected systems are noticed by the search engines
  - Your domain can be flagged or removed
- Users will avoid the site
  - Sales will drop
  - Users will avoid your brand
- Malware might be removed quickly
  - Recovery takes much longer

1.4 - Denial of Service

Denial of Service
- Force a service to fail
  - Overload the service
- Take advantage of a design failure or vulnerability
  - Keep your systems patched!
- Cause a system to be unavailable
  - Competitive advantage
- Create a smokescreen for some other exploit
  - Precursor to a DNS spoofing attack
- Doesn't have to be complicated
  - Turn off the power

A "friendly" DoS
- Unintentional DoSing - It's not always a ne'er-do-well
- Network DoS - Layer 2 loop without STP
- Bandwidth DoS - Downloading multi-gigabyte Linux distributions over a DSL line
- The water line breaks
  - Get a good shop vacuum

Distributed Denial of Service (DDoS)
- Launch an army of computers to bring down a service
  - Use all the bandwidth or resources - traffic spike
- This is why the attackers have botnets
  - Thousands or millions of computers at your command
  - At its peak, Zeus botnet infected over 3.6 million PCs
  - Coordinated attack
- Asymmetric threat
  - The attacker may have fewer resources than the victim

DDoS amplification
- Turn your small attack into a big attack
  - Often reflected off another device or service
- An increasingly common DDoS technique
  - Turn Internet services against the victim
- Uses protocols with little (if any) authentication or checks
  - NTP, DNS, ICMP
  - A common example of protocol abuse

Application DoS
- Make the application break or work harder
  - Increase downtime and costs
- Fill the disk space
  - A 42 kilobyte .zip compressed file
  - Uncompresses to 4.5 petabytes (4,500 terabytes)
  - Anti-virus will identify these
- Overuse a measured cloud resource
  - More CPU/memory/network is more money
- Increase the cloud server response time
  - Victim deploys a new application instance - repeat

Operational Technology (OT) DoS
- The hardware and software for industrial equipment
  - Electric grids, traffic control, manufacturing plants, etc.
- This is more than a web server failing
  - Power grid drops offline
  - All traffic lights are green
  - Manufacturing plant shuts down
- Requires a different approach
  - A much more critical security posture

1.4 - Malicious Scripts

Scripting and automation
- Automate tasks
  - You don't have to be there
  - Solve problems in your sleep
  - Monitor and resolve problems before they happen
- The need for speed
  - The script is as fast as the computer
  - No typing or delays
  - No human error
- Automate the attack
  - The hacker is on borrowed time

Windows PowerShell
- Command line for system administrators
  - .ps1 file extension
  - Included with Windows 8/8.1 and 10
- Extend command-line functions
  - Uses cmdlets (command-lets)
  - PowerShell scripts and functions
  - Standalone executables
- Attack Windows systems
  - System administration
  - Active Domain administration
  - File share access

Python
- General-purpose scripting language
  - .py file extension
- Popular in many technologies
  - Broad appeal and support
- Commonly used for cloud orchestration
  - Create and tear down application instances
- Attack the infrastructure
  - Routers, servers, switches

Shell script
- Scripting the Unix/Linux shell
  - Automate and extend the command line
  - Bash, Bourne, Korn, C
- Starts with a shebang or hash-bang #!
  - Often has a .sh file extension
- Attack the Linux/Unix environment
  - Web, database, virtualization servers
- Control the OS from the command line
  - Malware has a lot of options

Macros
- Automate functions within an application
  - Or operating system
- Designed to make the application easier to use
  - Can often create security vulnerabilities
- Attackers create automated exploits
  - They just need the user to open the file
  - Prompts to run the macro

Visual Basic for Applications (VBA)
- Automates processes within Windows applications
  - Common in Microsoft Office
- A powerful programming language
  - Interacts with the operating system
- CVE-2010-0815 / MS10-031
  - VBA does not properly search for ActiveX controls in a document
  - Run arbitrary code embedded in a document
  - Easy to infect a computer

1.5 - Threat Actors

Threat actors and attributes
- The entity responsible for an event that has an impact on the safety of another entity
  - Also called a malicious actor
- Broad scope of actors
  - And motivations vary widely
- Advanced Persistent Threat (APT)
  - Attackers are in the network and undetected
  - 2018 FireEye report:
    Americas: 71 days,
    EMEA: 177 days,
    APAC: 204 days

Insiders
- More than just passwords on sticky notes
  - Some insiders are out for no good
- Sophistication may not be advanced, but the insider has institutional knowledge
  - Attacks can be directed at vulnerable systems
  - The insider knows what to hit
- Extensive resources
  - Eating away from the inside

Nation states
- Governments
  - National security, job security
  - Always an external entity
- Highest sophistication
  - Military control, utilities, financial control
  - United States and Israel destroyed 1,000 nuclear centrifuges with the Stuxnet worm
- Constant attacks
  - Commonly an Advanced Persistent Threat (APT)

1.5 - Threat Actors (continued)

Hacktivist
- A hacker with a purpose
  - Social change or a political agenda
  - Often an external entity
- Can be remarkably sophisticated
  - Very specific hacks
  - DoS, web site defacing, release of private documents, etc.
- Funding is limited
  - Some organizations have fundraising options

Script kiddies
- Runs pre-made scripts without any knowledge of what's really happening
  - Not necessarily a youngster
- Can be internal or external
  - But usually external
- Not very sophisticated
- No formal funding
  - Looking for low hanging fruit
- Motivated by the hunt
  - Working the ego, trying to make a name

Organized crime
- Professional criminals
  - Motivated by money
  - Almost always an external entity
- Very sophisticated
  - Best hacking money can buy
- Crime that's organized
  - One person hacks, one person manages the exploits, another person sells the data, another handles customer support
- Lots of capital to fund hacking efforts

Hackers
- Experts with technology
  - Often driven by money, power, and ego
- Authorized
  - An ethical hacker with good intentions
  - And permission to hack
- Unauthorized
  - Malicious, violates security for personal gain
- Semi-authorized
  - Finds a vulnerability, doesn't use it

Shadow IT
- Going rogue
  - Working around the internal IT organization
- Information Technology can put up roadblocks
  - Shadow IT is unencumbered
  - Use the cloud
  - Might also be able to innovate
- Not always a good thing
  - Wasted time and money
  - Security risks
  - Compliance issues
  - Dysfunctional organization

Competitors
- Many different motivations
  - DoS, espionage, harm reputation
- High level of sophistication
  - Based on some significant funding
  - The competitive upside is huge (and very unethical)
- Many different intents
  - Shut down your competitor during an event
  - Steal customer lists
  - Corrupt manufacturing databases
  - Take financial information

1.5 - Attack Vectors

Attack vectors
- A method used by the attacker
  - Gain access or infect to the target
- A lot of work goes into finding vulnerabilities in these vectors
  - Some are more vulnerable than others
- IT security professional spend their career watching these vectors
  - Closing up existing vectors
  - Finding new ones

Direct access attack vectors
- There's a reason we lock the data center
  - Physical access to a system is a significant attack vector
- Modify the operating system
  - Reset the administrator password in a few minutes
- Attach a keylogger
  - Collect usernames and passwords
- Transfer files
  - Take it with you
- Denial of service
  - This power cable is in the way

Wireless attack vectors
- Default login credentials
  - Modify the access point configuration
- Rogue access point
  - A less-secure entry point to the network
- Evil twin
  - Attacker collects authentication details
  - On-path attacks
- Protocol vulnerabilities
  - 2017 - WPA2 Key Reinstallation Attack (KRACK)
  - Older encryption protocols (WEP, WPA)

1.5 - Attack Vectors (continued)

Email attack vectors
- One of the biggest (and most successful) attack vectors
  - Everyone has email
- Phishing attacks
  - People want to click links
- Deliver the malware to the user
  - Attach it to the message
- Social engineering attacks
  - Invoice scam

Supply chain attack vectors
- Tamper with the underlying infrastructure
  - Or manufacturing process
- Gain access to a network using a vendor
  - 2013 Target credit card breach
- Malware can modify the manufacturing process
  - 2010 - Stuxnet disrupts Iran's uranium enrichment program
- Counterfeit networking equipment
  - Install backdoors, substandard performance and availability
  - 2020 - Fake Cisco Catalyst 2960-X and WS-2960X-48TS-L

Social media attack vectors
- Attackers thank you for putting your personal information online
  - Where you are and when
  - Vacation pictures are especially telling
- User profiling
  - Where were you born?
  - What is the name of your school mascot?
- Fake friends are fake
  - The inner circle can provide additional information

Removable media attack vectors
- Get around the firewall
  - The USB interface
- Malicious software on USB flash drives
  - Infect air gapped networks
  - Industrial systems, high-security services
- USB devices can act as keyboards
  - Hacker on a chip
- Data exfiltration
  - Terabytes of data walk out the door
  - Zero bandwidth used

Cloud attack vectors
- Publicly-facing applications and services
  - Mistakes are made all the time
- Security misconfigurations
  - Data permissions and public data stores
- Brute force attacks
  - Or phish the users of the cloud service
- Orchestration attacks
  - Make the cloud build new application instances
- Denial of service
  - Disable the cloud services for everyone

1.5 - Threat Intelligence

Threat intelligence
- Research the threats - And the threat actors
- Data is everywhere
  - Hacker group profiles, tools used by the attackers, and much more
- Make decisions based on this intelligence
  - Invest in the best prevention
- Used by researchers, security operations teams, and others

Open-source intelligence (OSINT)
- Open-source
  - Publicly available sources
  - A good place to start
- Internet
  - Discussion groups, social media
- Government data
  - Mostly public hearings, reports, websites, etc.
- Commercial data
  - Maps, financial reports, databases

Closed/proprietary intelligence
- Someone else has already compiled the threat information
  - You can buy it
- Threat intelligence services
  - Threat analytics, correlation across different data sources
- Constant threat monitoring
  - Identify new threats
  - Create automated prevention workflows

Vulnerability databases
- Researchers find vulnerabilities
  - Everyone needs to know about them
- Common Vulnerabilities and Exposures (CVE)
  - A community managed list of vulnerabilities
  - Sponsored by the U.S. Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency (CISA)
- U.S. National Vulnerability Database (NVD)
  - A summary of CVEs
  - Also sponsored by DHS and CISA
- NVD provides additional details over the CVE list
  - Patch availability and severity scoring

1.5 - Threat Intelligence (continued)

Public/private information-sharing centers
- Public threat intelligence
  - Often classified information
- Private threat intelligence
  - Private companies have extensive resources
- Need to share critical security details
  - Real-time, high-quality cyber threat information sharing
- Cyber Threat Alliance (CTA)
  - Members upload specifically formatted threat intelligence
  - CTA scores each submission and validates across other submissions
  - Other members can extract the validated data

Automated indicator sharing (AIS)
- Intelligence industry needs a standard way to share important threat data
  - Share information freely
- Structured Threat Information eXpression (STIX)
  - Describes cyber threat information
  - Includes motivations, abilities, capabilities, and response information
- Trusted Automated eXchange of Indicator Information (TAXII)
  - Securely shares STIX data

Dark web intelligence
- Dark web
  - Overlay networks that use the Internet
  - Requires specific software and configurations to access
- Hacking groups and services
  - Activities
  - Tools and techniques
  - Credit card sales
  - Accounts and passwords
- Monitor forums for activity
  - Company names, executive names

Indicators of compromise (IOC)
- An event that indicates an intrusion
  - Confidence is high
  - He's calling from inside the house
- Indicators
  - Unusual amount of network activity
  - Change to file hash values
  - Irregular international traffic
  - Changes to DNS data
  - Uncommon login patterns
  - Spikes of read requests to certain files

Predictive analysis
- Analyze large amounts of data very quickly
  - Find suspicious patterns
  - Big data used for cybersecurity
- Identify behaviors
  - DNS queries, traffic patterns, location data
- Creates a forecast for potential attacks
  - An early-warning system
- Often combined with machine learning
  - Less emphasis on signatures

Threat maps
- Identify attacks and trends
  - View worldwide perspective
- Created from real attack data
  - Identify and react

File/code repositories
- See what the hackers are building
  - Public code repositories, GitHub
- See what people are accidentally releasing
  - Private code can often be published publicly
- Attackers are always looking for this code
  - Potential exploits exist
  - Content for phishing attacks

1.5 - Threat Research

Threat research
- Know your enemy
  - And their tools of war
- A never-ending process
  - The field is constantly moving and changing
- Information from many different places
  - You can't rely on a single source

Vendor websites
- Vendors and manufacturers
  - They wrote the software
- They know when problems are announced
  - Most vendors are involved in the disclosure process
- They know their product better than anyone
  - They react when surprises happen
  - Scrambling after a zero-day announcement
  - Mitigating and support options

Vulnerability feeds
- Automated vulnerability notifications
  - National Vulnerability Database (https://nvd.nist.gov)
  - CVE Data Feeds (https://cve.mitre.org)
- Third-party feeds
  - Additional vulnerability coverage
- Roll-up to a vulnerability management system
  - Coverage across teams
  - Consolidated view of security issues

1.5 - Threat Intelligence (continued)

Conferences
- Watch and learn
  - An early warning of things to come
- Researchers
  - New DDoS methods, intelligence gathering, hacking the latest technologies
- Stories from the trenches
  - Fighting and recovering from attacks
  - New methods to protect your data
- Building relationships - forge alliances

Academic journals
- Research from academic professionals
  - Cutting edge security analysis
- Evaluations of existing security technologies
  - Keeping up with the latest attack methods
- Detailed post mortem
  - Tear apart the latest malware and see what makes it tick
- Extremely detailed information
  - Break apart topics into their smaller pieces

Request for comments (RFC)
- Published by the Internet Society (ISOC)
  - Often written by the Internet Engineering Task Force (IETF)
  - Internet Society description is RFC 1602
- Not all RFCs are standards documents
  - Experimental, Best Current Practice, Standard Track, and Historic
- Many informational RFCs analyze threats
  - RFC 3833 - Threat Analysis of the Domain Name System
  - RFC 7624 - Confidentiality in the Face of Pervasive Surveillance:
  - A Threat Model and Problem Statement

Local industry groups
- A gathering of local peers
  - Shared industry and technology, geographical presence
- Associations
  - Information Systems Security Association, Network Professional Association
  - Meet others in the area, discuss local challenges
- Industry user groups
  - Cisco, Microsoft, VMware, etc. - Secure specific technologies

Social media
- Hacking group conversations - Monitor the chatter
- Honeypot monitoring on Twitter
  - Identify new exploit attempts
- Keyword monitoring - CVE-2020-*, bugbounty, 0-day
- Analysis of vulnerabilities - Professionals discussing the details
- Command and control - Use social media as the transport

Threat feeds
- Monitor threat announcements - Stay informed
- Many sources of information
  - U.S. Department of Homeland Security
  - U.S. Federal Bureau of Investigation
  - SANS Internet Storm Center
  - VirusTotal Intelligence:
  - Google and Facebook correlation

TTP
- Tactics, techniques, and procedures
  - What are adversaries doing and how are they doing it?
- Search through data and networks
  - Proactively look for threats
  - Signatures and firewall rules can't catch everything
- Different types of TTPs
  - Information on targeted victims (Finance for energy companies)
  - Infrastructure used by attackers (DNS and IP addresses)
  - Outbreak of a particular malware variant on a service type

1.6 - Vulnerability Types

Zero-day attacks
- Many applications have vulnerabilities
  - We've just not found them yet
- Someone is working hard to find the next big vulnerability
  - The good guys share these with developers
- Attackers keep these yet-to-be-discovered holes to themselves
  - They want to use these vulnerabilities for personal gain
- Zero-day
  - The vulnerability has not been detected or published
  - Zero-day exploits are increasingly common
- Common Vulnerabilities and Exposures (CVE)
  - http://cve.mitre.org/

Open permissions
- Very easy to leave a door open
  - The hackers will always find it
- Increasingly common with cloud storage
  - Statistical chance of finding an open permission
- June 2017 - 14 million Verizon records exposed
  - Third-party left an Amazon S3 data repository open
  - Researcher found the data before anyone else
- Many, many other examples
  - Secure your permissions!

1.6 - Vulnerability Types (continued)

Unsecured root accounts
- The Linux root account
  - The Administrator or superuser account
- Can be a misconfiguration
  - Intentionally configuring an easy-to-hack password
  - 123456, ninja, football
- Disable direct login to the root account
  - Use the su or sudo option
- Protect accounts with root or administrator access
  - There should not be a lot of these

Errors
- Error messages can provide useful information to an attacker
  - Service type, version information, debug data
- September 2015 - Patreon is compromised
  - Used a debugger to help monitor and troubleshoot web site issues
  - Was left exposed to the Internet
  - Effectively allowed for remote code executions
  - Gigabytes of customer data was released online

Weak encryption
- Encryption protocol (AES, 3DES, etc.)
  - Length of the encryption key (40 bits, 128 bits, 256 bits, etc.)
  - Hash used for the integrity check (SHA, MD5, etc.)
  - Wireless encryption (WEP, WPA)
- Some cipher suites are easier to break than others
  - Stay updated with the latest best practices
- TLS is one of the most common issues
  - Over 300 cipher suites
- Which are good and which are bad?
  - Weak or null encryption (less than 128 bit key sizes), outdated hashes (MD5)

Insecure protocols
- Some protocols aren't encrypted
  - All traffic sent in the clear - Telnet, FTP, SMTP, IMAP
- Verify with a packet capture
  - View everything sent over the network
- Use the encrypted versions- SSH, SFTP, IMAPS, etc.

Default settings
- Every application and network device has a default login
  - Not all of these are ever changed
- Mirai botnet
  - Takes advantage of default configurations
  - Takes over Internet of Things (IoT) devices
  - 60+ default configurations
  - Cameras, routers, doorbells, garage door openers, etc.
- Mirai released as open-source software
  - There's a lot more where that came from

Open ports and services
- Services will open ports
  - It's important to manage access
- Often managed with a firewall
  - Manage traffic flows
  - Allow or deny based on port number or application
- Firewall rulesets can be complex
  - It's easy to make a mistake
- Always test and audit
  - Double and triple check

Improper patch management
- Often centrally managed
  - The update server determine when you patch
  - Test all of your apps, then deploy
  - Efficiently manage bandwidth
- Firmware - The BIOS of the device
- Operating system- Monthly and on-demand patches
- Applications
  - Provided by the manufacturer as-needed

Legacy platforms
- Some devices remain installed for a long time
  - Perhaps too long
- Legacy devices
  - Older operating systems, applications, middleware
- May be running end-of-life software
  - The risk needs to be compared to the return
- May require additional security protections
  - Additional firewall rules
  - IPS signature rules for older operating systems

1.6 - Third-party Risks

Third-party risks
- IT security doesn't change because it's a third-party
  - There should be more security, not less
- Always expect the worst
  - Prepare for a breach
- Human error is still the biggest issue
  - Everyone needs to use IT security best practices
- All security is important
  - Physical security and cybersecurity work hand-in-hand

System integration risk
- Professional installation and maintenance
  - Can include elevated OS access
- Can be on-site
  - With physical or virtual access to data and systems
  - Keylogger installations and USB flash drive data transfers
- Can run software on the internal network
  - Less security on the inside
  - Port scanners, traffic captures
  - Inject malware and spyware, sometimes inadvertently

1.6 - Third-party Risks (continued)

Lack of vendor support
- Security requires diligence
  - The potential for a vulnerability is always there
- Vendors are the only ones who can fix their products
  - Assuming they know about the problem
  - And care about fixing it
- Trane Comfortlink II thermostats
  - Control the temperature from your phone
  - Trane notified of three vulnerabilities in April 2014
  - Two patched in April 2015, one in January 2016

Supply chain risk
- You can't always control security at a third-party location
  - Always maintain local security controls
- Hardware and software from a vendor can contain malware
  - Verify the security of new systems
- Counterfeit hardware is out there
  - It looks like a Cisco switch…Is it malicious?

Outsourced code development
- Accessing the code base
  - Internal access over a VPN
  - Cloud-based access
- Verify security to other systems
  - The development systems should be isolated
- Test the code security
  - Check for backdoors
  - Validate data protection and encryption

Data storage
- Consider the type of data
  - Contact information
  - Healthcare details, financial information
- Storage at a third-party may need encryption
  - Limits exposure, adds complexity
- Transferring data
  - The entire data flow needs to be encrypted

1.6 - Vulnerability Impacts

Vulnerability impacts
- Malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016
  - The Cost of Malicious Cyber Activity to the U.S. Economy,
  - The Council of Economic Advisers, February 2018
- Many other non-economic impacts - Far reaching effects
- These are the reasons we patch vulnerabilities

Data loss
- Vulnerability: Unsecured databases
  - No password or default password
- July 2020 - Internet-facing databases are being deleted
  - No warning, no explanation
- Thousands of databases are missing
  - I hope you had a backup
- Overwrites data with iterations of the word "meow"
  - No messages or motivational content

Identity theft
- May through July 2017 - Equifax
  - Data breach of 147.9 million Americans,
  - 15.2 million British citizens, 19,000 Canadian citizens
  - Names, SSNs, birthdates, addresses, some driver's license numbers
- Apache Struts vulnerability from March 7, 2017
  - Breach started March 12th
  - Wasn't patched by Equifax until July 30th after discovering "suspicious network traffic"
  - September 7th - Public disclosure
- September 15th - CIO and CSO depart Equifax
- July 2019 - Equifax pays $575 million in fines

Financial loss
- March 2016 - Bank of Bangladesh
  - Society for Worldwide Interbank Financial Telecommunications (SWIFT)
- Attackers sent secure messages to transfer nearly one billion dollars in reserves to accounts in Philippines and Sri Lanka
  - Fortunately, most of the messages were incorrectly formatted
- Thirty-five requests were acted upon
  - $81 million lost and laundered through the Filipino casino industry
- Similar SWIFT vulnerabilities: $12 million from Wells Fargo, $60 million from Taiwanese Far Eastern International Bank

Reputation impacts
- Getting hacked isn't a great look
  - Organizations are often required to disclose
  - Stock prices drop, at least for the short term
- October 2016 - Uber breach
  - 25.6 million Names, email addresses, mobile numbers
- Didn't publicly announce it until November 2017
  - Allegedly paid the hackers $100,000 and had them sign an NDA
  - 2018 - Uber paid $148 million in fines
- Hackers pleaded guilty in October 2019
  - August 2020 - Uber's former Chief Security Officer

Availability loss
- Outages and downtime - Systems are unavailable
- The pervasive ransomware threat
  - Brings down the largest networks
- September 2020 - BancoEstado
  - One of Chile's three biggest banks
  - Ransomware attack over the weekend
- Bank closed for an extended period
  - Segmented network - Only hit internal systems
  - Wipe and restore everything

1.7 - Threat Hunting

Threat hunting
- The constant game of cat and mouse
  - Find the attacker before they find you
- Strategies are constantly changing
  - Firewalls get stronger, so phishing gets better
- Intelligence data is reactive
  - You can't see the attack until it happens
- Speed up the reaction time
  - Use technology to fight

Intelligence fusion
- An overwhelming amount of security data
  - Too much data to properly detect, analyze, and react
- Many data types
  - Dramatically different in type and scope
- Separate teams
  - Security operations, security intelligence, threat response
- Fuse the security data together with big data analytics
  - Analyze massive and diverse datasets
  - Pick out the interesting data points and correlations

Fusing the data
- Collect the data
  - Logs and sensors, network information, Internet events, intrusion detection
- Add external sources
  - Threat feeds, governmental alerts, advisories and bulletins, social media
- Correlate with big data analytics
  - Focuses on predictive analytics and user behavior analytics
  - Mathematical analysis of unstructured data

Cybersecurity maneuvers
- In the physical world, move troops and tanks
  - Stop the enemy on a bridge or shore
- In the virtual world, move firewalls and operating systems
  - Set a firewall rule, block an IP address, delete malicious software
- Automated maneuvers
  - Moving at the speed of light
  - The computer reacts instantly
- Combine with fused intelligence
  - Ongoing combat from many fronts
- Tomorrow it's a different fight

1.7 - Vulnerability Scans

Vulnerability scanning
- Usually minimally invasive
  - Unlike a penetration test
- Port scan
  - Poke around and see what's open
- Identify systems
  - And security devices
- Test from the outside and inside
  - Don't dismiss insider threats
- Gather as much information as possible
  - We'll separate wheat from chaff later

Scan types
- Scanners are very powerful
  - Use many different techniques to identify vulnerabilities
- Non-intrusive scans
  - Gather information, don't try to exploit a vulnerability
- Intrusive scans
  - You'll try out the vulnerability to see if it works
- Non-credentialed scans
  - The scanner can't login to the remote device
- Credentialed scan
  - You're a normal user, emulates an insider attack

Identify vulnerabilities
- The scanner looks for everything
  - Well, not everything - The signatures are the key
- Application scans
  - Desktop, mobile apps
- Web application scans
  - Software on a web server
- Network scans
  - Misconfigured firewalls, open ports, vulnerable devices

Vulnerability research
- The vulnerabilities can be cross-referenced online
  - Almost all scanners give you a place to go
- National Vulnerability Database: http://nvd.nist.gov/
- Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org/cve/
- Microsoft Security Bulletins: http://www.microsoft.com/technet/security/current.aspx
- Some vulnerabilities cannot be definitively identified
  - You'll have to check manually to see if a system is vulnerable
  - The scanner gives you a heads-up

CVE-2020-25079 — An issue was discovered on D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices. cgi-bin/ddns_enc.cgi allows authenticated command injection.
Published: September 02, 2020; 12:15:12 PM -04:00
V3.1: 8.8 HIGH
V2: 9.0 HIGH

1.7 - Vulnerability Scans (continued)

- National Vulnerability Database: http://nvd.nist.gov/
  - Synchronized with the CVE list
  - Enhanced search functionality
- Common Vulnerability Scoring System (VCSS)
  - Quantitative scoring of a vulnerability - 0 to 10
  - The scoring standards change over time
  - Different scoring for VCSS 2.0 vs VCSS 3.x
- Industry collaboration
  - Enhanced feed sharing and automation

Vulnerability scan log review

- Lack of security controls
  - No firewall
  - No anti-virus
  - No anti-spyware
- Misconfigurations
  - Open shares
  - Guest access
- Real vulnerabilities
  - Especially newer ones
  - Occasionally the old ones

Dealing with false positives

- False positives
  - A vulnerability is identified that doesn't really exist
- This is different than a low-severity vulnerability
  - It's real, but it may not be your highest priority
- False negatives
  - A vulnerability exists, but you didn't detect it
- Update to the latest signatures
  - If you don't know about it, you can't see it
- Work with the vulnerability detection manufacturer
  - They may need to update their signatures for your environment

Configuration review

- Validate the security of device configurations
  - It's easy to misconfigure one thing
  - A single unlocked window puts the entire home at risk
- Workstations
  - Account configurations, local device settings
- Servers - Access controls, permission settings
- Security devices - Firewall rules, authentication options

1.7 - Security Information and Event Management

SIEM

- Security Information and Event Management
  - Logging of security events and information
- Log collection of security alerts
  - Real-time information
- Log aggregation and long-term storage
  - Usually includes advanced reporting features
- Data correlation - Link diverse data types
- Forensic analysis - Gather details after an event

Syslog

- Standard for message logging
  - Diverse systems, consolidated log
- Usually a central log collector
  - Integrated into the SIEM
- You're going to need a lot of disk space
  - No, more. More than that.
  - Data storage from many devices over an extended timeframe

SIEM data

- Data inputs
  - Server authentication attempts
  - VPN connections
  - Firewall session logs
  - Denied outbound traffic flows
  - Network utilizations
- Packet captures
  - Network packets
  - Often associated with a critical alert
  - Some organizations capture everything

Security monitoring

- Constant information flow
  - Important metrics in the incoming logs
- Track important statistics
  - Exceptions can be identified
- Send alerts when problems are found
  - Email, text, call, etc.
- Create triggers to automate responses
  - Open a ticket, reboot a server

Analyzing the data

- Big data analytics
  - Analyze large data stores
  - Identify patterns that would normally remain invisible
- User and entity behavior analytics (UEBA)
  - Detect insider threats
  - Identify targeted attacks
  - Catches what the SIEM and DLP systems might miss
- Sentiment analysis
  - Public discourse correlates to real-world behavior
  - If they hate you, they hack you
  - Social media can be a barometer

SOAR

- Security orchestration, automation, and response
  - Automate routine, tedious, and time intensive activities
- Orchestration
  - Connect many different tools together
  - Firewalls, account management, email filters
- Automation - Handle security tasks automatically
- Response - Make changes immediately

1.8 - Penetration Testing

Penetration testing
- Pentest
  - Simulate an attack
- Similar to vulnerability scanning
  - Except we actually try to exploit the vulnerabilities
- Often a compliance mandate
  - Regular penetration testing by a 3rd-party
- National Institute of Standards and Technology Technical Guide to Information Security Testing and Assessment
  - https://professormesser.link/800115 (PDF)

Rules of engagement
- An important document
  - Defines purpose and scope
  - Makes everyone aware of the test parameters
- Type of testing and schedule
  - On-site physical breach, internal test, external test
  - Normal working hours, after 6 PM only, etc.
- The rules
  - IP address ranges
  - Emergency contacts
  - How to handle sensitive information
  - In-scope and out-of-scope devices or applications

Working knowledge
- How much do you know about the test?
  - Many different approaches
- Unknown environment
  - The pentester knows nothing about the systems under attack
  - "Blind" test
- Known environment
  - Full disclosure
- Partially known environment
  - A mix of black and white
  - Focus on certain systems or applications

Exploiting vulnerabilities
- Try to break into the system
  - Be careful; this can cause a denial of service or loss of data
  - Buffer overflows can cause instability
  - Gain privilege escalation
- You may need to try many different vulnerability types
  - Password brute-force, social engineering, database injections, buffer overflows
- You'll only be sure you're vulnerable if you can bypass security
  - If you can get through, the attackers can get through

The process
- Initial exploitation - Get into the network
- Lateral movement
  - Move from system to system
  - The inside of the network is relatively unprotected
- Persistence
  - Once you're there, you need to make sure there's a way back in
  - Set up a backdoor, build user accounts, change or verify default passwords
- The pivot
  - Gain access to systems that would normally not be accessible
  - Use a vulnerable system as a proxy or relay

Pentest aftermath
- Cleanup
  - Leave the network in its original state
  - Remove any binaries or temporary files
  - Remove any backdoors
  - Delete user accounts created during the test
- Bug bounty
  - A reward for discovering vulnerabilities
  - Earn money for hacking a system
  - Document the vulnerability to earn cash

1.8 - Reconnaissance

Reconnaissance
- Need information before the attack
  - Can't rush blindly into battle
- Gathering a footprint
  - Learn everything you can
- Understand the security posture
  - Firewalls, security configurations
- Minimize the attack area
  - Focus on key systems
- Create a network map
  - Identify routers, networks, remote sites

Passive footprinting
- Learn as much as you can from open sources
  - There's a lot of information out there
  - Remarkably difficult to protect or identify
- Social media
- Corporate web site
- Online forums, Reddit
- Social engineering
- Dumpster diving
- Business organizations

1.8 - Reconnaissance (continued)

Wardriving or warflying
- Combine WiFi monitoring and a GPS
  - Search from your car or plane
  - Search from a drone
- Huge amount of intel in a short period of time
  - And often some surprising results
- All of this is free
  - Kismet, inSSIDer
  - Wireless Geographic
  - Logging Engine
  - http://wigle.net

Open Source Intelligence (OSINT)
- Gathering information from many open sources
  - Find information on anyone or anything
  - The name is not related to open-source software
- Data is everywhere - https://osintframework.com/
- Automated gathering - Many software tools available

Active footprinting
- Trying the doors
  - Maybe one is unlocked
  - Don't open it yet
  - Relatively easy to be seen
- Visible on network traffic and logs
- Ping scans, port scans, DNS queries, OS scans, OS fingerprinting, Service scans, version scans

1.8 - Security Teams

Security teams
- Cybersecurity involves many skills
  - Operational security, penetration testing, exploit research, web application hardening, etc.
- Become an expert in your niche
  - Everyone has a role to play
- The teams
  - Red team, blue team, purple team, white team

Red team
- Offensive security team - The hired attackers
- Ethical hacking - Find security holes
- Exploit vulnerabilities -Gain access
- Social engineering - Constant vigilance
- Web application scanning - Test and test again

Blue team
- Defensive security - Protecting the data
- Operational security - Daily security tasks
- Incident response - Damage control
- Threat hunting - Find and fix the holes
- Digital forensics - Find data everywhere

Purple team
- Red and blue teams
  - Working together
- Competition isn't necessarily useful
  - Internal battles can stifle organizational security
  - Cooperate instead of compete
- Deploy applications and data securely
  - Everyone is on-board
- Create a feedback loop
  - Red informs blue, blue informs red

White team
- Not on a side
  - Manages the interactions between red teams and blue teams
- The referees in a security exercise
  - Enforces the rules
  - Resolves any issues
  - Determines the score
- Manages the post-event assessments
  - Lessons learned
  - Results

2.1 - Configuration Management

Configuration management
- The only constant is change
  - Operating systems, patches, application updates, network modifications, new application instances, etc.
- Identify and document hardware and software settings
  - Manage the security when changes occur
- Rebuild those systems if a disaster occurs
  - Documentation and processes will be critical

Diagrams
- Network diagrams - Document the physical wire and device
- Physical data center layout
  - Can include physical rack locations
- Device diagrams - Individual cabling

Baseline configuration
- The security of an application environment should be well defined
  - All application instances must follow this baseline
  - Firewall settings, patch levels, OS file versions
  - May require constant updates
- Integrity measurements check for the secure baseline
  - These should be performed often
  - Check against well-documented baselines
  - Failure requires an immediate correction

2.1 - Configuration Management (continued)

Standard naming conventions
- Create a standard
  - Needs to be easily understood by everyone
- Devices
  - Asset tag names and numbers
  - Computer names - location or region
  - Serial numbers
- Networks - Port labeling
- Domain configurations
  - User account names
  - Standard email addresses

IP schema
- An IP address plan or model
  - Consistent addressing for network devices
  - Helps avoid duplicate IP addressing
- Locations
  - Number of subnets, hosts per subnet
- IP ranges
  - Different sites have a different subnet
  - 10.1.x.x/24, 10.2.x.x/24, 10.3.x.x/24
- Reserved addresses
  - Users, printers, routers/default gateways

2.1 - Protecting Data

Protecting Data
- A primary job task
  - An organization is out of business without data
- Data is everywhere
  - On a storage drive, on the network, in a CPU
- Protecting the data
  - Encryption, security policies
- Data permissions
  - Not everyone has the same access

Data sovereignty
- Data sovereignty
  - Data that resides in a country is subject to the laws of that country
  - Legal monitoring, court orders, etc.
- Laws may prohibit where data is stored
  - GDPR (General Data Protection Regulation)
  - Data collected on EU citizens must be stored in the EU
  - A complex mesh of technology and legalities
- Where is your data stored?
  - Your compliance laws may prohibit moving data out of the country

Data masking
- Data obfuscation
  - Hide some of the original data
- Protects PII
  - And other sensitive data
- May only be hidden from view
  - The data may still be intact in storage
  - Control the view based on permissions
- Many different techniques
  - Substituting, shuffling, encrypting, masking out, etc.

Data encryption
- Encode information into unreadable data
  - Original information is plaintext, encrypted form is ciphertext
- This is a two-way street
  - Convert between one and the other
  - If you have the proper key
- Confusion
  - The encrypted data is drastically different than the plaintext
- Diffusion
  - Change one character of the input, and many characters change of the output

Data at-rest
- The data is on a storage device
  - Hard drive, SSD, flash drive, etc.
- Encrypt the data
  - Whole disk encryption
  - Database encryption
  - File- or folder-level encryption
- Apply permissions
  - Access control lists
  - Only authorized users can access the data

Data in-transit
- Data transmitted over the network
  - Also called data in-motion
- Not much protection as it travels
  - Many different switches, routers, devices
- Network-based protection
  - Firewall, IPS
- Provide transport encryption
  - TLS (Transport Layer Security)
  - IPsec (Internet Protocol Security)

Data in-use
- Data is actively processing in memory
  - System RAM, CPU registers and cache
- The data is almost always decrypted
  - Otherwise, you couldn't do anything with it
- The attackers can pick the decrypted information out of RAM
  - A very attractive option
- Target Corp. breach - November 2013
  - 110 million credit cards
  - Data in-transit encryption and data at-rest encryption
  - Attackers picked the credit card numbers out of the point-of-sale RAM

2.1 - Protecting Data (continued)

Tokenization
- Replace sensitive data with a non-sensitive placeholder
  - SSN 266-12-1112 is now 691-61-8539
- Common with credit card processing
  - Use a temporary token during payment
  - An attacker capturing the card numbers can't use them later
- This isn't encryption or hashing
  - The original data and token aren't mathematically related
  - No encryption overhead

Information Rights Management (IRM)
- Control how data is used
  - Microsoft Office documents, email messages, PDFs
- Restrict data access to unauthorized persons
  - Prevent copy and paste
  - Control screenshots
  - Manage printing
  - Restrict editing
- Each user has their own set of rights
  - Attackers have limited options

2.1 - Data Loss Prevention

Data Loss Prevention (DLP)
- Where's your data?
  - Social Security numbers, credit card numbers, medical records
- Stop the data before the attackers get it
  - Data "leakage"
- So many sources, so many destinations
  - Often requires multiple solutions in different places

Data Loss Prevention (DLP) systems
- On your computer
  - Data in use
  - Endpoint DLP
- On your network
  - Data in motion
- On your server
  - Data at rest

USB blocking
- DLP on a workstation
  - Allow or deny certain tasks
- November 2008 - U.S. Department of Defense
  - Worm virus "agent.btz" replicates using USB storage
  - Bans removable flash media and storage devices
- All devices had to be updated
  - Local DLP agent handled USB blocking
- Ban was lifted in February 2010
  - Replaced with strict guidelines

Cloud-based DLP
- Located between users and the Internet
  - Watch every byte of network traffic
  - No hardware, no software
- Block custom defined data strings
  - Unique data for your organization
- Manage access to URLs
  - Prevent file transfers to cloud storage
- Block viruses and malware
  - Anything traversing the network

DLP and email
- Email continues to be the most critical risk vector
  - Inbound threats, outbound data loss
- Check every email inbound and outbound
  - Internal system or cloud-based
- Inbound - Block keywords, identify impostors, quarantine email messages
- Outbound - Fake wire transfers, W-2 transmissions, employee information

Emailing a spreadsheet template
- November 2016 - Boeing employee emails spouse a spreadsheet to use as a template
- Contained the PII of 36,000 Boeing employees
  - In hidden columns
  - Social security numbers, date of birth, etc.
- Boeing sells its own DLP software
  - But only uses it for classified work

2.1 - Managing Security

Geographical considerations
- Legal implications
  - Business regulations vary between states
  - For a recovery site outside of the country, personnel must have a passport and be able to clear immigration
  - Refer to your legal team
- Offsite backup
  - Organization-owned site or 3rd-party secure facility
- Offsite recovery
  - Hosted in a different location, outside the scope of the disaster
  - Travel considerations for support staff and employees

Response and recovery controls
- Incident response and recovery has become commonplace
  - Attacks are frequent and complex
- Incident response plan should be established
  - Documentation is critical
  - Identify the attack
  - Contain the attack
- Limit the impact of an attacker
  - Limit data exfiltration
  - Limit access to sensitive data

2.1 - Managing Security (continued)

SSL/TLS inspection
- Commonly used to examine outgoing SSL/TLS
  - Secure Sockets Layer/Transport Layer Security
  - For example, from your computer to your bank
- Wait a second. Examine encrypted traffic?
  - Is that possible?
- SSL/TLS relies on trust
  - Without trust, none of this works

Trust me, I'm SSL
- Your browser contains a list of trusted CAs
  - My browser contains about 170 trusted CAs certificates
- Your browser doesn't trust a web site unless a CA has signed the web server's encryption certificate
  - The web site pays some money to the CA for this
- The CA has ostensibly performed some checks
  - Validated against the DNS record, phone call, etc.
- Your browser checks the web server's certificate
  - If it's signed by a trusted CA, the encryption works seamlessly

Hashing
- Represent data as a short string of text
  - A message digest
- One-way trip
  - Impossible to recover the original message from the digest
  - Used to store passwords / confidentiality
- Verify a downloaded document is the same as the original
  - Integrity
- Can be a digital signature
  - Authentication, non-repudiation, and integrity
- Will not have a collision (hopefully)
  - Different messages will not have the same hash

API considerations
- API (Application Programming Interface)
  - Control software or hardware programmatically
- Secure and harden the login page
  - Don't forget about the API
- On-path attack
  - Intercept and modify API messages, replay API commands
- API injection
  - Inject data into an API message
- DDoS (Distributed Denial of Service)
  - One bad API call can bring down a system

API security
- Authentication
  - Limit API access to legitimate users
  - Over secure protocols
- Authorization
  - API should not allow extended access
  - Each user has a limited role
  - A read-only user should not be able to make changes
- WAF (Web Application Firewall)
  - Apply rules to API communication

2.1 - Site Resiliency

Site resiliency
- Recovery site is prepped
  - Data is synchronized
- A disaster is called
  - Business processes failover to the alternate processing site
- Problem is addressed
  - This can take hours, weeks, or longer
- Revert back to the primary location
  - The process must be documented for both directions

Hot site
- An exact replica
  - Duplicate everything
- Stocked with hardware
  - Constantly updated
  - You buy two of everything
- Applications and software are constantly updated
  - Automated replication
- Flip a switch and everything moves
  - This may be quite a few switches

Cold Site
- No hardware
  - Empty building
- No data
  - Bring it with you
- No people
  - Bus in your team

Warm site
- Somewhere between cold and hot
  - Just enough to get going
- Big room with rack space
  - You bring the hardware
- Hardware is ready and waiting
  - You bring the software and data

2.1 - Honeypots and Deception

Honeypots
- Attract the bad guys
  - And trap them there
- The "attacker" is probably a machine
  - Makes for interesting recon
- Honeypots
  - Create a virtual world to explore
- Many different options
  - Kippo, Google Hack Honeypot, Wordpot, etc.
- Constant battle to discern the real from the fake

Honeyfiles and honeynets
- Honeynets
  - More than one honeypot on a network
  - More than one source of information
  - Stop spammers - https://projecthoneypot.org
- Honeyfiles
  - Bait for the honeynet (passwords.txt)
  - An alert is sent if the file is accessed
  - A virtual bear trap

Fake telemetry
- Machine learning
  - Interpret big data to identify the invisible
- Train the machine with actual data
  - Learn how malware looks and acts
  - Stop malware based on actions instead of signatures
- Send the machine learning model fake telemetry
  - Make malicious malware look benign

DNS sinkhole
- A DNS that hands out incorrect IP addresses
  - Blackhole DNS
- This can be bad
  - An attacker can redirect users to a malicious site
- This can be good
  - Redirect known malicious domains to a benign IP address
  - Watch for any users hitting that IP address
  - Those devices are infected
- Can be integrated with a firewall
  - Identify infected devices not directly connected

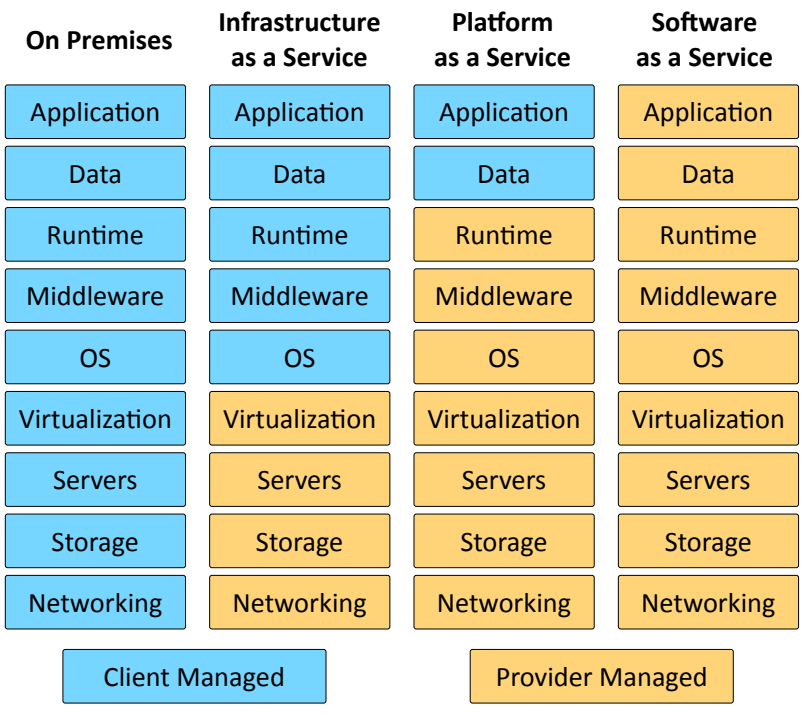
2.2 - Cloud Models

Infrastructure as a service (IaaS)
- Sometimes called Hardware as a Service (HaaS)
  - Outsource your equipment
- You're still responsible for the management
  - And for the security
- Your data is out there, but more within your control
- Web server providers

Platform as a service (PaaS)
- No servers, no software, no maintenance team, no HVAC
  - Someone else handles the platform, you handle the development
- You don't have direct control of the data, people, or infrastructure
  - Trained security professionals are watching your stuff
  - Choose carefully
- Put the building blocks together
  - Develop your app from what's available on the platform
  - SalesForce.com

Software as a service (SaaS)
- On-demand software
  - No local installation
  - Why manage your own email distribution?
  - Or payroll?
- Central management of data and applications
  - Your data is out there
- A complete application offering
  - No development work required
  - Google Mail

Anything as a Service (XaaS)
- A broad description of all cloud models
  - Use any combination of the cloud
- Services delivered over the Internet
  - Not locally hosted or managed
- Flexible consumption model
  - No large upfront costs or ongoing licensing
- IT becomes more of an operating model
  - And less of a cost-center model
  - Any IT function can be changed into a service



2.2 - Cloud Models (continued)

Cloud service providers
- Provide cloud services
  - SaaS, PaaS, IaaS, etc.
- Charge a flat fee or based on use
  - More data, more cost
- You still manage your processes
  - Internal staff
  - Development team
  - Operational support

Managed service providers
- Managed Service Provider (MSP)
  - Also a cloud service provider
  - Not all cloud service providers are MSPs
- MSP support
  - Network connectivity management
  - Backups and disaster recovery
  - Growth management and planning
- Managed Security Service Provider (MSSP)
  - Firewall management
  - Patch management, security audits
  - Emergency response

On-premises vs. off-premises
- On-premises
  - Your applications are on local hardware
  - Your servers are in your data center in your building
- Off-premises / hosted
  - Your servers are not in your building
  - They may not even be running on your hardware
  - Usually a specialized computing environment

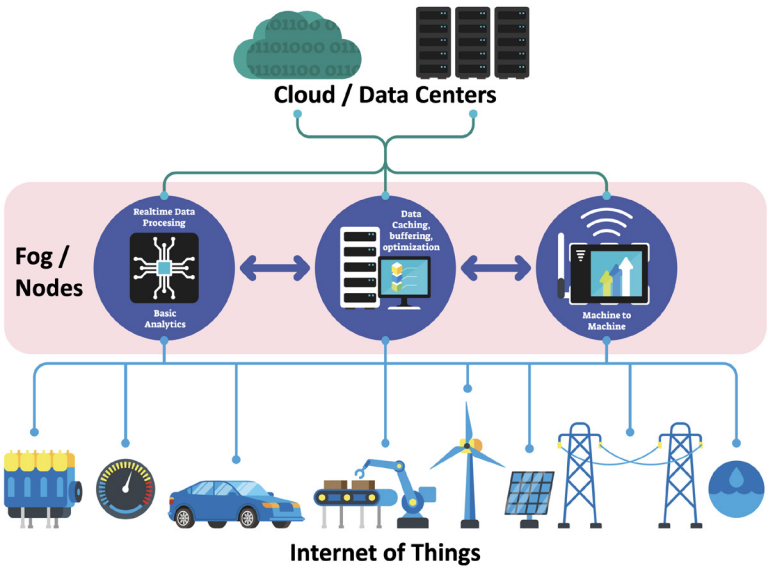
Cloud deployment models
- Public
  - Available to everyone over the Internet
- Community
  - Several organizations share the same resources
- Private
  - Your own virtualized local data center
- Hybrid
  - A mix of public and private

2.2 - Edge and Fog Computing

Cloud computing
- Computing on-demand
  - Instantly available computing power
  - Massive data storage capacity
- Fast implementation
  - IT teams can adjust rapidly to change
  - Smaller startup costs and pay-as-you-go
- Not always the best solution
  - Latency - the cloud is far away
  - Limited bandwidth
  - Difficult to protect data
  - Requires Internet/network connectivity

Edge computing
- Over 30 billion IoT devices on the Internet
  - Devices with very specific functions
  - A huge amount of data
- Edge computing - "Edge"
  - Process application data on an edge server
  - Close to the user
- Often process data on the device itself
  - No latency, no network requirement
  - Increased speed and performance
  - Process where the data is, instead of processing in the cloud

Fog computing
- Fog
  - A cloud that's close to your data
  - Cloud + Internet of Things - Fog computing
- A distributed cloud architecture - Extends the cloud
- Distribute the data and processing
  - Immediate data stays local - No latency
  - Local decisions made from local data
  - No bandwidth requirements
  - Private data never leaves - Minimizes security concerns
  - Long-term analysis can occur in the cloud - Internet only when required



2.2 - Designing the Cloud

Designing the cloud
- On-demand computing power
  - Click a button
- Elasticity
  - Scale up or down as needed
- Applications also scale
  - Access from anywhere
- How does it all happen?
  - Planning and technology

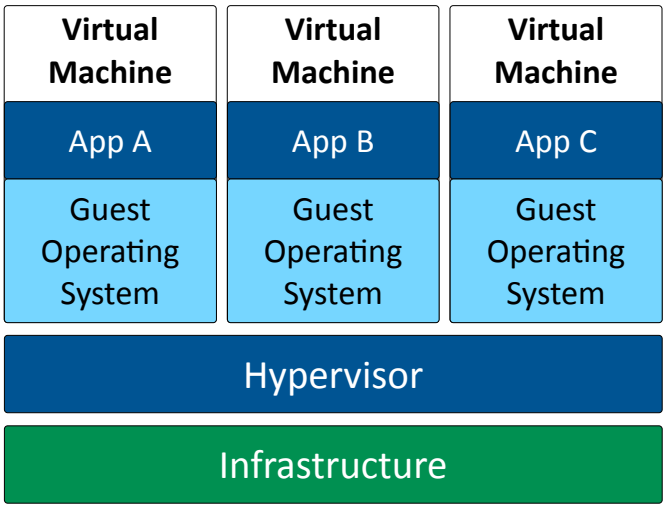
Thin client
- Basic application usage
  - Applications actually run on a remote server
  - Virtual Desktop Infrastructure (VDI),
  - Desktop as a Service (DaaS)
  - Local device is a keyboard, mouse, and screen.
- Minimal operating system on the client
  - No huge memory or CPU needs
- Network connectivity
  - Big network requirement
  - Everything happens across the wire

Virtualization
- Virtualization
  - Run many different operating systems on the same hardware
- Each application instance has its own operating system
  - Adds overhead and complexity
  - Virtualization is relatively expensive

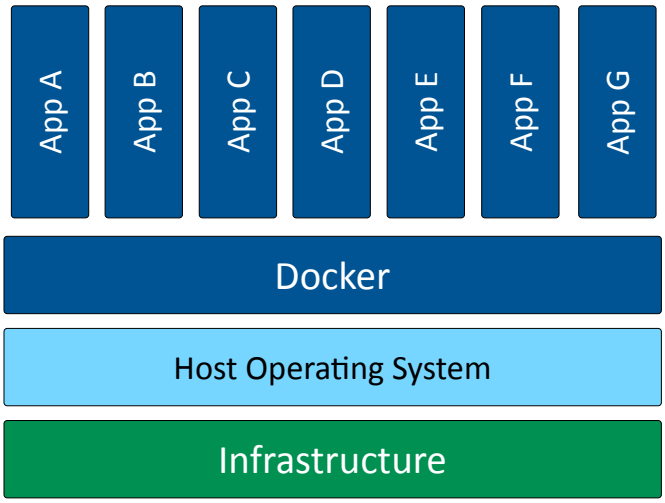
Application containerization
- Container
  - Contains everything you need to run an application
  - Code and dependencies
  - A standardized unit of software
- An isolated process in a sandbox
  - Self-contained
  - Apps can't interact with each other
- Container image
  - A standard for portability
  - Lightweight, uses the host kernel
  - Secure separation between applications

Microservices and APIs
- Monolithic applications
  - One big application that does everything
- Application contains all decision making processes
  - User interface
  - Business logic
  - Data input and output
- Code challenges
  - Large codebase
  - Change control challenges
- APIs
  - Application Programming Interfaces
- API is the "glue" for the microservices
  - Work together to act as the application
- Scalable
  - Scale just the microservices you need
- Resilient
  - Outages are contained
- Security and compliance
  - Containment is built-in

Virtualized Applications



Containerized Applications

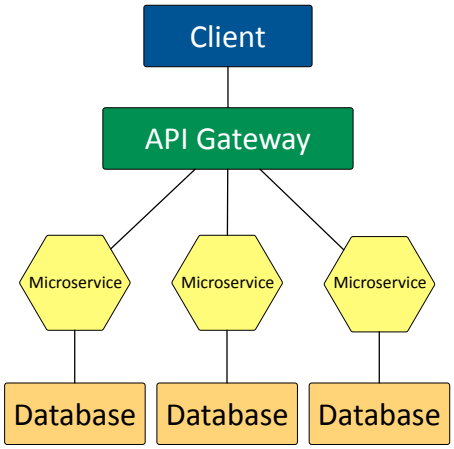


2.2 - Designing the Cloud (continued)

Serverless architecture

- Function as a Service (FaaS)
  - Applications are separated into individual, autonomous functions
  - Remove the operating system from the equation
- Developer still creates the server-side logic
  - Runs in a stateless compute container
- May be event triggered and ephemeral
  - May only run for one event
- Managed by a third-party
  - All OS security concerns are at the third-party

Microservice Architecture



Transit gateway

- Virtual Private Cloud (VPC)
  - A pool of resources created in a public cloud
- Common to create many VPCs
  - Many different application clouds
- Connect VPCs with a transit gateway
  - And users to VPCs
  - A "cloud router"
- Now make it secure
  - VPCs are commonly on different IP subnets
  - Connecting to the cloud is often through a VPN

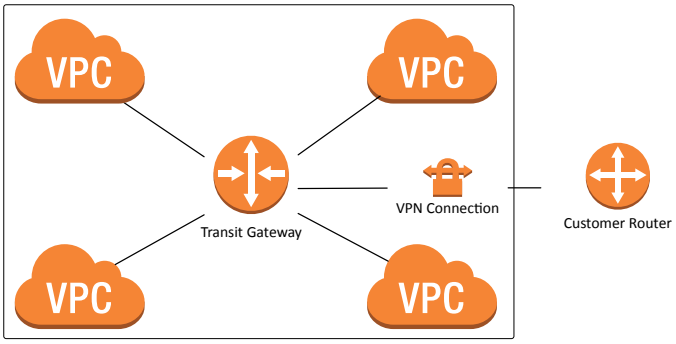
Resource policies

- Assigning permissions to cloud resources
  - Not the easiest task
  - Everything is in constant motion
- Specify which resources can be provisioned (Azure)
  - Create a service in a specific region, deny all others
- Specify the resource and what actions are permitted (Amazon)
  - Allow access to an API gateway from an IP address range
- Explicitly list the users who can access the resource (Amazon)
  - Userlist is associated with the resource

Service integration

- Service Integration and Management (SIAM)
- Many different service providers
  - The natural result of multisourcing
- Every provider works differently
  - Different tools and processes
- SIAM is the integration of these diverse providers
  - Provide a single business-facing IT organization
- An evolving set of processes and procedures

Transit Gateway Network Architecture



2.2 - Infrastructure as Code

Infrastructure as code

- Describe an infrastructure
  - Define servers, network, and applications as code
- Modify the infrastructure and create versions
  - The same way you version application code
- Use the description (code) to build other application instances
  - Build it the same way every time based on the code
- An important concept for cloud computing
  - Build a perfect version every time

SDN (Software Defined Networking)

- Networking devices have two functional planes of operation
  - Control plane, data plane
- Directly programmable
  - Configuration is different than forwarding
- Agile - Changes can be made dynamically
- Centrally managed - Global view, single pane of glass
- Programmatically configured
  - No human intervention
- Open standards / vendor neutral
  - A standard interface to the network

2.2 - Infrastructure as Code (continued)

SDV (Software Defined Visibility)
- You must see the traffic to secure the data
  - React and respond
- Dynamic deployments include security and network visibility devices
  - Next-generation firewalls, web application firewalls,
  - Security Information and Event Management (SIEM)
- Data is encapsulated and encrypted
  - VXLAN and SSL/TLS
- New technologies change what you can see
  - Infrastructure as code, microservices
- Security devices monitor application traffic
  - SDV provides visibility to traffic flows
- Visibility expands as the application instances expand
  - Real-time metrics across all traffic flows
- Application flows can be controlled via API
  - Identify and react to threats

2.2 - Virtualization Security

VM sprawl avoidance
- Click a button
  - You've built a server
  - Or multiple servers, networks, and firewalls
- It becomes almost too easy to build instances
  - This can get out of hand very quickly
- The virtual machines are sprawled everywhere
  - You aren't sure which VMs are related to which applications
  - It becomes extremely difficult to deprovision
- Formal process and detailed documentation
  - You should have information on every virtual object

VM escape protection
- The virtual machine is self-contained
  - There's no way out - Or is there?
- Virtual machine escape
  - Break out of the VM and interact with the host operating system or hardware
- Once you escape the VM, you have great control
  - Control the host and control other guest VMs
- This would be a huge exploit
  - Full control of the virtual world

Escaping the VM
- March 2017 - Pwn2Own competition
  - Hacking contest
  - You pwn it, you own it - along with some cash
- JavaScript engine bug in Microsoft Edge
  - Code execution in the Edge sandbox
- Windows 10 kernel bug
  - Compromise the guest operating system
- Hardware simulation bug in VMware
  - Escape to the host
- Patches were released soon afterwards

2.3 - Secure Deployments

Development to production
- Your programming team has been working on a new application
  - How will you deploy it safely and reliably?
- Patch Tuesday
  - Test and deploy Wednesday? Thursday? Friday?
- Manage the process
  - Safely move from a non-production phase to full production

Sandboxing
- Isolated testing environment
  - No connection to the real world or production system
  - A technological safe space
- Use during the development process
  - Try some code, break some code, nobody gets hurt
- Incremental development
  - Helps build the application

Building the application
- Development
  - Secure environment
  - Writing code
  - Developers test in their sandboxes
- Test
  - Still in the development stage
  - All of the pieces are put together
  - Does it all work?
  - Functional tests
  - If it works in test, then it's ready for staging

Verifying the application
- Quality Assurance (QA)
  - Verifies features are working as expected
  - Validates new functionality
  - Verifies old errors don't reappear
- Staging
  - Almost ready to roll it out
  - Works and feels exactly like the production environment
  - Working with a copy of production data
  - Run performance tests
  - Test usability and features

2.3 - Secure Deployments (continued)

Using the application
- Production
  - Application is live
  - Rolled out to the user community
- A challenging step
  - Impacts the users
- Logistical challenges
  - New servers
  - New software
  - Restart or interrupt of service

Secure baselines
- The security of an application environment should be well defined
  - All application instances must follow this baseline
  - Firewall settings, patch levels, OS file versions
  - May require constant updates
- Integrity measurements check for the secure baseline
  - These should be performed often
  - Check against well-documented baselines
  - Failure requires an immediate correction

2.3 - Provisioning and Deprovisioning

Provisioning
- Deploy an application
  - Web server, database server, middleware server, user workstation configurations, certificate updates, etc.
- Application software security
  - Operating system, application
- Network security
  - Secure VLAN, internal access, external access
- Software deployed to workstations
  - Check executables for malicious code, verify security posture of the workstation

Scalability and elasticity
- Handle application workload
  - Adapt to dynamic changes
- Scalability
  - The ability to increase the workload in a given infrastructure
  - Build an application instance that can handle
  - 100,000 transactions per second
- Elasticity
  - Increase or decrease available resources as the workload changes
  - Deploy multiple application instances to handle
  - 500,000 transactions per second

Orchestration
- Automation is the key to cloud computing
  - Services appear and disappear automatically, or at the push of a button
- Entire application instances can be instantly provisioned
  - All servers, networks, switches, firewalls, and policies
- Instances can move around the world as needed
  - Follow the sun
- The security policies should be part of the orchestration
  - As applications are provisioned, the proper security is automatically included

Deprovisioning
- Dismantling and removing an application instance
  - All good things
- Security deprovisioning is important
  - Don't leave open holes, don't close important ones
- Firewall policies must be reverted
  - If the application is gone, so is the access
- What happens to the data?
  - Don't leave information out there

2.3 - Secure Coding Techniques

Secure coding concepts
- A balance between time and quality
  - Programming with security in mind is often secondary
- Testing, testing, testing
  - The Quality Assurance (QA) process
- Vulnerabilities will eventually be found
  - And exploited

Input validation
- What is the expected input?
  - Validate actual vs. expected
- Document all input methods
  - Forms, fields, type
- Check and correct all input (normalization)
  - A zip code should be only X characters long with a letter in the X column
  - Fix any data with improper input
- The fuzzers will find what you missed
  - Don't give them an opening

Stored procedures
- SQL databases
  - Client sends detailed requests for data
  - 'SELECT * FROM wp_options WHERE option_id = 1'
- Client requests can be complex
  - And sometimes modified by the user
  - This would not be good

2.3 - Secure Coding Techniques (continued)

- Stored procedures limit the client interactions
  - 'CALL get_options'
  - That's it. No modifications to the query are possible.
- To be really secure, use only stored procedures
  - The application doesn't use any SQL queries

Obfuscation/camouflage

- Obfuscate
  - Make something normally understandable very difficult to understand
- Take perfectly readable code and turn it into nonsense
  - The developer keeps the readable code and gives you the chicken scratch
  - Both sets of code perform exactly the same way
- Helps prevent the search for security holes
  - Makes it more difficult to figure out what's happening - But not impossible

Code reuse/dead code

- Code reuse
  - Use old code to build new applications
  - Copy and paste
- If the old code has security vulnerabilities, reusing the code spreads it to other applications
  - You're making this much more difficult for everyone
- Dead code
  - Calculations are made, code is executed, results are tallied
  - The results aren't used anywhere else in the application
- All code is an opportunity for a security problem
  - Make sure your code is as alive as possible

Validation points

- Server-side validation
  - All checks occur on the server
  - Helps protect against malicious users
  - Attackers may not even be using your interface
- Client-side validation
  - The end-user's app makes the validation decisions
  - Can filter legitimate input from genuine users
  - May provide additional speed to the user
- Use both - But especially server-side validation

Memory management

- As a developer, you must be mindful of how memory is used
  - Many opportunities to build vulnerable code
- Never trust data input
  - Malicious users can attempt to circumvent your code
- Buffer overflows are a huge security risk
  - Make sure your data matches your buffer sizes
- Some built-in functions are insecure
  - Use best practices when designing your code

Third-party libraries and SDKs

- Your programming language does everything - Almost
- Third-party libraries and software development kits
  - Extend the functionality of a programming language
- Security risk
  - Application code written by someone else
  - Might be secure. Might not be secure.
  - Extensive testing is required
- Balancing act - Application features vs. unknown code base

Data exposure

- So much sensitive data
  - Credit card numbers, social security numbers, medical information, address details, email information
- How is the application handling the data?
  - No encryption when stored
  - No encryption across the network
  - Displaying information on the screen
- All input and output processes are important
  - Check them all for data exposure

Version control

- Create a file, make a change, make another change, and another change
  - Track those changes, revert back to a previous version
- Commonly used in software development
  - But also in operating systems, wiki software, and cloud-based file storage
- Useful for security
  - Compare versions over time
  - Identify modifications to important files
  - A security challenge
  - Historical information can be a security risk

2.3 - Software Diversity

Exploiting an application

- Attackers often exploit application vulnerabilities
  - They find the unlocked door and open it
- Once you exploit one binary, you can exploit them all
  - The application works the same on all systems
  - A Windows 10 exploit affects all Windows 10 users
- What if all of the computers were running different software?
  - Unique binaries
  - Functionally identical

Software diversity

- Alternative compiler paths would result in a different binary each time
  - Each compiled application would be a little bit different
  - But functionally the same
- An attack against different binaries would only be successful on a fraction of the users
  - An attacker wouldn't know what exploit to use
  - Make the game much harder to win

2.3 - Automation and Scripting

Automation and scripting
- Plan for change
  - Implement automatically
- Automated courses of action
  - Many problems can be predicted
  - Have a set of automated responses
- Continuous monitoring
  - Check for a particular event, and then react
- Configuration validation
  - Cloud-based technologies allow for constant change
  - Automatically validate a configuration before going live
  - Perform ongoing automated checks

Continuous integration (CI)
- Code is constantly written
  - And merged into the central repository many times a day
- So many chances for security problems
  - Security should be a concern from the beginning
- Basic set of security checks during development
  - Documented security baselines as the bare minimum
- Large-scale security analysis during the testing phase
  - Significant problems will have already been covered

Continuous delivery/deployment (CD)
- Continuous delivery
  - Automate the testing process
  - Automate the release process
  - Click a button and deploy the application
- Continuous deployment
  - Even more automation
  - Automatically deploy to production
  - No human integration or manual checks

2.4 - Authentication Methods

Directory services
- Keep all of an organization's usernames and passwords in a single database
  - Also contains computers, printers, and other devices
- Large distributed database
  - Constantly replicated
- All authentication requests reference this directory
  - Each user only needs one set of credentials
  - One username and password for all services
- Access via Kerberos or LDAP

Federation
- Provide network access to others
  - Not just employees - Partners, suppliers, customers, etc.
  - Provides SSO and more
- Third-parties can establish a federated network
  - Authenticate and authorize between the two organizations
  - Login with your Facebook credentials
- The third-parties must establish a trust relationship
  - And the degree of the trust

Attestation
- Prove the hardware is really yours
  - A system you can trust
- Easy when it's just your computer
  - More difficult when there are 1,000
- Remote attestation
  - Device provides an operational report to a verification server
  - Encrypted and digitally signed with the TPM
  - An IMEI or other unique hardware component can be included in the report

Short message service (SMS)
- Text messaging
  - Includes more than text these days
- Login factor can be sent via SMS to a predefined phone number
  - Provide username and password
  - Phone receives an SMS
  - Input the SMS code into the login form
- Security issues exist
  - Phone number can be reassigned to a different phone
  - SMS messages can be intercepted

Push notification
- Similar process to an SMS notification
  - Authentication factor is pushed to a specialized app
  - Usually on a mobile device
- Security challenges
  - Applications can be vulnerable
  - Some push apps send in the clear
- Still more secure than SMS
  - Multiple factors are better than one factor

Authentication apps
- Pseudo-random token generators
  - A useful authentication factor
- Carry around a physical hardware token generator
  - Where are my keys again?
- Use software-based token generator on your phone
  - Powerful and convenient

2.4 - Authentication Methods (continued)

TOTP
- Time-based One-Time Password algorithm
  - Use a secret key and the time of day
  - No incremental counter
- Secret key is configured ahead of time
  - Timestamps are synchronized via NTP
- Timestamp usually increments every 30 seconds
  - Put in your username, password, and TOTP code
- One of the more common OTP methods
  - Used by Google, Facebook, Microsoft, etc.

HOTP
- One-time passwords
  - Use them once, and never again
  - Once a session, once each authentication attempt
- HMAC-based One-Time Password algorithm
  - Keyed-hash message authentication code (HMAC)
  - The keys are based on a secret key and a counter
- Token-based authentication
  - The hash is different every time
- Hardware and software tokens available
  - You'll need additional technology to make this work

Phone call
- A voice call provides the token
  - The computer is talking to you
  - "Your code is 1-6-2-5-1-7."
- Similar disadvantages to SMS
  - Phone call can be intercepted or forwarded
  - Phone number can be added to another phone

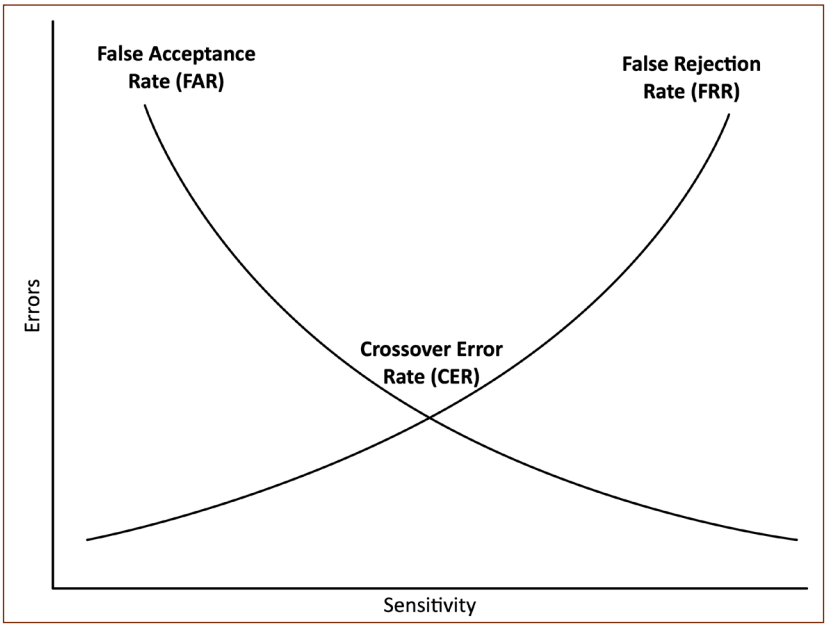
Static codes
- Authentication factors that don't change
  - You just have to remember
- Personal Identification Number (PIN)
  - Your secret numbers
- Can also be alphanumeric
  - A password or passphrase

Smart cards
- Integrated circuit card - Contact or contactless
- Common on credit cards - Also used for access control
- Must have physical card to provide digital access
  - A digital certificate
- Multiple factors
  - Use the card with a PIN or fingerprint

2.4 - Biometrics

Biometric factors
- Fingerprint scanner
  - Phones, laptops, door access
- Retinal scanner
  - Unique capillary structure in the back of the eye
- Iris scanner
  - Texture, color
- Voice recognition
  - Talk for access
- Facial recognition
  - Shape of the face and features
- Gait analysis
  - Identify a person based on how they walk
  - Many unique measurements
- Veins
  - Vascular scanners
  - Match the blood vessels visible from the surface of the skin

Biometric acceptance rates
- False acceptance rate (FAR)
  - Likelihood that an unauthorized user will be accepted
  - Not sensitive enough
- False rejection rate (FRR)
  - Likelihood that an authorized user will be rejected
  - Too sensitive
- Crossover error rate (CER)
  - Defines the overall accuracy of a biometric system
  - The rate at which FAR and FRR are equal
  - Adjust sensitivity to equalize both values



2.4 - Multi-factor Authentication

AAA framework
- Identification
  - This is who you claim to be
  - Usually your username
- Authentication
  - Prove you are who you say you are
  - Password and other authentication factors
- Authorization
  - Based on your identification and authentication, what access do you have?
- Accounting
  - Resources used: Login time, data sent and received, logout time

Cloud vs. on-premises authentication
- Cloud-based security
  - Third-party can manage the platform
  - Centralized platform
  - Automation options with API integration
  - May include additional options (for a cost)
- On-premises authentication system
  - Internal monitoring and management
  - Need internal expertise
  - External access must be granted and managed

Multi-factor authentication
- Factors
  - Something you know
  - Something you have
  - Something you are
- Attributes
  - Somewhere you are
  - Something you can do
  - Something you exhibit
  - Someone you know

Something you know
- Password
  - Secret word/phrase, string of characters
  - Very common authentication factor
- PIN
  - Personal identification number
  - Not typically contained anywhere on a smart card or ATM card
- Pattern
  - Complete a series of patterns
  - Only you know the right format

Something you have
- Smart card
  - Integrates with devices
  - May require a PIN
- USB token - Certificate is on the USB device
- Hardware or software tokens
  - Generates pseudo-random authentication codes
- Your phone -SMS a code to your phone

Something you are
- Biometric authentication
  - Fingerprint, iris scan, voice print
- Usually stores a mathematical representation of your biometric
  - Your actual fingerprint isn't usually saved
- Difficult to change
  - You can change your password
  - You can't change your fingerprint
- Used in very specific situations
  - Not foolproof

Somewhere you are
- Provide a factor based on your location
  - The transaction only completes if you are in a particular geography
- IP address
  - Not perfect, but can help provide more info
  - Works with IPv4, not so much with IPv6
- Mobile device location services
  - Geolocation to a very specific area
  - Must be in a location that can receive GPS information or near an identified mobile or 802.11 network
  - Still not a perfect identifier of location

Something you can do
- A personal way of doing things
  - You're special
- Handwriting analysis
  - Signature comparison
  - Writing technique
- Typing technique
  - Delays between keystrokes
- Very similar to biometrics
  - Close to something you are

Other attributes
- Something you exhibit
  - A unique trait, personal to you
  - Gait analysis - the way you walk
  - Typing analysis - the way you hit the enter key too hard

- Someone you know
  - A social factor
  - It's not what you know…
  - Web of trust
  - Digital signature

2.5 - Disk Redundancy

Redundancy
- Duplicate parts of the system
  - If a part fails, the redundant part can be used
- Maintain uptime
  - The organization continues to function
- No hardware failure
  - Servers keep running
- No software failure
  - Services always available
- No system failure
  - Network performing optimally

Geographic dispersal
- Bad things can happen in a local area
  - Hurricanes, tornadoes, flooding,
- Disperse technologies to different geographies
  - Use multiple data centers
  - In different locations
- Data centers might be part of the normal operations
  - East coast and west coast operations centers
- May be part of a disaster recovery center
  - If Florida gets hit, fire up the Denver data center

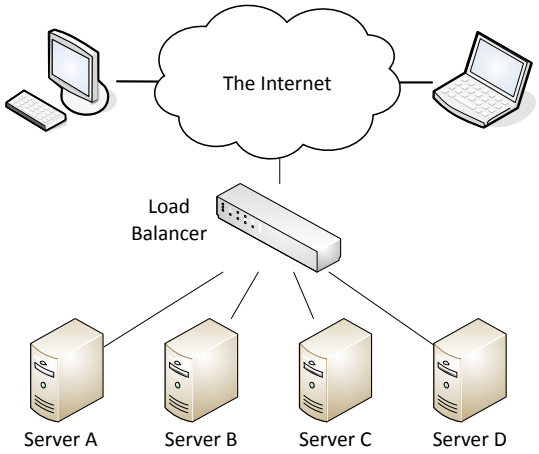
Disk redundancy
- Multipath I/O (Input/Output)
  - Especially useful for network-based storage subsystems
  - Multiple Fibre Channel interfaces with multiple switches
- RAID - Redundant Array of Independent Disks
- Multiple drives create redundancy
  - Many different designs and implementations

RAID Level	Description	Details
RAID 0	Striping without parity	High performance, no fault tolerance
RAID 1	Mirroring	Duplicates data for fault tolerance, but requires twice the disk space
RAID 5	Striping with parity	Fault tolerant, only requires an additional disk for redundancy
RAID 0+1, RAID 1+0, RAID 5+1, etc.	Multiple RAID types	Combine RAID methods to increase redundancy

2.5 - Network Redundancy

Load balancing
- Some servers are active - Others are on standby
- If an active server fails, the passive server takes its place

NIC teaming
- Load Balancing / Fail Over (LBFO)
  - Aggregate bandwidth, redundant paths
  - Becomes more important in the virtual world
- Multiple network adapters
  - Looks like a single adapter
  - Integrate with switches
- NICs talk to each other
  - Usually multicast instead of broadcast
  - Fails over when a NIC doesn't respond



2.5 - Power Redundancy

UPS - Uninterruptible Power Supply
- Short-term backup power
- Blackouts, brownouts, surges
- UPS types
  - Offline/Standby UPS
  - Line-interactive UPS
  - On-line/Double-conversion UPS
- Features
  - Auto shutdown, battery capacity, outlets, phone line suppression

Generators
- Long-term power backup
  - Fuel storage required
- Power an entire building
  - Some power outlets may be marked as generator-powered
- It may take a few minutes to get the generator up to speed
  - Use a battery UPS while the generator is starting

2.5 - Power Redundancy (continued)

Dual-power supplies
- Redundancy
  - Internal server power supplies
  - External power circuits
- Each power supply can handle 100% of the load
  - Would normally run at 50% of the load
- Hot-swappable
  - Replace a faulty power supply without powering down

Power distribution units (PDUs)
- Provide multiple power outlets
  - Usually in a rack
- Often include monitoring and control
  - Manage power capacity
  - Enable or disable individual outlets

2.5 - Replication

SAN replication
- Share data between different devices
  - If one device fails, you can still work with the data
  - VERY fast recovery times compared to traditional backups
- Storage area networks (SANs)
  - Specialized high-performance network of storage devices
- SAN-to-SAN replication
  - Duplicate data from one data center to another
- SAN snapshot
  - Create a state of data based on a point in time
  - Copy that state to other SANs

VM replication
- Virtual machine redundancy
  - Maintain one VM, replicate to all others
  - The virtual machine is really just one big file
- Consistent service offering
  - Maintain copies anywhere in the world
- Recover from a replicated copy
  - Provides a backup if needed
- Efficient copying
  - Only replicates the data that has changed

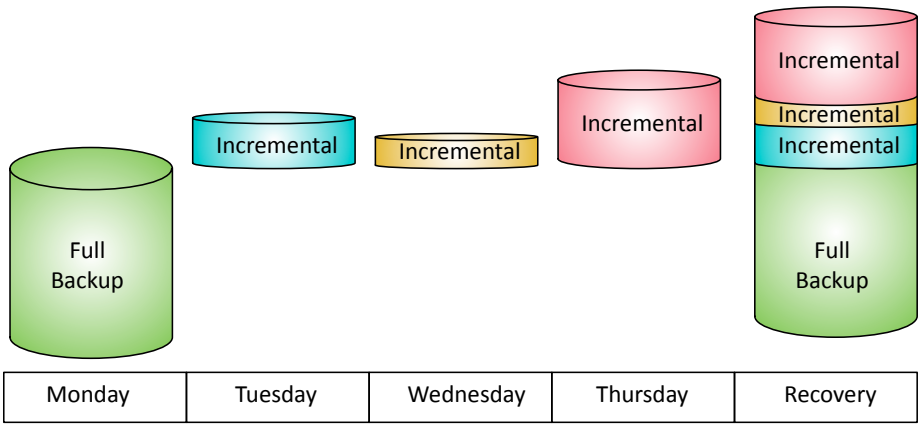
On premises vs. cloud redundancy
- Speed
  - Local devices are connect over very fast networks
  - Cloud connections are almost always slower
- Money
  - Purchasing your own storage is an expensive capital investment
  - Cloud costs have a low entry point and can scale
- Security
  - Local data is private
  - Data stored in the cloud requires additional security controls

2.5 - Backup Types

Backup Types
- The archive attribute
  - Set when a file is modified
- Full - Everything
  - You'll want this one first
- Incremental
  - All files changed since the last incremental backup
- Differential
  - All files changed since the last full backup

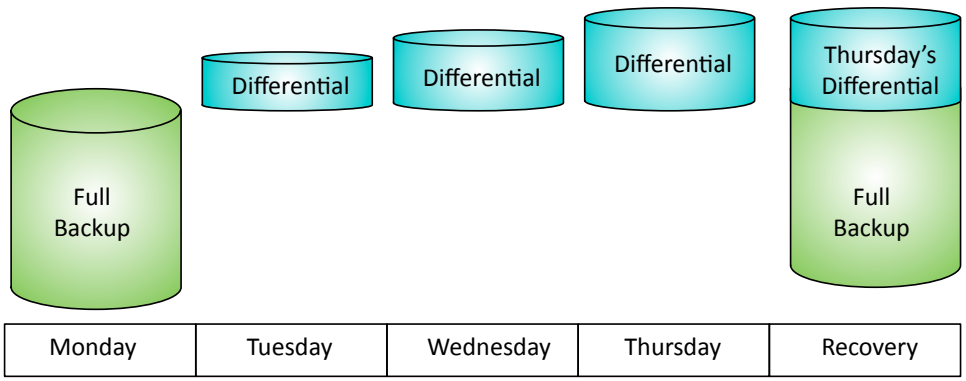
Type	Data Selection	Backup / Restore Time	Archive Attribute
Full	All selected data	High / Low (one tape set)	Cleared
Incremental	New files and files modified since the last backup	Low / High (Multiple tape sets)	Cleared
Differential	All data modified since the last full backup	Moderate / Moderate (No more than 2 sets)	Not Cleared

Incremental Backup
- A full backup is taken first
- Subsequent backups contain data changed since the last full backup and last incremental backup
  - These are usually smaller than the full backup
- A restoration requires the full backup and all of the incremental backups



2.5 - Backup Types (continued)

Differential Backup
- A full backup is taken first
- Subsequent backups contain data changed since the last full backup
  - These usually grow larger as data is changed
- A restoration requires the full backup and the last differential backup



Backup media
- Magnetic tape
  - Sequential storage
  - 100 GB to multiple terabytes per cartridge
  - Easy to ship and store
- Disk
  - Faster than magnetic tape - Deduplicate and compress
- Copy
  - A useful strategy
  - May not include versioning - May need to keep offsite

NAS vs. SAN
- Network Attached Storage (NAS)
  - Connect to a shared storage device across the network
  - File-level access
- Storage Area Network (SAN)
  - Looks and feels like a local storage device
  - Block-level access
  - Very efficient reading and writing
- Requires a lot of bandwidth
  - May use an isolated network and high-speed network technologies

Other backups
- Cloud
  - Backup to a remote device in the cloud
  - Support many devices
  - May be limited by bandwidth
- Image
  - Capture an exactly replica of everything on a storage drive
  - Restore everything on a partition, including operating system files and user documents

Backup locations
- Offline backup
  - Backup to local devices
  - Fast and secure
  - Must be protected and maintained
  - Often requires offsite storage for disaster recovery
- Online backup
  - Remote network-connected third-party
  - Encrypted
  - Accessible from anywhere
  - Speed is limited by network bandwidth

2.5 - Resiliency

Non-persistence
- The cloud is always in motion
  - Application instances are constantly built and torn down
- Snapshots can capture the current configuration and data
  - Preserve the complete state of a device, or just the configuration
- Revert to known state
  - Fall back to a previous snapshot
- Rollback to known configuration
  - Don't modify the data, but use a previous configuration
- Live boot media
  - Run the operating system from removable media - very portable!

High availability
- Redundancy doesn't always mean always available
  - May need to be powered on manually
- HA (high availability)
  - Always on, always available
- May include many different components working together
  - Active/Active can provide scalability advantages
- Higher availability almost always means higher costs
  - There's always another contingency you could add
  - Upgraded power, high-quality server components, etc.

Order of restoration
- Application-specific
  - Certain components may need to be restored first
  - Databases should be restored before the application
- Backup-specific
  - Incremental backups restore the full backup, then all subsequent incremental backups
  - Differential backups restore the full backup, then the last differential backup

2.5 - Resiliency (continued)

Diversity
- Technologies
  - A zero-day OS vulnerability can cause significant outages
  - Multiple security devices
- Vendors
  - A single vendor can become a disadvantage
  - No options during annual renewals
  - A bad support team may not be able to resolve problems in a timely manner
- Cryptographic
  - All cryptography is temporary
  - Diverse certificate authorities can provide additional protection
- Controls
  - Administrative controls
  - Physical controls
  - Technical controls
  - Combine them together
  - Defense in depth

2.6 - Embedded Systems

Embedded systems
- Hardware and software designed for a specific function
  - Or to operate as part of a larger system
- Is built with only this task in mind
  - Can be optimized for size and/or cost
- Common examples
  - Traffic light controllers
  - Digital watches
  - Medical imaging systems

SoC (System on a Chip)
- Multiple components running on a single chip
  - Common with embedded systems
- Small form-factor
  - External interface support
  - Cache memory, flash memory
  - Usually lower power consumption
- Security considerations are important
  - Difficult to upgrade hardware
  - Limited off-the-shelf security options

Field-programmable gate array (FPGA)
- An integrated circuit that can be configured after manufacturing
  - Array of logic blocks
  - Programmed in the field
- A problem doesn't require a hardware replacement
  - Reprogram the FPGA
- Common in infrastructure
  - Firewall logic
  - Routers

SCADA/ICS
- Supervisory Control and Data Acquisition System
  - Large-scale, multi-site Industrial Control Systems (ICS)
- PC manages equipment
  - Power generation, refining, manufacturing equipment
  - Facilities, industrial, energy, logistics
- Distributed control systems
  - Real-time information
  - System control
- Requires extensive segmentation
  - No access from the outside

Smart devices / IoT (Internet of Things)
- Sensors - Heating and cooling, lighting
- Smart devices - Home automation, video doorbells
- Wearable technology - Watches, health monitors
- Facility automation - Temperature, air quality, lighting
- Weak defaults
  - IOT manufacturers are not security professionals

Specialized
- Medical devices
  - Heart monitors, insulin pumps
  - Often use older operating systems
- Vehicles
  - Internal network is often accessible from mobile networks
  - Control internal electronics
- Aircraft
  - DoS could damage the aircraft
  - An outage would be problematic
- Smart meters - Measure power and water usage

VoIP
- Voice over Internet Protocol
  - Instead of analog phone line or the
  - Plain Old Telephone Service (POTS)
- A relatively complex embedded system
  - Can be relatively important
- Each device is a computer
  - Separate boot process
  - Individual configurations
  - Different capabilities and functionalities

HVAC
- Heating, Ventilation, and Air Conditioning
  - Thermodynamics, fluid mechanics, and heat transfer
- A complex science
  - Not something you can properly design yourself
  - Must be integrated into the fire system
- PC manages equipment
  - Makes cooling and heating decisions for workspaces and data centers
- Traditionally not built with security in mind
  - Difficult to recover from an infrastructure DoS

2.6 - Embedded Systems (continued)

Drones
- Flying vehicle
  - No pilot on board
- May be manually controlled from the ground
  - Often with some autonomy
  - Set it and forget it
- Extensive commercial and non-commercial use
  - May require federal licenses
  - Security and fail-safes are required

Printers, scanners, and fax machines
- All-in-one or multifunction devices (MFD)
  - Everything you need in one single device
- No longer a simple printer
  - Very sophisticated firmware
- Some images are stored locally on the device
  - Can be retrieved externally
- Logs are stored on the device
  - Contain communication and fax details

RTOS (Real-Time Operating System)
- An operating system with a deterministic processing schedule
  - No time to wait for other processes
  - Industrial equipment, automobiles,
  - Military environments
- Extremely sensitive to security issues
  - Non-trivial systems
  - Need to always be available
  - Difficult to know what type of security is in place

Surveillance systems
- Video/audio surveillance
  - Embedded systems in the cameras and the monitoring stations
- Secure the security system
  - Restrict access from others - Prevent a denial of service
- Physically difficult to replace cameras
  - Accessible independently over the network
  - May allow for firmware upgrades

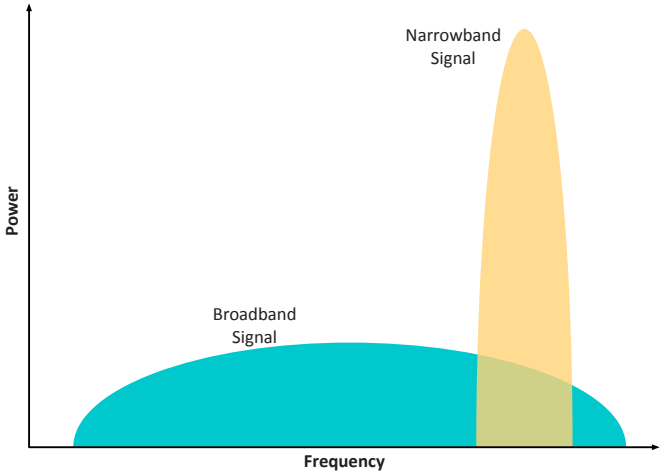
2.6 - Embedded Systems Communication

5G
- Fifth generation cellular networking
  - Launched worldwide in 2020
- Significant performance improvements
  - At higher frequencies
  - Eventually 10 gigabits per second
  - Slower speeds from 100-900 Mbit/s
- Significant IoT impact
  - Bandwidth becomes less of a constraint
  - Larger data transfers
  - Faster monitoring and notification
  - Additional cloud processing

Narrowband
- Communicate analog signals over a narrow range of frequencies
  - Over a longer distance - Conserve the frequency use
- Many IoT devices can communicate over long distances
  - SCADA equipment - Sensors in oil fields

Baseband
- Generally a single cable with a digital signal
  - Can be fiber or copper
- The communication signal uses all of the bandwidth
  - Utilization is either 0% or 100%
- Bidirectional communication
  - But not at the same time using the same wire/fiber
- Ethernet standard - 100BASE-TX, 1000BASE-T, 10GBASE-T

Subscriber identity module (SIM)
- SIM card
  - A universal integrated circuit card
- Used to provide information to a cellular network provider
  - Phones, tablets, embedded systems
- Contains mobile details
  - IMSI (International Mobile Subscriber Identity)
  - Authentication information, contact information
- Important to manage
  - Many embedded systems, many SIM cards



Zigbee
- Internet of Things networking
  - Open standard - IEEE 802.15.4 PAN
- Alternative to WiFi and Bluetooth
  - Longer distances than Bluetooth
  - Less power consumption than WiFi
- Mesh network of all Zigbee devices in your home
  - Light switch communicates to light bulbs
  - Tell Amazon Echo to lock the door
- Uses the ISM band
  - Industrial, Scientific, and Medical
  - 900 MHz and 2.4 GHz frequencies in the US

2.6 - Embedded Systems Constraints

Embedded systems

- Not usually a fully capable computer
  - Low cost, purpose-built
- Adds additional constraints
  - May have limited or missing features
  - Upgradability limitations
  - Limits in communication options
- An ongoing trade off
  - Low cost systems - Unique management challenges

Constraints

- Power - May not have access to a main power source
  - Batteries may need to be replaced and maintained
- Compute
  - Low-power CPUs are limited in speed
  - Cost and heat considerations
- Network
  - May not have the option for a wired link
  - May be in the middle of a field
  - Wireless is the limiting factor
- Crypto
  - Limited hardware options
  - Difficult to change or modify cryptography features
- Inability to patch
  - Some IoT devices have no field-upgradable options
  - Upgrade options may be limited or difficult to install
- Authentication
  - Security features are often an afterthought
  - Limited options, no multi-factor, limited integration with existing directory services
- Range
  - Purpose-built - usually does one thing very well
  - May not provide much additional functionality
- Cost
  - Single-purpose functionality comes at a low cost
  - Low cost may affect product quality
- Implied trust
  - Limited access to the hardware and software
  - Difficult to verify the security posture

2.7 - Physical Security Controls

Barricades / bollards

- Prevent access
  - There are limits to the prevention
- Channel people through a specific access point
  - And keep out other things
  - Allow people, prevent cars and trucks
- Identify safety concerns
  - And prevent injuries
- Can be used to an extreme
  - Concrete barriers / bollards
  - Moats

Access control vestibules

- All doors normally unlocked
  - Opening one door causes others to lock
- All doors normally locked
  - Unlocking one door prevents others from being unlocked
- One door open / other locked
  - When one is open, the other cannot be unlocked
- One at a time, controlled groups
  - Managed control through an area

Alarms

- Circuit-based
  - Circuit is opened or closed
  - Door, window, fence
  - Useful on the perimeter
- Motion detection
  - Radio reflection or passive infrared
  - Useful in areas not often in use
- Duress
  - Triggered by a person - The big red button

Signs

- Clear and specific instructions
  - Keep people away from restricted areas
  - Consider visitors
- Consider personal safety
  - Fire exits
  - Warning signs
  - Chemicals
  - Construction
  - Medical resources
- Informational
  - In case of emergency, call this number

Video surveillance

- CCTV (Closed circuit television)
  - Can replace physical guards
- Camera features are important
  - Motion recognition can alarm and alert when something moves
  - Object detection can identify a license plate or person's face
- Often many different cameras
  - Networked together and recorded over time

Industrial camouflage

- Conceal an important facility in plain sight
  - Blends in to the local environment
- Protect a data center
  - No business signs
  - No visual clues
  - Surround it with a water feature
  - Install a guard gate
  - Planters out front are bollards

Guards and access lists
- Security guard
  - Physical protection at the reception area of a facility
  - Validates identification of existing employees
  - Provides guest access
- ID badge
  - Picture, name, other details
  - Must be worn at all times
- Access list
  - Physical list of names
  - Enforced by security guard
- Maintains a visitor log

Guards
- Two-person integrity/control
  - Minimize exposure to an attack
  - No single person has access to a physical asset
- Robot sentries
  - Monitoring
  - Rounds / Periodic checks
  - An emerging technology

Biometrics
- Biometric authentication
  - Fingerprint, retina, voiceprint
- Usually stores a mathematical representation of your biometric
  - Your actual fingerprint isn't usually saved
- Difficult to change
  - You can change your password
  - You can't change your fingerprint
- Used in very specific situations
  - Not foolproof

Door access controls
- Conventional - Lock and key
- Deadbolt - Physical bolt
- Electronic - Keyless, PIN
- Token-based
  - RFID badge, magnetic swipe card, or key fob
- Biometric - Hand, fingers or retina
- Multi-factor - Smart card and PIN

Cable locks
- Temporary security
  - Connect your hardware to something solid
- Cable works almost anywhere
  - Useful when mobile
- Most devices have a standard connector
  - Reinforced notch
- Not designed for long-term protection
  - Those cables are pretty thin

USB data blocker
- Don't connect to unknown USB interfaces
  - Even if you need a quick charge
  - Prevent "juice jacking"
- Use a USB data blocker
  - Allow the voltage, reject the data
- Use your power adapter
  - Avoid the issue entirely

Proper lighting
- More light means more security
  - Attackers avoid the light
  - Easier to see when lit
  - Non IR cameras can see better
- Specialized design
  - Consider overall light levels
  - Lighting angles may be important
  - Facial recognition
  - Avoid shadows and glare

Fencing
- Build a perimeter
  - Usually very obvious
  - May not be what you're looking for
- Transparent or opaque
  - See through the fence (or not)
- Robust
  - Difficult to cut the fence
- Prevent climbing
  - Razor wire
  - Build it high

Fire suppression
- Electronics require unique responses to fire
  - Water is generally a bad thing
- Detection
  - Smoke detector, flame detector, heat detector
- Suppress with water
  - Where appropriate
- Suppress with chemicals
  - Halon - No longer manufactured
  - Destroys ozone
  - Commonly replaced with Dupont FM-200

Sensors
- Motion detection
  - Identify movement in an area
- Noise detection
  - Recognize an increase in sound
- Proximity reader
  - Commonly used with electronic door locks
  - Combined with an access card
- Moisture detection
  - Useful to identify water leaks
- Temperature
  - Monitor changes over time

2.7 - Physical Security Controls (continued)

Drones
- Quickly cover large areas
  - More than just one building
- More than physical security
  - Site surveys, damage assessments
- On-board sensors
  - Motion detection
  - Thermal sensors
- Video evidence
  - High resolution video capture

Faraday cage
- Blocks electromagnetic fields
  - Discovered by Michael Faraday in 1836
- A mesh of conductive material
  - The cage cancels the electromagnetic field's effect on the interior
  - The window of a microwave oven
- Not a comprehensive solution
  - Not all signal types are blocked
  - Some signal types are not blocked at all
- Can restrict access to mobile networks
  - Some very specific contingencies would need to be in place for emergency calls

Screened subnet
- Formerly known as a demilitarized zone (DMZ)
  - An additional layer of security between the Internet and you
  - Public access to public resources

Protected distribution
- Protected Distribution System (PDS)
  - A physically secure cabled network
- Protect your cables and fibers
  - All of the data flows through these conduits
- Prevent cable and fiber taps
  - Direct taps and inductive taps
- Prevent cable and fiber cuts
  - A physical denial of service (DoS)
- Hardened protected distribution system
  - Sealed metal conduit, periodic visual inspection

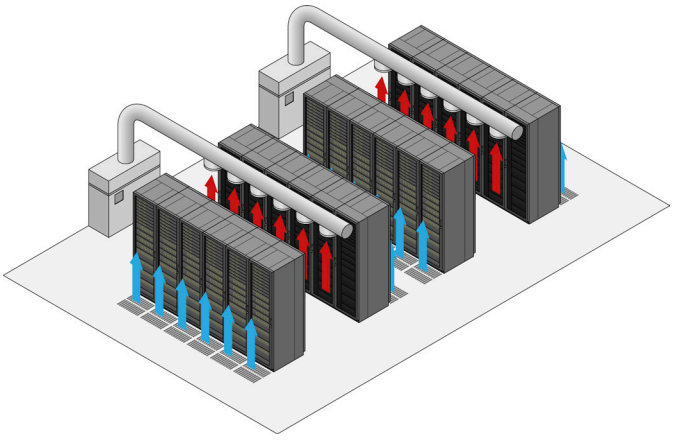
2.7 - Secure Areas

Secure areas
- Physically secure the data
  - As important as the digital security
- An important part of a security policy
  - Not a question to leave unanswered
- Secure active operations
  - Prevent physical access to the systems
- Secure offline data
  - Backups are an important security concern

Air gap
- Physical separation between networks
  - Secure network and insecure network
  - Separate customer infrastructures
- Most environments are shared
  - Shared routers, switches, firewalls
  - Some of these are virtualized
- Specialized networks require air gaps
  - Stock market networks
  - Power systems/SCADA
  - Airplanes
  - Nuclear power plant operations

Vaults and safes
- Vault
  - A secure reinforced room
  - Store backup media
  - Protect from disaster or theft
  - Often onsite
- Safe
  - Similar to a vault, but smaller
  - Less expensive to implement
  - Space is limited - Install at more locations

Hot and cold aisles
- Data centers
  - Lots and lots of equipment
  - This equipment generates heat
- Optimize cooling
  - Keep components at optimal temperatures
- Conserve energy
  - Data centers are usually very large rooms
  - Focus the cooling
  - Lower energy costs



2.7 - Secure Data Destruction

Data destruction and media sanitization
- Disposal becomes a legal issue
  - Some information must not be destroyed
  - Consider offsite storage
- You don't want critical information in the trash
  - People really do dumpster dive
  - Recycling can be a security concern
  - Physically destroy the media
- Reuse the storage media
  - Sanitize the media for reuse
  - Ensure nothing is left behind

Protect your rubbish
- Secure your garbage - Fence and a lock
- Shred your documents
  - This will only go so far
  - Governments burn the good stuff
- Burn documents - No going back
- Pulp the paper
  - Large tank washing to remove ink
  - Paper broken down into pulp
  - Creates recycled paper

Physical destruction
- Shredder / pulverizer
  - Heavy machinery, complete destruction
- Drill / Hammer
  - Quick and easy - Platters, all the way through
- Electromagnetic (degaussing)
  - Remove the magnetic field
  - Destroys the drive data and renders the drive unusable
- Incineration - Fire hot.

Certificate of destruction
- Destruction is often done by a 3rd party
  - How many drills and degaussers do you have?
- Need confirmation that your data is destroyed
  - Service should include a certificate
- A paper trail of broken data
  - You know exactly what happened

Sanitizing media
- Purge data
  - Remove it from an existing data store
  - Delete some of the data from a database
- Wipe data
  - Unrecoverable removal of data on a storage device
  - Usually overwrites the data storage locations
  - Useful when you need to reuse or continue using the media

Data security
- July 2013 - UK National Health Service Surrey
  - Provided hard drives to a 3rd-party to be destroyed
  - Contained 3,000 patient records
  - Received a destruction certificate, but not actually destroyed.
  - Sold on eBay. Buyer contacted authorities, fined £200,000
- File level overwriting
  - Sdelete – Windows Sysinternals
- Whole drive wipe secure data removal
  - DBAN - Darik's Boot and Nuke
  - Physical drive destruction -
  - One-off or industrial removal and destroy

2.8 - Cryptography Concepts

Cryptography
- Greek: "kryptos"
  - Hidden, secret
- Confidentiality
  - It's a secret
- Authentication and access control
  - I know it's you. I REALLY know it's you.
- Non-repudiation - You said it. You can't deny it.
- Integrity - Tamper-proof

Cryptography terms
- Plaintext - An unencrypted message (in the clear)
- Ciphertext - An encrypted message
- Cipher - The algorithm used to encrypt and/or decrypt
- Cryptanalysis
  - The art of cracking encryption
  - Researchers are constantly trying to find weaknesses in ciphers
  - A mathematically flawed cipher is bad for everyone

Cryptographic keys
- Keys
  - Add the key to the cypher to encrypt
  - Larger keys are generally more secure
- Some encryption methods use one key
  - Some use more than one key
  - Every method is a bit different

Give weak keys a workout
- A weak key is a weak key
  - By itself, it's not very secure
- Make a weak key stronger by performing multiple processes
  - Hash a password. Hash the hash of the password. And continue…
  - Key stretching, key strengthening
- Brute force attacks would require reversing each of those hashes
  - The attacker has to spend much more time, even though the key is small

2.8 - Cryptography Concepts (continued)

Key stretching libraries
- Already built for your application
  - No additional programming involved
- bcrypt
  - Generates hashes from passwords
  - An extension to the UNIX crypt library
  - Uses Blowfish cipher to perform multiple rounds of hashing
- Password-Based Key Derivation Function 2 (PBKDF2)
  - Part of RSA public key cryptography standards (PKCS #5, RFC 2898)

Lightweight cryptography
- Powerful cryptography has traditionally required strength
  - A powerful CPU and lots of time
- Internet of Things (IoT) devices have limited power
  - Both watts and CPU
- New standards are being created
  - National Institute of Standards and Technology (NIST) leading the effort
  - Provide powerful encryption
  - Include integrity features
  - Keep costs low

Homomorphic encryption (HE)
- Encrypted data is difficult to work with
  - Decrypt the data
  - Perform a function
  - Encrypt the answer
- Homomorphic encryption
  - Perform calculations of data while it's encrypted
  - Perform the work directly on the encrypted data
  - The decrypted data can only be viewed with the private key
- Many advantages
  - Securely store data in the cloud
  - Perform research on data without viewing the data

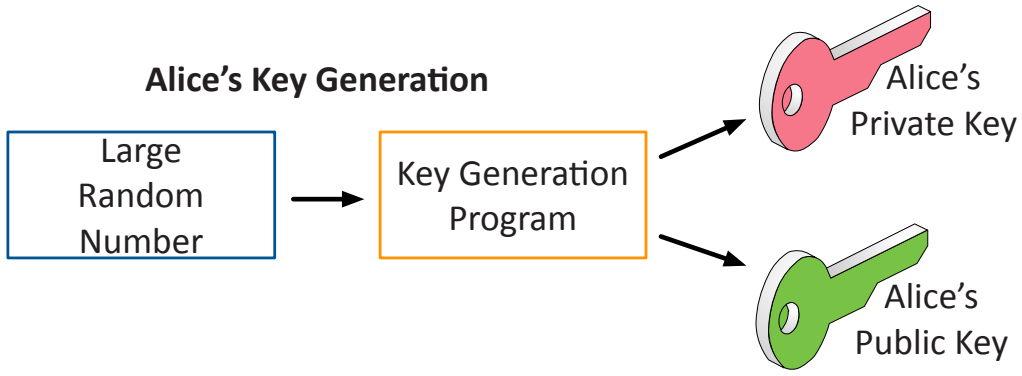
2.8 - Symmetric and Asymmetric Cryptography

Symmetric encryption
- A single, shared key
  - Encrypt with the key
  - Decrypt with the same key
  - If it gets out, you'll need another key
- Secret key algorithm
  - A shared secret
- Doesn't scale very well
  - Can be challenging to distribute
- Very fast to use
  - Less overhead than asymmetric encryption
  - Often combined with asymmetric encryption

Asymmetric encryption
- Public key cryptography
  - Two (or more) mathematically related keys
- Private key - Keep this private
- Public key - Anyone can see this key - Give it away
- The private key is the only key that can decrypt data encrypted with the public key
  - You can't derive the private key from the public key

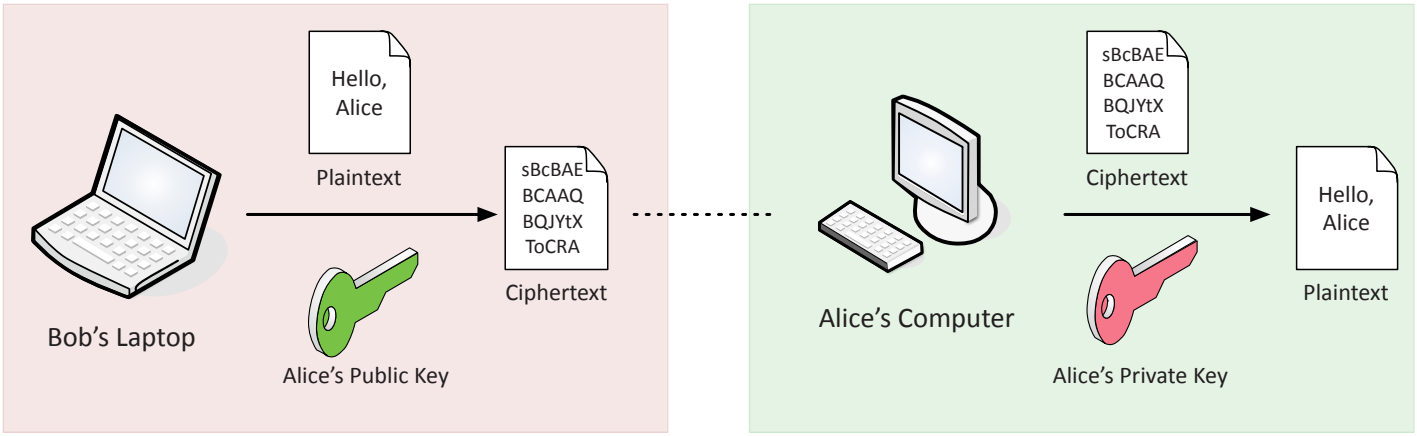
The key pair
- Asymmetric encryption
  - Public Key Cryptography
- Key generation
  - Build both the public and private key at the same time
  - Lots of randomization
  - Large prime numbers
  - Lots and lots of math
- Everyone can have the public key
  - Only Alice has the private key

Elliptic curve cryptography (ECC)
- Asymmetric encryption
  - Need large integers composed of two or more large prime factors
- Instead of numbers, use curves!
  - Uses smaller keys than non-ECC asymmetric encryption
  - Smaller storage and transmission requirements
  - Perfect for mobile devices



2.8 - Symmetric and Asymmetric Cryptography (continued)

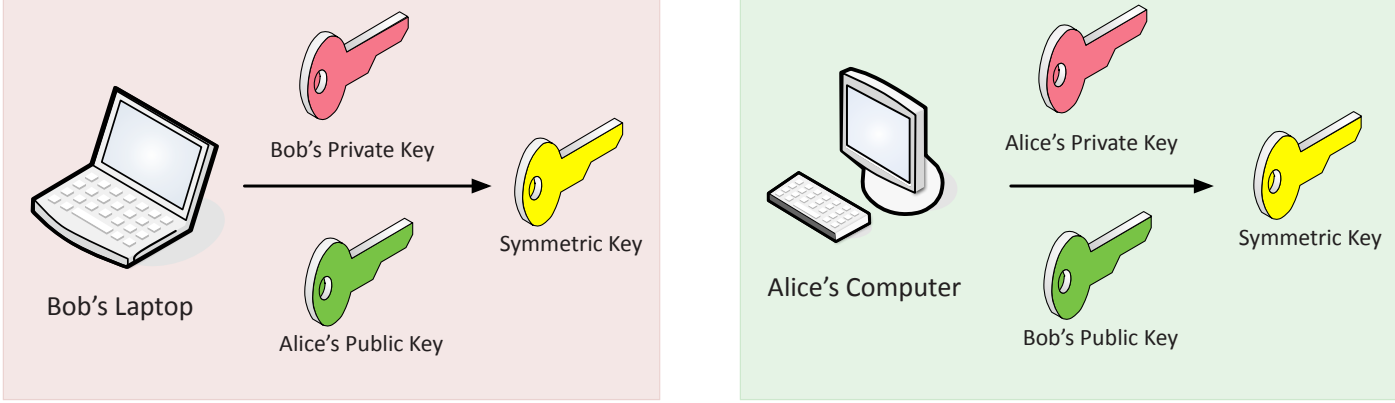
Asymmetric encryption



1. Bob combines Alice's public key with plaintext to create ciphertext

2. Alice uses her private key to decrypt the ciphertext into the original plaintext

Symmetric key from asymmetric keys



1. Bob combines his private key with Alice's public key to create a symmetric key

2. Alice combines her private key with Bob's public key to create the same symmetric key

2.8 - Hashing and Digital Signatures

Hashes

- Represent data as a short string of text - A message digest
- One-way trip
  - Impossible to recover the original message from the digest
  - Used to store passwords / confidentiality
- Verify a downloaded document is the same as the original
  - Integrity
- Can be a digital signature
  - Authentication, non-repudiation, and integrity
- Will not have a collision (hopefully)
  - Different messages will not have the same hash

Collision

- Hash functions
  - Take an input of any size - Create a fixed size string
  - Message digest, checksum
- The hash should be unique
  - Different inputs should never create the same hash
  - If they do, it's a collision
- MD5 has a collision problem
  - Found in 1996 - Don't use MD5

Practical hashing

- Verify a downloaded file
  - Hashes may be provided on the download site
  - Compare the downloaded file hash with the posted hash value
- Password storage
  - Instead of storing the password, store a salted hash
  - Compare hashes during the authentication process
  - Nobody ever knows your actual password

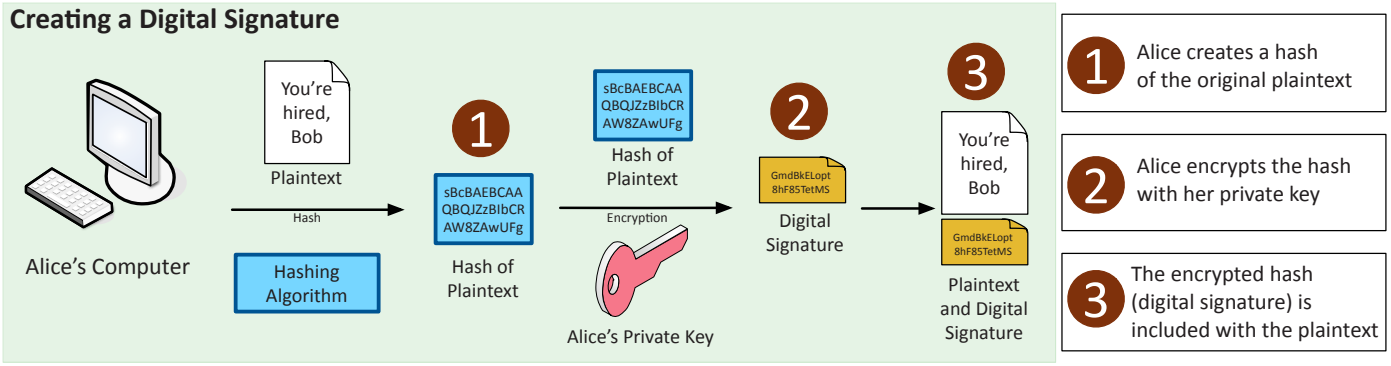
2.8 - Hashing and Digital Signatures (continued)

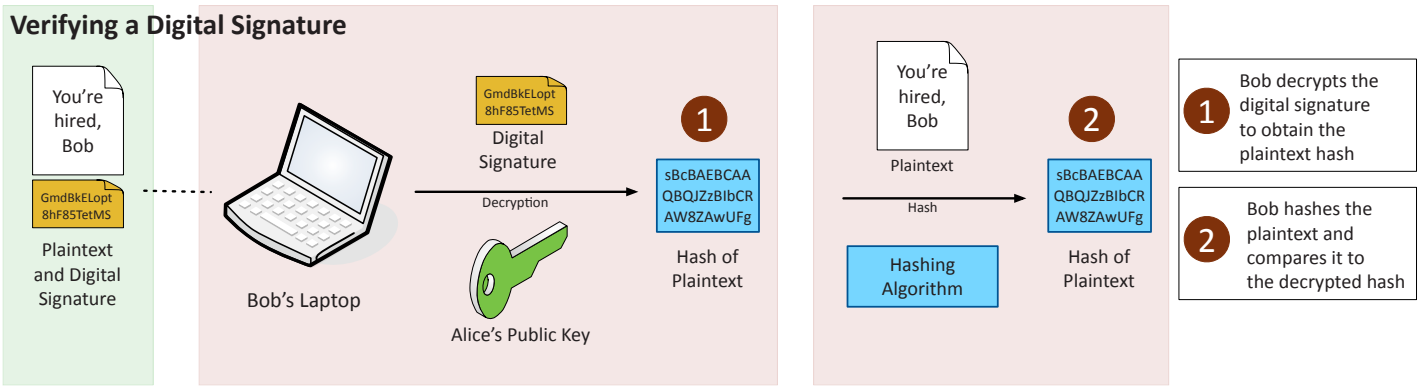
Adding some salt

- Salt
  - Random data added to a password when hashing
- Every user gets their own random salt
  - The salt is commonly stored with the password
- Rainbow tables won't work with salted hashes
  - Additional random value added to the original password
- This slows things down the brute force process
  - It doesn't completely stop the reverse engineering
- Each user gets a different random hash
  - The same password creates a different hash

Digital signatures

- Prove the message was not changed
  - Integrity
- Prove the source of the message
  - Authentication
- Make sure the signature isn't fake
  - Non-repudiation
- Sign with the private key
  - The message doesn't need to be encrypted
  - Nobody else can sign this (obviously)
- Verify with the public key
  - Any change in the message will invalidate the signature





2.8 - Cryptographic Keys

Cryptographic Keys

- There's very little that isn't known about the cryptographic process
  - The algorithm is usually a known entity
  - The only thing you don't know is the key
- The key determines the output
  - Encrypted data
  - Hash value
  - Digital signature
- Keep your key private!
  - It's the only thing protecting your data

Key strength

- Larger keys tend to be more secure
  - Prevent brute-force attacks
  - Attackers can try every possible key combination
- Symmetric encryption
  - 128-bit or larger symmetric keys are common
  - These numbers get larger as time goes on
- Asymmetric encryption
  - Complex calculations of prime numbers
  - Larger keys than symmetric encryption
  - Common to see key lengths of 3,072 bits or larger

Key exchange

- A logistical challenge
  - How do you transfer an encryption key across an insecure medium without having an encryption key?
- Out-of-band key exchange
  - Don't send the symmetric key over the 'net
  - Telephone, courier, in-person, etc.

2.8 - Cryptographic Keys (continued)

- In-band key exchange
  - It's on the network
  - Protect the key with additional encryption
  - Use asymmetric encryption to deliver a symmetric key

Real-time encryption/decryption

- There's a need for fast security
  - Without compromising the security part
- Share a symmetric session key using asymmetric encryption
  - Client encrypts a random (symmetric) key with a server's public key
  - The server decrypts this shared key and uses it to encrypt data
  - This is the session key
- Implement session keys carefully
  - Need to be changed often (ephemeral keys)
  - Need to be unpredictables

Symmetric key from asymmetric keys

- Use public and private key cryptography to create a symmetric key
  - Math is powerful

Traditional web server encryption

- SSL/TLS uses encryption keys to protect web server communication
  - Traditionally, this has been based on the web server's RSA key pair
  - One key that encrypts all symmetric keys
- This server's private key can rebuild everything
  - If you capture all of the traffic, you can decrypt all of the data
- One point of failure for all of your web site encryption

Perfect Forward Secrecy (PFS)

- Change the method of key exchange
  - Don't use the server's private RSA key
- Elliptic curve or Diffie-Hellman ephemeral
  - The session keys aren't kept around
- Can't decrypt with the private server key
  - Every session uses a different private key for the exchange
- PFS requires more computing power
  - Not all servers choose to use PFS
- The browser must support PFS
  - Check your SSL/TLS information for details

2.8 - Steganography

Obfuscation

- The process of making something unclear
  - It's now much more difficult to understand
- But it's not impossible to understand
  - If you know how to read it
- Make source code difficult to read
  - But it doesn't change the functionality of the code
- Hide information inside of an image
  - Steganography

Steganography

- Greek for "concealed writing"
  - Security through obscurity
- Message is invisible
  - But it's really there
- The covertext
  - The container document or file

Common steganography techniques

- Network based
  - Embed messages in TCP packets
- Use an image
  - Embed the message in the image itself
- Invisible watermarks
  - Yellow dots on printers

Other steganography types

- Audio steganography
  - Modify the digital audio file
  - Interlace a secret message within the audio
  - Similar technique to image steganography
- Video steganography
  - A sequence of images
  - Use image steganography on a larger scale
  - Manage the signal to noise ratio
  - Potentially transfer much more information

2.8 - Quantum Computing

Quantum computing

- Computers based on quantum physics
  - This is not an upgrade to your existing computer
  - This is a new computing technology
- Classical mechanics
  - Smallest form of information is a bit
  - Bits are zeros and ones
- Quantum mechanics
  - Smallest form of information is a qubit
  - Bits are zeros, ones, and any combination in-between, at the same time
  - This is called quantum superposition
- Search quickly through large databases
  - Index everything at the same time
- Simulate the quantum world
  - Medical advances, weather prediction, astrophysics, and much more

2.8 - Quantum Computing (continued)

Post-quantum cryptography

- Breaks our existing encryption mechanisms
  - Quickly factor large prime numbers
- This would cause significant issues
  - None of the existing cryptography could be trusted
  - No financial transactions would be safe
  - No data would be private
- Peter Shor invented Shor's algorithm in 1994
  - Given an integer N, find its prime factors
  - Traditional computers would take longer than the lifetime of the universe
  - Shor's algorithm would theoretically be much, much faster
- Time for updated cryptography
  - Not vulnerable to quantum computer based attacks
- NTRU
  - A cryptosystem using lattice theory
  - Relies on the "closest-vector" problem
  - Instead of finding the prime factorizations of large numbers
- We will need to consider our options for future cryptography
  - This is a problem that can be easily seen and addressed

Quantum communication

- Protect against eavesdropping using quantum cryptography
  - Quantum Key Distribution (QKD)
- Create unbreakable encryption
  - Send a random stream of qubits (the key) across a quantum network channel
- Both sides can verify the key
  - If it's identical, the key was not viewed during transmission
- An attacker eavesdropping on the communication would modify the data stream
  - The attacker would have to violate quantum physics

2.8 - Stream and Block Ciphers

Stream ciphers

- Encryption is done one bit or byte at a time
  - High speed, low hardware complexity
- Used with symmetric encryption
  - Not commonly used with asymmetric encryption
- The starting state should never be the same twice
  - Key is often combined with an initialization vector (IV)

Block ciphers

- Encrypt fixed-length groups
  - Often 64-bit or 128-bit blocks
  - Pad added to short blocks
  - Each block is encrypted or decrypted independently
- Symmetric encryption
  - Similar to stream ciphers
- Block cipher modes of operation
  - Avoid patterns in the encryption
  - Many different modes to choose from

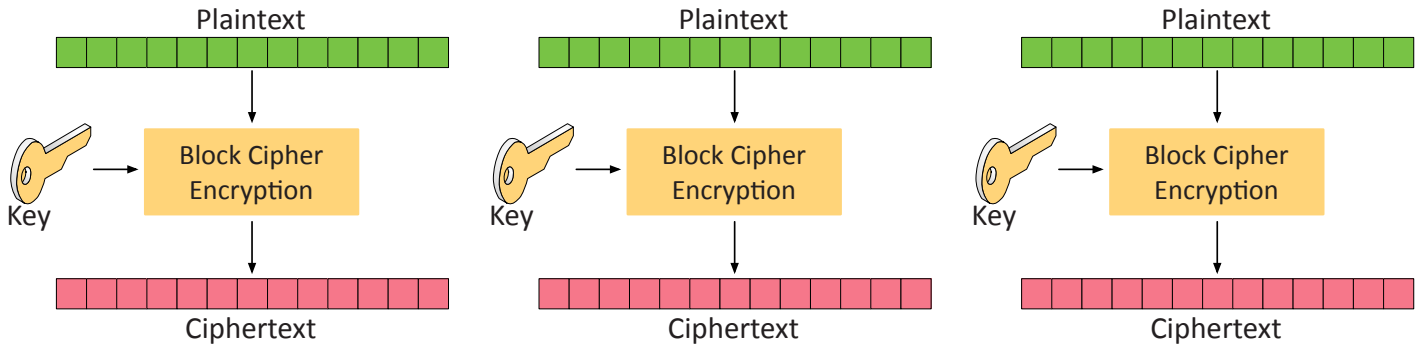
Block cipher mode of operation

- Encrypt one fixed-length group of bits at a time
  - A block
- Mode of operation
  - Defines the method of encryption
  - May provide a method of authentication
- The block size is a fixed size
  - Not all data matches the block size perfectly
  - Split your plaintext into smaller blocks
  - Some modes require padding before encrypting

ECB (Electronic Code Book)

- The simplest encryption mode
  - Too simple for most use cases
- Each block is encrypted with the same key
  - Identical plaintext blocks create identical ciphertext blocks

ECB (Electronic Code book) cipher mode



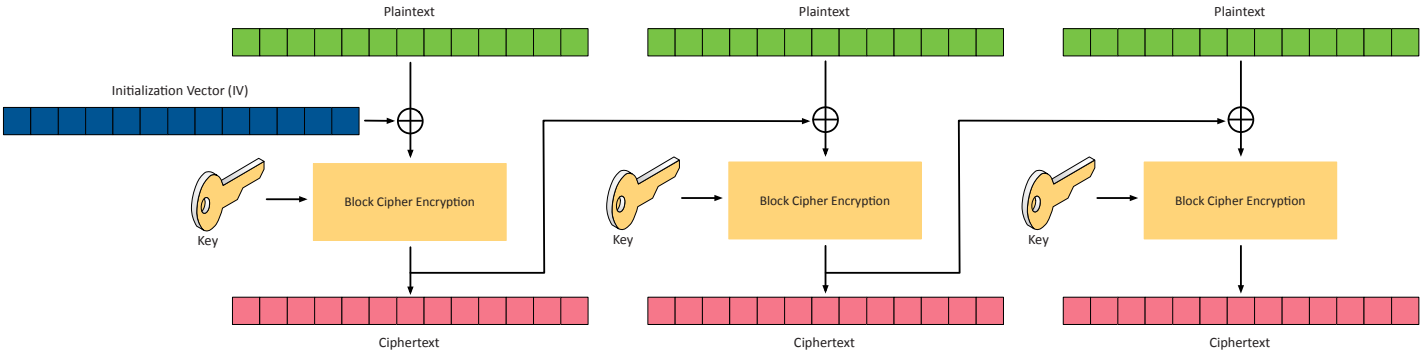
2.8 - Stream and Block Ciphers (continued)

CBC (Cipher Block Chaining)
- A popular mode of operation - Relatively easy to implement
- Each plaintext block is XORed with the previous ciphertext block
  - Adds additional randomization
  - Use an initialization vector for the first block

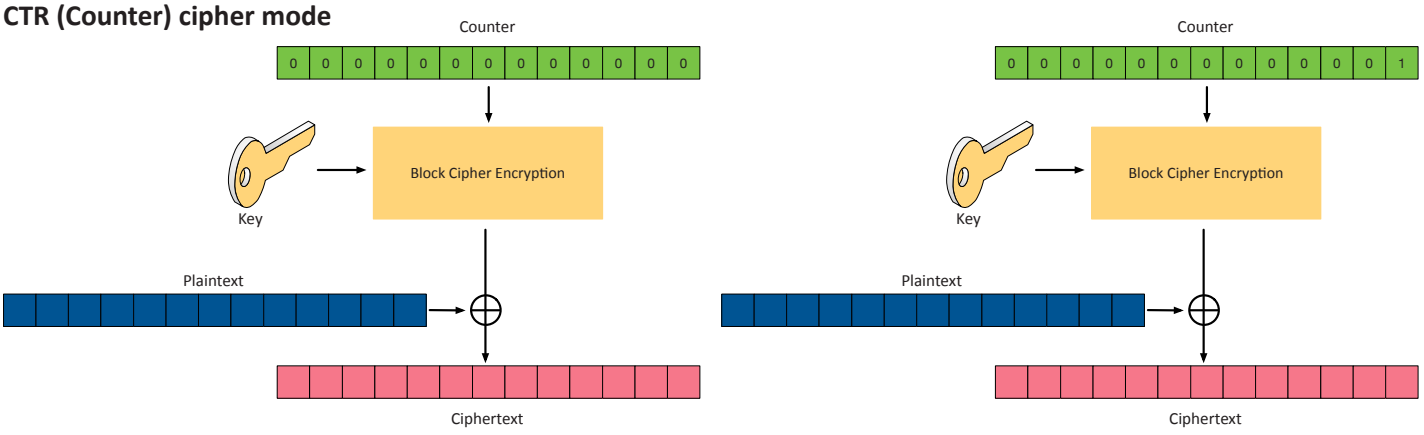
CTR (Counter)
- Block cipher mode / acts like a stream cipher
  - Encrypts successive values of a "counter"
- Plaintext can be any size, since it's part of the XOR i.e., 8 bits at a time (streaming) instead of a 128-bit block

GCM (Galois/Counter Mode)
- Encryption with authentication
  - Authentication is part of the block mode
  - Combines Counter Mode with
  - Galois authentication
- Minimum latency, minimum operation overhead
  - Very efficient encryption and authentication
- Commonly used in packetized data
  - Network traffic security (wireless, IPsec)
  - SSH, TLS

CBC (Cipher Block Chaining) cipher mode



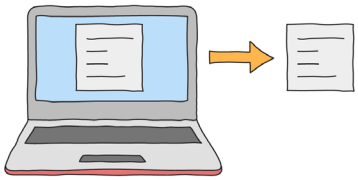
CTR (Counter) cipher mode



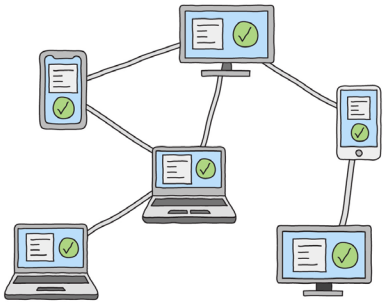
2.8 - Blockchain Technology

Blockchain
- A distributed ledger
  - Keep track of transactions
- Everyone on the blockchain network maintains the ledger
  - Records and replicates to anyone and everyone
- Many practical applications
  - Payment processing
  - Digital identification
  - Supply chain monitoring
  - Digital voting

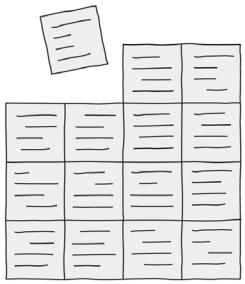
2.8 - Blockchain Technology (continued)



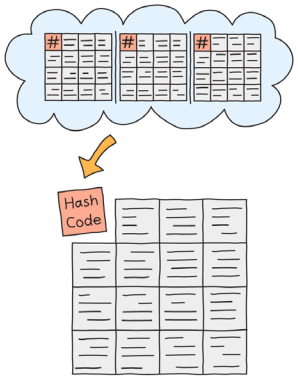
1 A transaction is requested. The transaction could be any digital transaction from transferring Bitcoins, medical records, data backups, to transferring house title information.



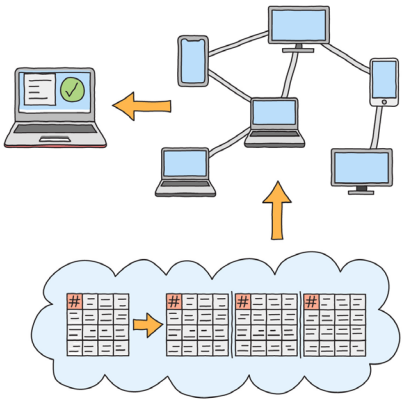
2 The transaction is sent to every computer, or node, in a decentralized network to be verified.



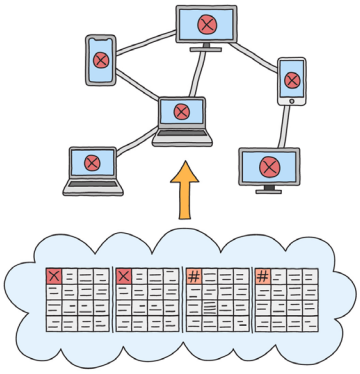
3 The verified transaction is added to a new block of data containing other recently verified transactions.



4 A secure code, called a Hash, is calculated from the previous blocks of transaction data in the Blockchain. The hash is added to the new block of verified transactions.



5 The block is added to the end of the Blockchain which is then updated to all nodes in the network for security. The transaction is complete.



6 If any blocks are altered, its hash and all following hashes in the chain are automatically recalculated. The altered chain will no longer match the chains stored by the rest of the network, and will be rejected.

2.8 - Cryptography Use Cases

Finding the balance

- Low power devices
  - Mobile devices, portable systems
  - Smaller symmetric key sizes
  - Use elliptic curve cryptography (ECC) for asymmetric encryption
- Low latency
  - Fast computation time
  - Symmetric encryption, smaller key sizes
- High resiliency
  - Larger key sizes
  - Encryption algorithm quality
  - Hashing provides data integrity

Use cases

- Confidentiality
  - Secrecy and privacy
  - Encryption (file-level, drive-level, email)
- Integrity
  - Prevent modification of data
  - Validate the contents with hashes
  - File downloads, password storage
- Obfuscation
  - Modern malware
  - Encrypted data hides the active malware code
  - Decryption occurs during execution
- Authentication
  - Password hashing
  - Protect the original password
  - Add salts to randomize the stored password hash
- Non-Repudiation
  - Confirm the authenticity of data
  - Digital signature provides both integrity and non-repudiation

2.8 - Cryptography Limitations

Finding the balance

- Cryptography isn't a perfect solution
  - It can have significant limitations
- Not all implementations are the same
  - Different platforms, different cryptographic options
- Cryptography can't fix bad technique
  - Hashing easily guessed passwords without a salt
- Every situation is different
  - Do your homework

Limitations

- Speed
  - Cryptography adds overhead
  - A system needs CPU, CPU needs power
  - More involved encryption increases the load
- Size
  - Typical block ciphers don't increase the size of encrypted data
  - AES block size is 128 bits/16 bytes
  - Encrypting 8 bytes would potentially double the storage size
- Weak keys
  - Larger keys are generally more difficult to brute force
  - The weak IV in RC4 resulted in the WEP security issues
- Time
  - Encryption and hashing takes time
  - Larger files take longer
  - Asymmetric is slower than symmetric
- Longevity
  - A specific cryptographic technology can becomes less secure over time
  - Smaller keys are easier to brute force, larger keys take longer to process
  - Key retirement is a good best practice
- Predictability and entropy
  - Random numbers are critical for secure cryptography
  - Hardware random number generators can be predictable
  - A passphrase needs to be appropriately random
- Key reuse
  - Reusing the same key reduces complexity
  - Less cost and effort to recertify keys
  - Less administrative overhead
  - If the key is compromised, everything using that key is at risk
  - IoT devices often have keys embedded in the firmware
- Resource vs. security constraints
  - IoT devices have limited CPU, memory, and power
  - Real-time applications can't delay
  - Difficult to maintain and update security components

3.1 - Secure Protocols

Voice and video

- SRTP
  - Secure Real-Time Transport Protocol / Secure RTP
- Adds security features to RTP
  - Keep conversations private
- Encryption
  - Uses AES to encrypt the voice/video flow
- Authentication, integrity, and replay protection
  - HMAC-SHA1 - Hash-based message authentication code using SHA1

Time synchronization

- Classic NTP has no security features
  - Exploited as amplifiers in DDoS attacks
  - NTP has been around prior to 1985
- NTPsec
  - Secure network time protocol
  - Began development in June of 2015
- Cleaned up the code base
  - Fixed a number of vulnerabilities

Email

- S/MIME
  - Secure/Multipurpose Internet Mail Extensions
  - Public key encryption and digital signing of mail content
  - Requires a PKI or similar organization of keys
- Secure POP and Secure IMAP
  - Use a STARTTLS extension to encrypt POP3 with SSL or use IMAP with SSL
- SSL/TLS
  - If the mail is browser based, always encrypt with SSL

Web

- SSL/TLS
  - Secure Sockets Layer/Transport Layer Security
- HTTPS
  - HTTP over TLS / HTTP over SSL / HTTP Secure
- Uses public key encryption
  - Private key on the server
  - Symmetric session key is transferred using asymmetric encryption
  - Security and speed

IPSec (Internet Protocol Security)
- Security for OSI Layer 3
  - Authentication and encryption for every packet
- Confidentiality and integrity/anti-replay
  - Encryption and packet signing
- Very standardized
  - Common to use multi-vendor implementations
- Two core IPSec protocols
  - Authentication Header (AH)
  - Encapsulation Security Payload (ESP)

File transfer
- FTPS
  - FTP over SSL (FTP-SSL)
  - File Transfer Protocol Secure
  - This is not SFTP
- SFTP
  - SSH File Transfer Protocol
  - Provides file system functionality
  - Resuming interrupted transfers, directory listings, remote file removal

LDAP (Lightweight Directory Access Protocol)
- Protocol for reading and writing directories over an IP network
  - An organized set of records, like a phone directory
- X.500 specification was written by the International Telecommunications Union (ITU)
  - They know directories!
- DAP ran on the OSI protocol stack
  - LDAP is lightweight, and uses TCP/IP
- LDAP is the protocol used to query and update an X.500 directory
  - Used in Windows Active Directory, Apple OpenDirectory, OpenLDAP, etc.

Directory services
- LDAP (Lightweight Directory Access Protocol)
- LDAPS (LDAP Secure)
  - A non-standard implementation of LDAP over SSL
- SASL (Simple Authentication and Security Layer)
  - Provides authentication using many different methods, i.e., Kerberos or client certificate

Remote access
- SSH (Secure Shell)
  - Encrypted terminal communication
  - Replaces Telnet (and FTP)
  - Provides secure terminal communication and file transfer features

Domain name resolution
- DNS had no security in the original design
  - Relatively easy to poison a DNS
- DNSSEC
  - Domain Name System Security Extensions
- Validate DNS responses
  - Origin authentication
  - Data integrity
- Public key cryptography
  - DNS records are signed with a trusted third party
  - Signed DNS records are published in DNS

Routing and switching
- SSH - Secure Shell
  - Encrypted terminal communication
- SNMPv3 - Simple Network
  - Management Protocol version 3
  - Confidentiality - Encrypted data
  - Integrity - No tampering of data
  - Authentication - Verifies the source
- HTTPS
  - Browser-based management
  - Encrypted communication

Network address allocation
- Securing DHCP
  - DHCP does not include any built-in security
  - There is no “secure” version of the DHCP protocol
- Rogue DHCP servers
  - In Active Directory, DHCP servers must be authorized
  - Some switches can be configured with “trusted” interfaces
  - DHCP distribution is only allowed from trusted interfaces
  - Cisco calls this DHCP Snooping
  - DHCP client DoS - Starvation attack
  - Use spoofed MAC addresses to exhaust the DHCP pool
  - Switches can be configured to limit the number of MAC addresses per interface
  - Disable an interface when multiple MAC addresses are seen

Subscription services
- Automated subscriptions
  - Anti-virus / Anti-malware signature updates
  - IPS updates
  - Malicious IP address databases / Firewall updates
- Constant updates
  - Each subscription uses a different update method
- Check for encryption and integrity checks
  - May require an additional public key configuration
  - Set up a trust relationship
  - Certificates, IP addresses

3.2 - Endpoint Protection

The endpoint
- The user's access - Applications and data
- Stop the attackers - Inbound attacks, outbound attacks
- Many different platforms - Mobile, desktop
- Protection is multi-faceted - Defense in depth

Anti-virus and anti-malware
- Anti-virus is the popular term
  - Refers specifically to a type of malware
  - Trojans, worms, macro viruses
- Malware refers to the broad malicious software category
  - Anti-malware stops spyware, ransomware, fileless malware
- The terms are effectively the same these days
  - The names are more of a marketing tool
  - Anti-virus software is also anti-malware software now
  - Make sure your system is using
  - a comprehensive solution

Endpoint detection and response (EDR)
- A different method of threat protection
  - Scale to meet the increasing number of threats
- Detect a threat
  - Signatures aren't the only detection tool
  - Behavioral analysis, machine learning, process monitoring
  - Lightweight agent on the endpoint
- Investigate the threat
  - Root cause analysis
- Respond to the threat
  - Isolate the system, quarantine the threat, rollback to a previous config
  - API driven, no user or technician intervention required

Data Loss Prevention (DLP)
- Where's your data?
  - Social Security numbers, credit card numbers, medical records
- Stop the data before the attacker gets it
  - Data "leakage"
- So many sources, so many destinations
  - Often requires multiple solutions
  - Endpoint clients
  - Cloud-based systems
  - Email, cloud storage, collaboration tools

Next-generation firewall (NGFW)
- The OSI Application Layer - All data in every packet
- Can be called different names
  - Application layer gateway
  - Stateful multilayer inspection, deep packet inspection
- Broad security controls
  - Allow or disallow application features
  - Identify attacks and malware
  - Examine encrypted data
  - Prevent access to URLs or URL categories

Host-based firewall
- Software-based firewall
  - Personal firewall, runs on every endpoint
- Allow or disallow incoming or outgoing application traffic
  - Control by application process
  - View all data
- Identify and block unknown processes
  - Stop malware before it can start
- Manage centrally

Finding intrusions
- Host-based Intrusion Detection System (HIDS)
  - Uses log files to identify intrusions
  - Can reconfigure firewalls to block
- Host-based Intrusion Prevention System (HIPS)
  - Recognize and block known attacks
  - Secure OS and application configs, validate incoming service requests
  - Often built into endpoint protection software
- HIPS identification
  - Signatures, heuristics, behavioral
  - Buffer overflows, registry updates, writing files to the Windows folder
  - Access to non-encrypted data

3.2 - Boot Integrity

Hardware root of trust
- Security is based on trust
  - Is your data safely encrypted?
  - Is this web site legitimate?
  - Has the operating system been infected?
- The trust has to start somewhere
  - Trusted Platform Module (TPM),
  - Hardware Security Module (HSM)
  - Designed to be the hardware root of the trust
- Difficult to change or avoid
  - It's hardware
  - Won't work without the hardware

Trusted Platform Module (TPM)
- A specification for cryptographic functions
  - Hardware to help with all of this encryption stuff
- Cryptographic processor
  - Random number generator, key generators
- Persistent memory
  - Comes with unique keys burned in during production
- Versatile memory
  - Storage keys, hardware configuration information
- Password protected
  - No dictionary attacks

3.2 - Boot Integrity (continued)

Boot integrity
- The attack on our systems is constant
  - Techniques are constantly changing
- Attackers compromise a device
  - And want it to stay compromised
- The boot process is a perfect infection point
  - Rootkits run in kernel mode
  - Have the same rights as the operating system
- Protecting the boot process is important
  - Secure boot, trusted boot, and measured boot
  - A chain of trust

UEFI BIOS Secure Boot
- Secure Boot
  - Part of the UEFI specification
- UEFI BIOS protections
  - BIOS includes the manufacturer's public key
  - Digital signature is checked during a BIOS update
  - BIOS prevents unauthorized writes to the flash
- Secure Boot verifies the bootloader
  - Checks the bootloader's digital signature
  - Bootloader must be signed with a trusted certificate
  - Or a manually approved the digital signature

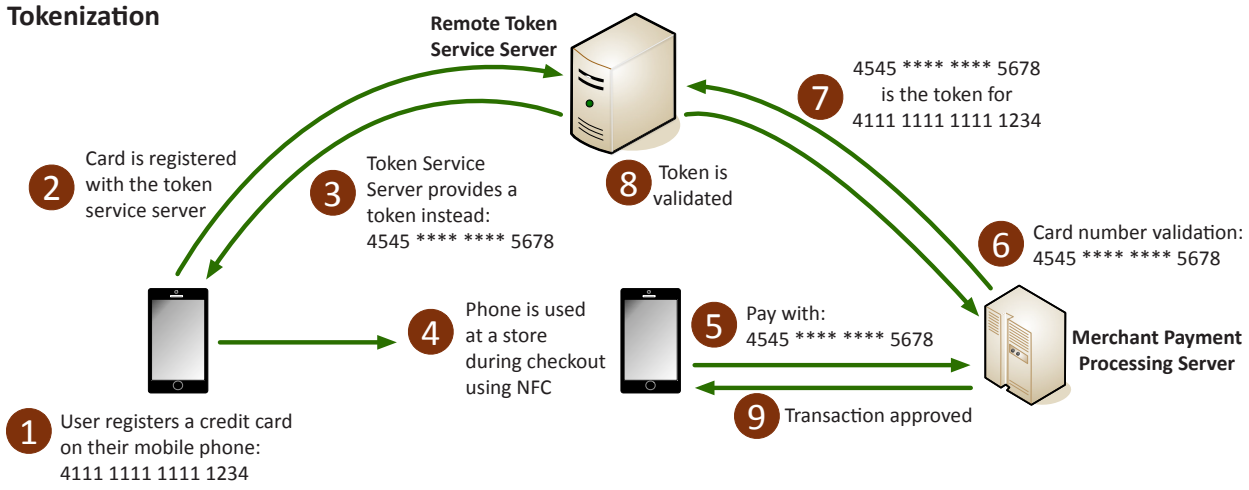
Trusted Boot
- Bootloader verifies digital signature of the OS kernel
  - A corrupted kernel will halt the boot process
- The kernel verifies all of the other startup components
  - Boot drivers, startup files
- Just before loading the drivers,
  - ELAM (Early Launch Anti-Malware) starts
  - Checks every driver to see if it's trusted
  - Windows won't load an untrusted driver

Measured Boot
- Nothing on this computer has changed
  - There have been no malware infections
  - How do you know?
- Easy when it's just your computer
  - More difficult when there are 1,000
- UEFI stores a hash of the firmware, boot drivers, and everything else loaded during the Secure Boot and
  - Trusted Boot process
  - Stored in the TPM
- Remote attestation
  - Device provides an operational report to a verification server
  - Encrypted and digitally signed with the TPM
- Attestation server receives the boot report
  - Changes are identified and managed

3.2 - Database Security

Database security
- Protecting stored data
  - And the transmission of that data
- Intellectual property storage
  - Data is valuable
- Compliance issues
  - PCI DSS, HIPAA, GDPR, etc.
- Keep the business running
  - Security provides continuity
- Breaches are expensive - Keep costs low

Tokenization
- Replace sensitive data with a non-sensitive placeholder
  - SSN 266-12-1112 is now 691-61-8539
- Common with credit card processing
  - Use a temporary token during payment
  - An attacker capturing the card numbers can't use them later
- This isn't encryption or hashing
  - The original data and token aren't mathematically related
  - No encryption overhead



3.2 - Database Security (continued)

Hashing a password

- Hashes represent data as a fixed-length string of text
  - A message digest, or "fingerprint"
- Will not have a collision (hopefully)
  - Different inputs will not have the same hash
- One-way trip
  - Impossible to recover the original message from the digest
  - A common way to store passwords

Adding some salt

- Salt
  - Random data added to a password when hashing
- Every user gets their own random salt
  - The salt is commonly stored with the password
- Rainbow tables won't work with salted hashes
  - Additional random value added to the original password
- This slows things down the brute force process
  - It doesn't completely stop the reverse engineering

3.2 - Application Security

Secure coding concepts

- A balance between time and quality
  - Programming with security in mind is often secondary
- Testing, testing, testing
  - The Quality Assurance (QA) process
- Vulnerabilities will eventually be found
  - And exploited

Input validation

- What is the expected input?
  - Validate actual vs. expected
- Document all input methods
  - Forms, fields, type
- Check and correct all input (normalization)
  - A zip code should be only X characters long with a letter in the X column
  - Fix any data with improper input
- The fuzzers will find what you missed
  - Don't give them an opening

Secure cookies

- Cookies
  - Information stored on your computer by the browser
- Used for tracking, personalization, session management
  - Not executable, not generally a security risk
  - Unless someone gets access to them
- Secure cookies have a Secure attribute set
  - Browser will only send it over HTTPS
- Sensitive information should not be saved in a cookie
  - This isn't designed to be secure storage

HTTP secure headers

- An additional layer of security
  - Add these to the web server configuration
  - You can't fix every bad application
- Enforce HTTPS communication
  - Ensure encrypted communication
- Only allow scripts, stylesheets, or images from the local site
- Prevent XSS attacks
  - Prevent data from loading into an inline frame (iframe)
  - Also helps to prevent XSS attacks

Code signing

- An application is deployed
  - Users run application executable or scripts
- So many security questions
  - Has the application been modified in any way?
  - Can you confirm that the application was written by a specific developer?
- The application code can be digitally signed by the developer
  - Asymmetric encryption
  - A trusted CA signs the developer's public key
  - Developer signs the code with their private key
  - For internal apps, use your own CA

Allow list / deny list

- Any application can be dangerous
  - Vulnerabilities, trojan horses, malware
- Security policy can control app execution
  - Allow list, deny/block list
- Allow list
  - Nothing runs unless it's approved
  - Very restrictive
- Deny list
  - Nothing on the "bad list" can be executed
  - Anti-virus, anti-malware

Examples of allow and deny lists

- Decisions are made in the operating system
  - Often built-in to the operating system management
- Application hash
  - Only allows applications with this unique identifier
- Certificate
  - Allow digitally signed apps from certain publishers
- Path
  - Only run applications in these folders
- Network zone
  - The apps can only run from this network zone

3.2 - Application Security (continued)

Static code analyzers

- Static Application Security Testing (SAST)
  - Help to identify security flaws
- Many security vulnerabilities found easily
  - Buffer overflows, database injections, etc.
- Not everything can be identified through analysis
  - Authentication security, insecure cryptography, etc.
  - Don't rely on automation for everything
- Still have to verify each finding
  - False positives are an issue

Dynamic analysis (fuzzing)

- Send random input to an application
  - Fault-injecting, robustness testing, syntax testing, negative testing
- Looking for something out of the ordinary
  - Application crash, server error, exception
- 1988 class project at the University of Wisconsin
  - "Operating System Utility Program Reliability"
  - Professor Barton Miller
  - The Fuzz Generator

Fuzzing engines and frameworks

- Many different fuzzing options
  - Platform specific, language specific, etc.
- Very time and processor resource heavy
  - Many, many different iterations to try
  - Many fuzzing engines use high-probability tests
- Carnegie Mellon Computer
  - Emergency Response Team (CERT)
  - CERT Basic Fuzzing Framework (BFF)
  - https://professormesser.link/bff

Fuzzing engine results

Final Results

- test.c:32: [5] (buffer) *gets: Does not check for buffer overflows (CWE-120, CWE-20). Use fgets() instead.*

```
gets(f);
```

- test.c:56: [5] (buffer) *strncat: Easily used incorrectly (e.g., incorrectly computing the correct maximum size to add) [MS-banned] (CWE-120). Consider strcat_s, strlcat, snprintf, or automatically resizing strings. Risk is high; the length parameter appears to be a constant, instead of computing the number of characters left.*

```
strncat(d,s,sizeof(d)); /* Misuse - this should be flagged as riskier. */
```

- test.c:57: [5] (buffer) *_tcsncat: Easily used incorrectly (e.g., incorrectly computing the correct maximum size to add) [MS-banned] (CWE-120). Consider strcat_s, strlcat, or automatically resizing strings. Risk is high; the length parameter appears to be a constant, instead of computing the number of characters left.*

```
_tcsncat(d,s,sizeof(d)); /* Misuse - flag as riskier */
```

- test.c:60: [5] (buffer) *MultiByteToWideChar: Requires maximum length in CHARACTERS, not bytes (CWE-120). Risk is high, it appears that the size is given as bytes, but the function requires size as characters.*

```
MultiByteToWideChar(CP_ACP,0,szName,-1,wszUserName,sizeof(wszUserName));
```

- test.c:62: [5] (buffer) *MultiByteToWideChar: Requires maximum length in CHARACTERS, not bytes (CWE-120). Risk is high, it appears that the size is given as bytes, but the function requires size as characters.*

```
MultiByteToWideChar(CP_ACP,0,szName,-1,wszUserName,sizeof wszUserName);
```

- test.c:73: [5] (misc) *SetSecurityDescriptorDacl: Never create NULL ACLs; an attacker can set it to Everyone (Deny All Access), which would even forbid administrator access (CWE-732).*

```
SetSecurityDescriptorDacl(&sd,TRUE,NULL,FALSE);
```

- test.c:73: [5] (misc) *SetSecurityDescriptorDacl: Never create NULL ACLs; an attacker can set it to Everyone (Deny All Access), which would even forbid administrator access (CWE-732).*

```
SetSecurityDescriptorDacl(&sd,TRUE,NULL,FALSE);
```

- test.c:17: [4] (buffer) *strcpy: Does not check for buffer overflows when copying to destination [MS-banned] (CWE-120). Consider using snprintf, strcpy_s, or strlcpy (warning: strncpy easily misused).*

```
strcpy(b, a);
```

- test.c:20: [4] (buffer) *sprintf: Does not check for buffer overflows (CWE-120). Use sprintf_s, snprintf, or vsnprintf.*

```
sprintf(s, "hello %s", bug);
```

3.2 - Application Hardening

Application hardening

- Minimize the attack surface
  – Remove all possible entry points
- Remove the potential for all known vulnerabilities
  – As well as the unknown
- Some hardening may have compliance mandates
  – HIPAA servers, PCI DSS, etc.
- There are many different resources
  – Center for Internet Security (CIS)
  – Network and Security Institute (SANS)
  – National Institute of Standards and Technology (NIST)

Open ports and services

- Every open port is a possible entry point
  – Close everything except required ports
- Control access with a firewall
  – NGFW would be ideal
- Unused or unknown services
  – Installed with the OS or from other applications
- Applications with broad port ranges
  – Open port 0 through 65,535
- Use Nmap or similar port scanner to verify
  – Ongoing monitoring is important

Registry

- The primary configuration database for Windows
  – Almost everything can be configured from the registry
- Useful to know what an application modifies
  – Many third-party tools can show registry changes
- Some registry changes are important security settings
  – Configure registry permissions
  – Disable SMBv1

Disk encryption

- Prevent access to application data files
  – File system encryption
- Full disk encryption (FDE)
  – Encrypt everything on the drive
  – BitLocker, FileVault, etc.
- Self-encrypting drive (SED)
  – Hardware-based full disk encryption
  – No operating system software needed
- Opal storage specification
  – The standard for of SED storage

Operating system hardening

- Many and varied
  – Windows, Linux, iOS, Android, et al.
- Updates
  – Operating system updates/service packs, security patches
- User accounts
  – Minimum password lengths and complexity
  – Account limitations
- Network access and security
  – Limit network access
- Monitor and secure
  – Anti-virus, anti-malware

3.2 - Application Hardening (continued)

Patch management
- Incredibly important
  - System stability, security fixes
- Monthly updates
  - Incremental (and important)
- Emergency out-of-band updates
  - Zero-day and important security discoveries
- Third-party updates
  - Application developers, device drivers
- Auto-update - Not always the best option

Sandboxing
- Applications cannot access unrelated resources
  - They play in their own sandbox
- Commonly used during development
  - Can be a useful production technique
- Used in many different deployments
  - Virtual machines
  - Mobile devices
  - Browser iframes (Inline Frames)
  - Windows User Account Control (UAC)

3.3 - Load Balancing

Balancing the load
- Distribute the load
  - Multiple servers
  - Invisible to the end-user
- Large-scale implementations
  - Web server farms, database farms
- Fault tolerance
  - Server outages have no effect
  - Very fast convergence

Load balancer
- Configurable load
  - Manage across servers
- TCP offload
  - Protocol overhead
- SSL offload
  - Encryption/Decryption
- Caching
  - Fast response
- Prioritization
  - QoS
- Content switching
  - Application-centric balancing

Scheduling
- Round-robin
  - Each server is selected in turn
- Weighted round-robin
  - Prioritize the server use
- Dynamic round-robin
  - Monitor the server load and distribute to the server with the lowest use
- Active/active load balancing

Affinity
- Affinity
  - A kinship, a likeness
- Many applications require communication to the same instance
  - Each user is “stuck” to the same server
  - Tracked through IP address or session IDs
  - Source affinity / sticky session / session persistence
- Active/active load balancing

Active/passive load balancing
- Some servers are active
  - Others are on standby
- If an active server fails, the passive server takes its place

3.3 - Network Segmentation

Segmenting the network
- Physical, logical, or virtual segmentation
  - Devices, VLANs, virtual networks
- Performance
  - High-bandwidth applications
- Security
  - Users should not talk directly to database servers
  - The only applications in the core are SQL and SSH
- Compliance
  - Mandated segmentation (PCI compliance)
  - Makes change control much easier

Physical segmentation
- Devices are physically separate - Switch A and Switch B
- Must be connected to provide communication
  - Direct connect, or another switch or router
- Web servers in one rack
  - Database servers on another
- Customer A on one switch, customer B on another
  - No opportunity for mixing data
- Separate devices
  - Multiple units, separate infrastructure

Logical segmentation with VLANs
- Virtual Local Area Networks (VLANs)
  - Separated logically instead of physically
  - Cannot communicate between VLANs without a Layer 3 device / router

3.3 - Network Segmentation (continued)

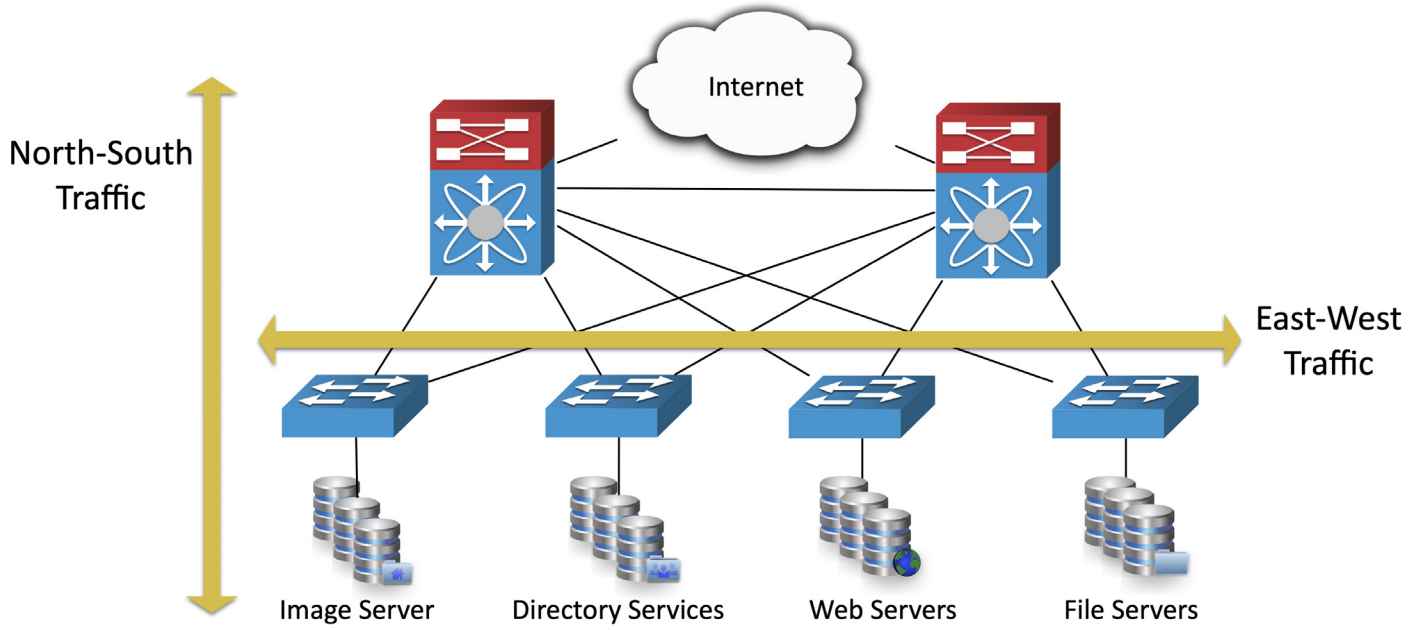
Screened subnet
- Previously known as the demilitarized zone (DMZ)
  - An additional layer of security between the Internet and you
  - Public access to public resources

East-west traffic
- Traffic flows within a data center
  - Important to know where traffic starts and ends
- East-west
  - Traffic between devices in the same data center
  - Relatively fast response times
- North-south traffic
  - Ingress/egress to an outside device
  - A different security posture than east-west traffic

Extranet
- A private network for partners
  - Vendors, suppliers
- Usually requires additional authentication
  - Only allow access to authorized users

Intranet
- Private network - Only available internally
- Company announcements, important documents, other company business
  - Employees only
- No external access
  - Internal or VPN access only

Zero-trust
- Many networks are relatively open on the inside
  - Once you're through the firewall, there are few security controls
- Zero trust is a holistic approach to network security
  - Covers every device, every process, every person
- Everything must be verified
  - Nothing is trusted
  - Multifactor authentication, encryption, system permissions, additional firewalls, monitoring and analytics, etc.



3.3 - Virtual Private Networks

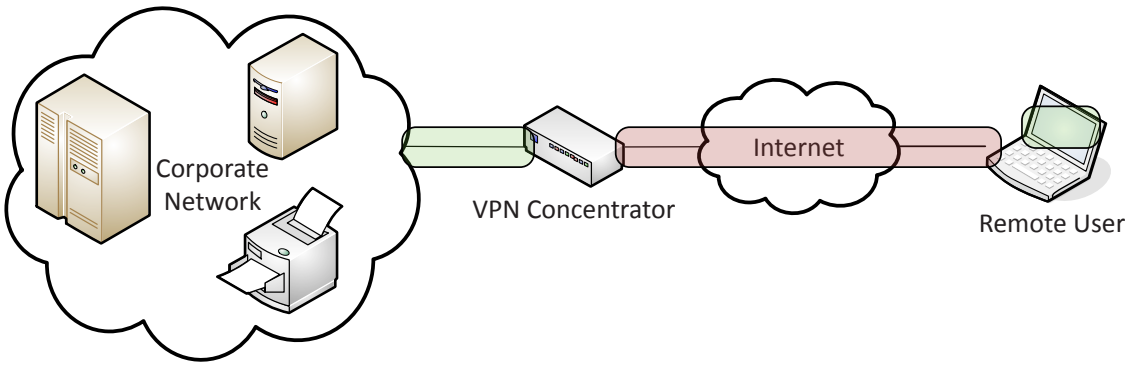
VPNs
- Virtual Private Networks
  - Encrypted (private) data traversing a public network
- Concentrator
  - Encryption/decryption access device
  - Often integrated into a firewall
- Many deployment options
  - Specialized cryptographic hardware
  - Software-based options available
- Used with client software
  - Sometimes built into the OS

SSL VPN (Secure Sockets Layer VPN)
- Uses common SSL/TLS protocol (tcp/443)
  - (Almost) No firewall issues!
- No big VPN clients
  - Usually remote access communication
- Authenticate users
  - No requirement for digital certificates or shared passwords (like IPSec)
- Can be run from a browser or from a (usually light) VPN client
  - Across many operating systems

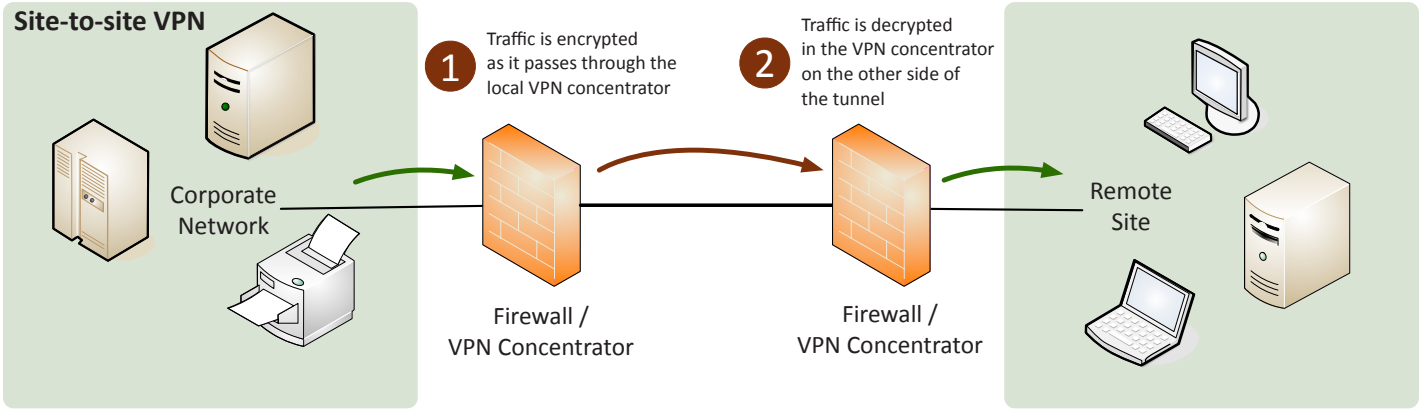
3.3 - Virtual Private Networks (continued)

Remote access VPN

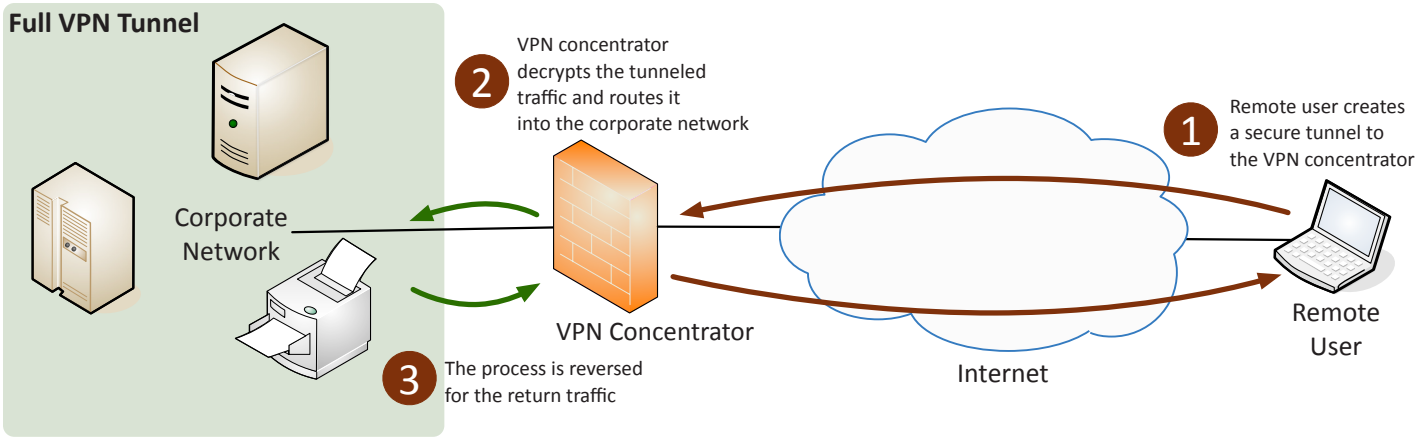
- On-demand access from a remote device
  - Software connects to a VPN concentrator
- Some software can be configured as always-on



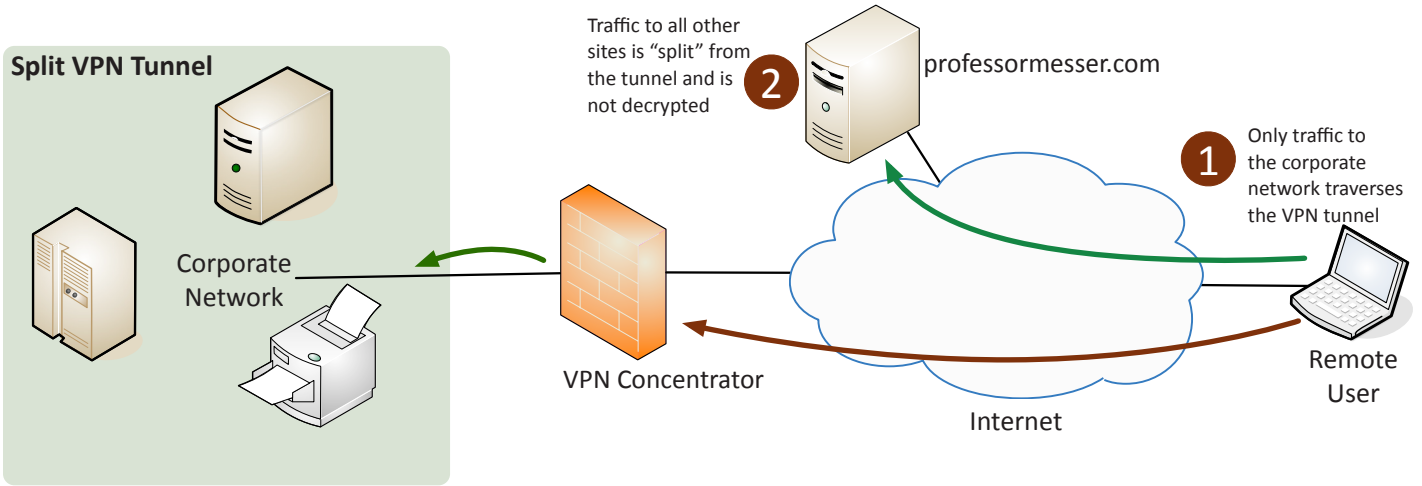
Site-to-site VPN



Full VPN Tunnel



Split VPN Tunnel



3.3 - Virtual Private Networks (continued)

L2TP

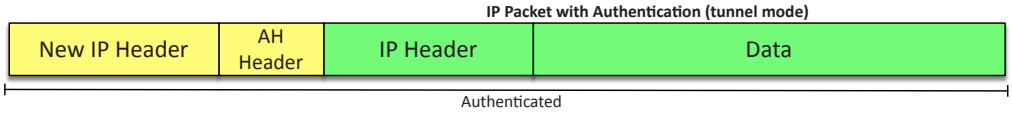
- Layer 2 Tunneling Protocol
  - Connecting sites over a layer 3 network as if they were connected at layer 2
- Commonly implemented with IPsec
  - L2TP for the tunnel, IPsec for the encryption
  - L2TP over IPsec (L2TP/IPsec)

IPSec (Internet Protocol Security)

- Security for OSI Layer 3
  - Authentication and encryption for every packet
- Confidentiality and integrity/anti-replay
  - Encryption and packet signing
- Very standardized
  - Common to use multi-vendor implementations
- Two core IPSec protocols
  - Authentication Header (AH)
  - Encapsulation Security Payload (ESP)

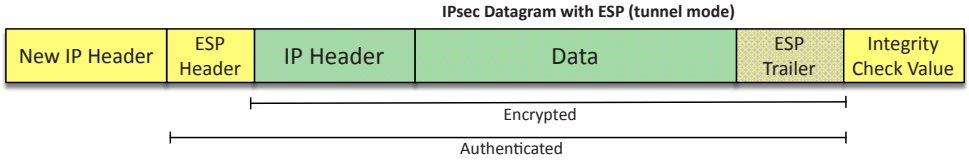
AH (Authentication Header)

- Data integrity
- Origin authentication
- Replay attack protection
- Keyed-hash mechanism
- No confidentiality/encryption



ESP (Encapsulating Security Payload)

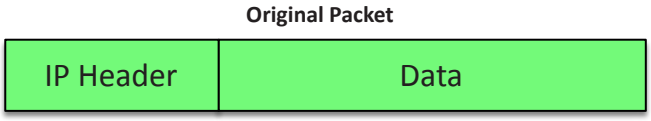
- Data confidentiality (encryption)
- Limited traffic flow confidentiality
- Data integrity
- Anti-replay protection

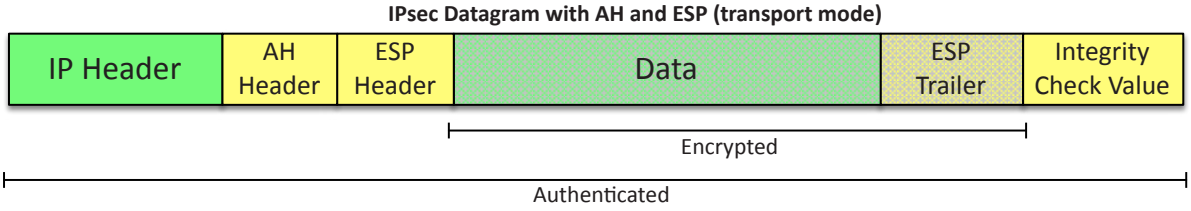


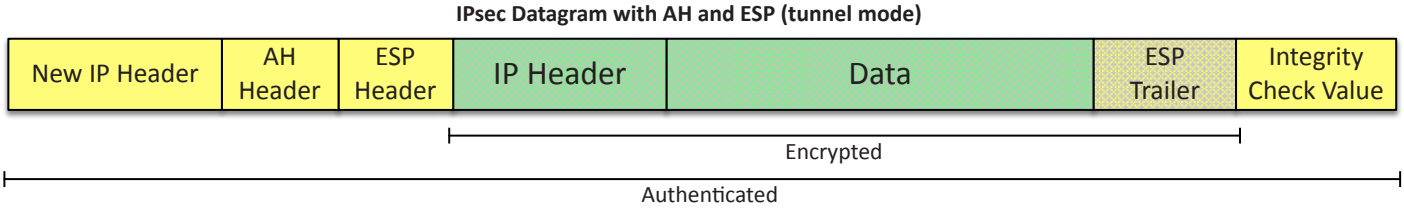
IPsec Transport mode and Tunnel mode

AH and ESP

- Combine the data integrity of AH with the confidentiality of ESP







3.3 - Virtual Private Networks (continued)

Authentication Header (AH)
- Hash of the packet and a shared key
  - SHA-2 is common
  - Adds the AH to the packet header
- This doesn't provide encryption
  - Provides data integrity (hash)
  - Guarantees the data origin (authentication)
  - Prevents replay attacks (sequence numbers)

Encapsulation Security Payload (ESP)
- Encrypts and authenticates the tunneled data
  - Commonly uses SHA-2 for hash, AES for encryption
  - Adds a header, a trailer, and an Integrity Check Value
- Combine with Authentication Header (AH) for integrity and authentication of the outer header

IPsec Transport mode and Tunnel mode
- Tunnel mode is the most common
  - Transport mode may not even be an option

HTML5 VPNs
- Hypertext Markup Language version 5
  - The language commonly used in web browsers
- Includes comprehensive API support
  - Application Programming Interface
  - Web cryptography API
- Create a VPN tunnel without a separate VPN application
  - Nothing to install
- Use an HTML5 compliant browser
  - Communicate directly to the VPN concentrator

3.3 - Port Security

Port security
- There's a lot of security that happens at the physical switch interface
  - Often the first and last point of transmission
- Control and protect
  - Limit overall traffic
  - Control specific traffic types
  - Watch for unusual or unwanted traffic
- Different options are available
  - Manage different security issues

Broadcasts
- Send information to everyone at once
  - One frame or packet, received by everyone
  - Every device must examine the broadcast
- Limited scope - The broadcast domain
- Routing updates, ARP requests - Can add up quickly
- Malicious software or a bad NIC
  - Not always normal traffic
- Not used in IPv6
  - Focus on multicast

Broadcast storm control
- The switch can control broadcasts
  - Limit the number of broadcasts per second
- Can often be used to control multicast and unknown unicast traffic
  - Tight security posture
- Manage by specific values or by percentage
  - Or the change over normal traffic patterns

Loop protection
- Connect two switches to each other
  - They'll send traffic back and forth forever
  - There's no "counting" mechanism at the MAC layer
- This is an easy way to bring down a network
  - And somewhat difficult to troubleshoot
  - Relatively easy to resolve
- IEEE standard 802.1D to prevent loops in bridged (switched) networks (1990)
  - Created by Radia Perlman
  - Used practically everywhere

BPDU Guard
- Spanning tree takes time to determine if a switch port should forward frames
  - Bypass the listening and learning states
  - Cisco calls this PortFast
- BPDU (Bridge Protocol Data Unit)
  - The spanning tree control protocol
- If a BPDU frame is seen on a PortFast configured interface (i.e., a workstation), shut down the interface
  - This shouldn't happen - Workstations don't send BPDUs

DHCP Snooping
- IP tracking on a layer 2 device (switch)
  - The switch is a DHCP firewall
  - Trusted: Routers, switches, DHCP servers
  - Untrusted: Other computers, unofficial DHCP servers
- Switch watches for DHCP conversations
  - Adds a list of untrusted devices to a table
- Filters invalid IP and DHCP information
  - Static IP addresses
  - Devices acting as DHCP servers
  - Other invalid traffic patterns

MAC filtering
- Media Access Control
  - The "hardware" address
- Limit access through the physical hardware address
  - Keeps the neighbors out
  - Additional administration with visitors
- Easy to find working MAC addresses through wireless LAN analysis
  - MAC addresses can be spoofed
  - Free open-source software
- Security through obscurity

3.3 - Secure Networking

Domain Name Resolution
- DNS had no security in the original design
  - Relatively easy to poison a DNS
- DNSSEC
  - Domain Name System Security Extensions
- Validate DNS responses
  - Origin authentication
  - Data integrity
- Public key cryptography
  - DNS records are signed with a trusted third party
  - Signed DNS records are published in DNS

Using a DNS for security
- Stop end users from visiting dangerous sites
  - The DNS resolves to a sinkhole address
- A query to a known-malicious address can identify infected systems
  - And prevent further exploitation
- Content filtering
  - Prevent DNS queries to unwanted or suspicious sites

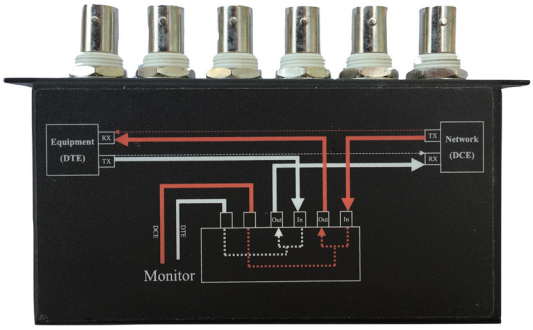
Out-of-band management
- The network isn't available
  - Or the device isn't accessible from the network
- Most devices have a separate management interface
  - Usually a serial connection / USB
- Connect a modem
  - Dial-in to manage the device
- Console router / comm server
  - Out-of-band access for multiple devices
  - Connect to the console router, then choose where you want to go

The need for QoS
- Many different devices
  - Desktop, laptop, VoIP phone, mobile devices
- Many different applications
  - Mission critical applications, streaming video, streaming audio
- Different apps have different network requirements
  - Voice is real-time
  - Recorded streaming video has a buffer
  - Database application is interactive
- Some applications are "more important" than others
  - Voice traffic needs to have priority over YouTube

QoS (Quality of Service)
- Prioritize traffic performance
  - Voice over IP traffic has priority over web-browsing
  - Prioritize by maximum bandwidth, traffic rate, VLAN, etc.
- Quality of Service
  - Describes the process of controlling traffic flows
- Many different methods
  - Across many different topologies

IPv6 security is different
- More IP address space
  - More difficult to IP/port scan (but not impossible)
  - The tools already support IPv6
- No need for NAT
  - NAT is not a security feature
- Some attacks disappear
  - No ARP, so no ARP spoofing
- New attacks will appear
  - For example, Neighbor Cache Exhaustion
- IPsec built in / IPsec ready

Taps and port mirrors
- Intercept network traffic
  - Send a copy to a packet capture device
- Physical taps
  - Disconnect the link, put a tap in the middle
  - Can be an active or passive tap
- Port mirror
  - Port redirection, SPAN (Switched Port ANalyzer)
  - Software-based tap
  - Limited functionality, but can work well in a pinch



Monitoring services
- Constant cybersecurity monitoring
  - Ongoing security checks
  - A staff of cybersecurity experts at a Security Operations Center (SoC)
- Identify threats
  - A broad range of threats across many different organizations
- Respond to events
  - Faster response time
- Maintain compliance
  - Someone else ensures PCI DSS, HIPAA compliance, etc.

FIM (File Integrity Monitoring)
- Some files change all the time
  - Some files should NEVER change
- Monitor important operating system and application files
  - Identify when changes occur
- Windows - SFC (System File Checker)
- Linux - Tripwire
- Many host-based IPS options

3.3 - Firewalls

The universal security control
- Standard issue
  - Home, office, and in your operating system
- Control the flow of network traffic
  - Everything passes through the firewall
- Corporate control of outbound and inbound data
  - Sensitive materials
- Control of inappropriate content
  - Not safe for work, parental controls
- Protection against evil
  - Anti-virus, anti-malware

Network-based firewalls
- Filter traffic by port number or application
  - Traditional vs. NGFW firewalls
- Encrypt traffic - VPN between sites
- Most firewalls can be layer 3 devices (routers)
  - Often sits on the ingress/egress of the network
  - Network Address
  - Translation (NAT) functionality
  - Authenticate dynamic routing communication

Stateless firewall
- Does not keep track of traffic flows
  - Each packet is individually examined, regardless of past history
  - Traffic sent outside of an active session will traverse a stateless firewall

Stateful firewall
- Stateful firewalls remember the "state" of the session
  - Everything within a valid flow is allowed

UTM / All-in-one security appliance
- Unified Threat Management (UTM) /
- Web security gateway
- URL filter / Content inspection
- Malware inspection
- Spam filter
- CSU/DSU
- Router, Switch
- Firewall
- IDS/IPS
- Bandwidth shaper
- VPN endpoint

Next-generation firewall (NGFW)
- The OSI Application Layer
  - All data in every packet
- Can be called different names
  - Application layer gateway
  - Stateful multilayer inspection
  - Deep packet inspection
- Requires some advanced decodes
  - Every packet must be analyzed and categorized before a security decision is determined

NGFWs
- Network-based Firewalls
  - Control traffic flows based on the application
  - Microsoft SQL Server, Twitter, YouTube
- Intrusion Prevention Systems
  - Identify the application
  - Apply application-specific vulnerability signatures to the traffic
- Content filtering
  - URL filters
  - Control website traffic by category

Web application firewall (WAF)
- Not like a "normal" firewall
  - Applies rules to HTTP/HTTPS conversations
- Allow or deny based on expected input
  - Unexpected input is a common method of exploiting an application
- SQL injection
  - Add your own commands to an application's SQL query
- A major focus of Payment Card Industry
  - Data Security Standard (PCI DSS)

Firewall rules
- Access control lists (ACLs)
  - Allow or disallow traffic based on tuples
  - Groupings of categories
  - Source IP, Destination IP, port number, time of day, application, etc.
- A logical path
  - Usually top-to-bottom
- Can be very general or very specific
  - Specific rules are usually at the top
- Implicit deny
  - Most firewalls include a deny at the bottom
  - Even if you didn't put one

Firewall characteristics
- Open-source vs. proprietary
  - Open-source provides traditional firewall functionality
  - Proprietary features include application control and high-speed hardware
- Hardware vs. software
  - Purpose-built hardware provides efficient and flexible connectivity options
  - Software-based firewalls can be installed almost anywhere
- Appliance vs. host-based vs. virtual
  - Appliances provide the fastest throughput
  - Host-based firewalls are application-aware and can view non-encrypted data
  - Virtual firewalls provide valuable East/West network security

3.3 - Network Access Control

Edge vs. access control
- Control at the edge
  - Your Internet link
  - Managed primarily through firewall rules
  - Firewall rules rarely change
- Access control
  - Control from wherever you are - Inside or outside
  - Access can be based on many rules
  - By user, group, location, application, etc.
  - Access can be easily revoked or changed
  - Change your security posture at any time

Posture assessment
- You can't trust everyone's computer
  - BYOD (Bring Your Own Device)
  - Malware infections / missing anti-malware
  - Unauthorized applications
- Before connecting to the network, perform a health check
  - Is it a trusted device?
  - Is it running anti-virus? Which one? Is it updated?
  - Are the corporate applications installed?
  - Is it a mobile device?
  - Is the disk encrypted?
  - The type of device doesn't matter - Windows, Mac, Linux, iOS, Android

Health checks/posture assessment
- Persistent agents
  - Permanently installed onto a system
  - Periodic updates may be required
- Dissolvable agents
  - No installation is required
  - Runs during the posture assessment
  - Terminates when no longer required
- Agentless NAC
  - Integrated with Active Directory
  - Checks are made during login and logoff
  - Can't be scheduled

Failing your assessment
- What happens when a posture assessment fails?
  - Too dangerous to allow access
- Quarantine network, notify administrators
  - Just enough network access to fix the issue
- Once resolved, try again
  - May require additional fixes

3.3 - Intrusion Prevention

NIDS and NIPS
- Intrusion Detection System / Intrusion Prevention System
  - Watch network traffic
- Intrusions
  - Exploits against operating systems, applications, etc.
  - Buffer overflows, cross-site scripting, other vulnerabilities
- Detection vs. Prevention
  - Detection – Alarm or alert
  - Prevention – Stop it before it gets into the network

Passive monitoring
- Examine a copy of the traffic
  - Port mirror (SPAN), network tap
- No way to block (prevent) traffic

Out-of-band-response
- When malicious traffic is identified,
  - IPS sends TCP RST (reset) frames
  - After-the-fact
  - Limited UDP response available

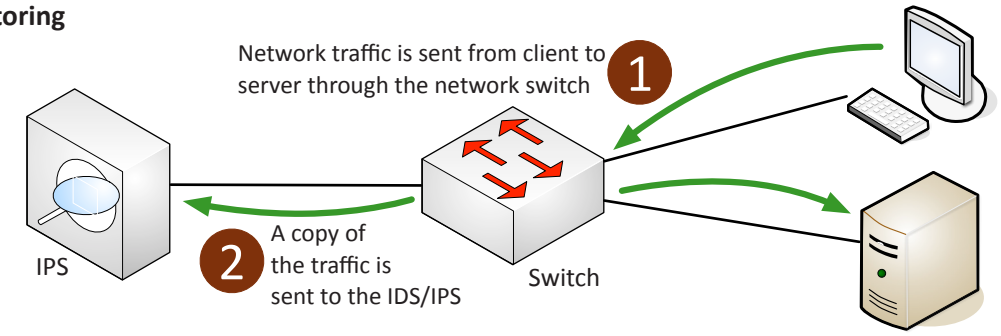
Inline monitoring
- IDS/IPS sits physically inline
  - All traffic passes through the IDS/IPS

In-band response
- Malicious traffic is immediately identified
  - Dropped at the IPS
  - Does not proceed through the network

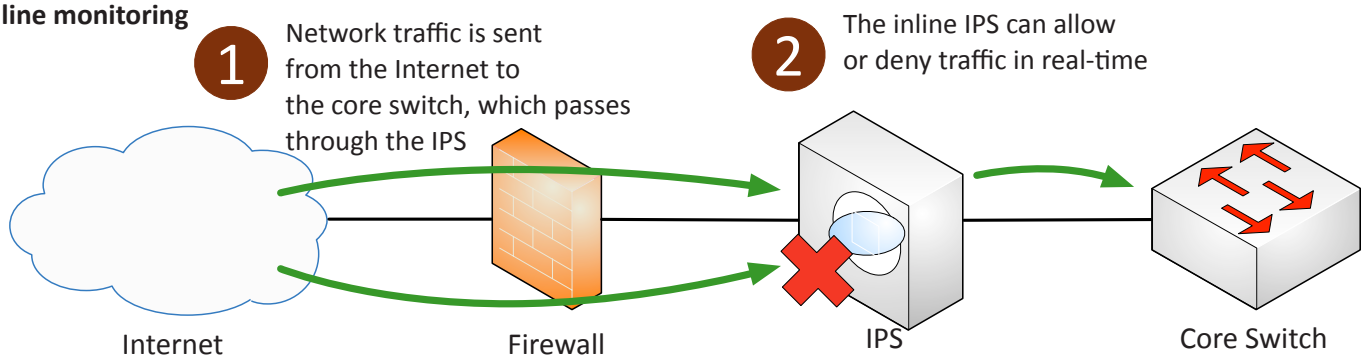
Identification technologies
- Signature-based
  - Look for a perfect match
- Anomaly-based
  - Build a baseline of what's "normal"
- Behavior-based
  - Observe and report
- Heuristics
  - Use artificial intelligence to identify

3.3 - Intrusion Prevention (continued)

Passive monitoring



Inline monitoring



3.3 - Other Network Appliances

Hardware Security Module (HSM)

- High-end cryptographic hardware
  - Plug-in card or separate hardware device
- Key backup
  - Secured storage
- Cryptographic accelerators
  - Offload that CPU overhead from other devices
- Used in large environments

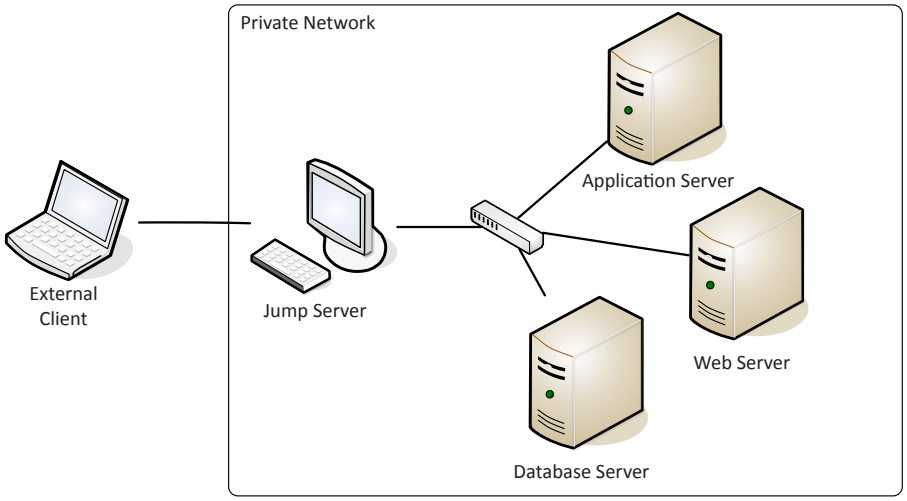
Clusters, redundant power

Jump server

- Access secure network zones
  - Provides an access mechanism to a protected network
- Highly-secured device
  - Hardened and monitored
- SSH / Tunnel / VPN to the jump server
  - RDP, SSH, or jump from there
- A significant security concern
  - Compromise to the jump server is a significant breach

Sensors and collectors

- Aggregate information from network devices
  - Built-in sensors, separate devices
  - Integrated into switches, routers, servers, firewalls, etc.
- Sensors
  - Intrusion prevention systems, firewall logs, authentication logs, web server access logs, database transaction logs, email logs
- Collectors
  - Proprietary consoles (IPS, firewall),
  - SIEM consoles, syslog servers
  - Many SIEMs include a correlation engine to compare diverse sensor data



3.4 - Wireless Cryptography

Securing a wireless network

- An organization's wireless network can contain confidential information
  - Not everyone is allowed access
- Authenticate the users before granting access
  - Who gets access to the wireless network?
  - Username, password, multi-factor authentication
- Ensure that all communication is confidential
  - Encrypt the wireless data
- Verify the integrity of all communication
  - The received data should be identical to the original sent data
  - A message integrity check (MIC)

Wireless encryption

- All wireless computers are radio transmitters and receivers
  - Anyone can listen in
- Solution: Encrypt the data - Everyone has an encryption key
- Only people with the right key can transmit and listen
  - WPA2 and WPA3

WPA2 and CCMP

- Wi-Fi Protected Access II (WPA2)
  - WPA2 certification began in 2004
- CCMP block cipher mode
  - Counter Mode with Cipher Block Chaining
  - Message Authentication Code Protocol, or
  - Counter/CBC-MAC Protocol
- CCMP security services
  - Data confidentiality with AES
  - Message Integrity Check (MIC) with CBC-MAC

WPA3 and GCMP

- Wi-Fi Protected Access 3 (WPA3) - Introduced in 2018
- GCMP block cipher mode
  - Galois/Counter Mode Protocol
  - A stronger encryption than WPA2
- GCMP security services
  - Data confidentiality with AES
  - Message Integrity Check (MIC) with
  - Galois Message Authentication Code (GMAC)

The WPA2 PSK problem

- WPA2 has a PSK brute-force problem
  - Listen to the four-way handshake
  - Some methods can derive the PSK hash without the handshake
  - Capture the hash
- With the hash, attackers can brute force the pre-shared key (PSK)
- This has become easier as technology improves
  - A weak PSK is easier to brute force
  - GPU processing speeds
  - Cloud-based password cracking
- Once you have the PSK, you have everyone's wireless key
  - There's no forward secrecy

SAE

- WPA3 changes the PSK authentication process
  - Includes mutual authentication
  - Creates a shared session key without sending that key across the network
  - No more four-way handshakes, no hashes, no brute force attacks
  - Adds perfect forward secrecy
- Simultaneous Authentication of Equals (SAE)
  - A Diffie-Hellman derived key exchange with an authentication component
  - Everyone uses a different session key, even with the same PSK
  - An IEEE standard - the dragonfly handshake

3.4 - Wireless Authentication Methods

Wireless authentication methods

- Gain access to a wireless network
  - Mobile users
  - Temporary users
- Credentials
  - Shared password / pre-shared key (PSK)
  - Centralized authentication (802.1X)
- Configuration
  - Part of the wireless network connection
  - Prompted during the connection process

Wireless security modes

- Configure the authentication on your wireless access point / wireless router
- Open System
  - No password is required
- WPA3-Personal / WPA3-PSK
  - WPA3 with a pre-shared key
  - Everyone uses the same key
  - Unique WPA3 session key is derived from the PSK using SAE (Simultaneous Authentication of Equals)
- WPA3-Enterprise / WPA3-802.1X
  - Authenticates users individually with an authentication server (i.e., RADIUS)

Captive Portal

- Authentication to a network - Common on wireless networks
- Access table recognizes a lack of authentication
  - Redirects your web access to a captive portal page
- Username / password - And additional authentication factors
- Once proper authentication is provided, the web session continues
  - Until the captive portal removes your access

3.4 - Wireless Authentication Methods (continued)

Using WPS
- Wi-Fi Protected Setup
  - Originally called Wi-Fi Simple Config
- Allows "easy" setup of a mobile device
  - A passphrase can be complicated to a novice
- Different ways to connect
  - PIN configured on access point must be entered on the mobile device
  - Push a button on the access point
  - Near-field communication -
  - Bring the mobile device close to the access point

The WPS hack
- December 2011 - WPS has a design flaw
  - It was built wrong from the beginning
- PIN is an eight-digit number
  - Really seven digits and a checksum
  - Seven digits, 10,000,000 possible combinations
- The WPS process validates each half of the PIN
  - First half, 4 digits. Second half, 3 digits.
  - First half, 10,000 possibilities, second half, 1,000 possibilities
- It takes about four hours to go through all of them
  - Most devices never considered a lockout function
  - Brute force lockout features are now the norm

3.4 - Wireless Authentication Protocols

Wireless authentication
- We've created many authentication methods through the years
  - A network administrator has many choices
- Use a username and password
  - Other factors can be included
- Commonly used on wireless networks
  - Also works on wired networks

EAP
- Extensible Authentication Protocol (EAP)
  - An authentication framework
- Many different ways to authenticate based on RFC standards
  - Manufacturers can build their own EAP methods
- EAP integrates with 802.1X
  - Prevents access to the network until the authentication succeeds

IEEE 802.1X
- IEEE 802.1X
  - Port-based Network Access Control (NAC)
  - You don't get access to the network until you authenticate
- Used in conjunction with an access database
  - RADIUS, LDAP, TACACS+

IEEE 802.1X and EAP
- Supplicant
  - The client
- Authenticator
  - The device that provides access
- Authentication server
  - Validates the client credentials

EAP-FAST
- EAP Flexible Authentication via Secure Tunneling
  - Authentication server (AS) and supplicant share a protected access credential (PAC) (shared secret)
- Supplicant receives the PAC
- Supplicant and AS mutually authenticate and negotiate a Transport Layer Security (TLS) tunnel
- User authentication occurs over the TLS tunnel
- Need a RADIUS server
  - Provides the authentication database and EAP-FAST services

PEAP
- Protected Extensible Authentication Protocol
  - Protected EAP
  - Created by Cisco, Microsoft, and RSA Security
- Also encapsulates EAP in a TLS tunnel
  - AS uses a digital certificate instead of a PAC
  - Client doesn't use a certificate
- User authenticates with MSCHAPv2
  - Authenticates to Microsoft's MS-CHAPv2 databases
- User can also authenticate with a GTC
  - Generic Token Card, hardware token generator

EAP-TLS
- EAP Transport Layer Security
  - Strong security, wide adoption
  - Support from most of the industry
- Requires digital certificates on the AS and all other devices
  - AS and supplicant exchange certificates for mutual authentication
  - TLS tunnel is then built for the user authentication process
- Relatively complex implementation
  - Need a public key infrastructure (PKI)
  - Must deploy and manage certificates to all wireless clients
  - Not all devices can support the use of digital certificates

3.4 - Wireless Authentication Protocols (continued)

EAP-TTLS

- EAP Tunneled Transport Layer Security
  - Support other authentication protocols in a TLS tunnel
- Requires a digital certificate on the AS
  - Does not require digital certificates on every device
  - Builds a TLS tunnel using this digital certificate
- Use any authentication method inside the TLS tunnel
  - Other EAPs
  - MSCHAPv2
  - Anything else

RADIUS Federation

- Use RADIUS with federation
  - Members of one organization can authenticate to the network of another organization
  - Use their normal credentials
- Use 802.1X as the authentication method
  - And RADIUS on the backend - EAP to authenticate
- Driven by eduroam (education roaming)
  - Educators can use their normal authentication when visiting a different campus
  - https://www.eduroam.org/

3.4 - Installing Wireless Networks

Site surveys

- Determine existing wireless landscape
  - Sample the existing wireless spectrum
- Identify existing access points
  - You may not control all of them
- Work around existing frequencies
  - Layout and plan for interference
- Plan for ongoing site surveys
  - Things will certainly change
- Heat maps - Identify wireless signal strengths

Wireless survey tools

- Signal coverage
- Potential interference
- Built-in tools
- 3rd-party tools
- Spectrum analyzer

Wireless packet analysis

- Wireless networks are incredibly easy to monitor
  - Everyone “hears” everything
- You have to be quiet
  - You can’t hear the network if you’re busy transmitting
- Some network drivers won’t capture wireless information
  - You’ll need specialized adapters/chipsets and drivers
- View wireless-specific information
  - Signal-to-noise ratio, channel information, etc.
- Try it yourself! - https://www.wireshark.org

Channel selection and overlaps

- Overlapping channels
  - Frequency conflicts - use non-overlapping channels
  - Automatic or manual configurations

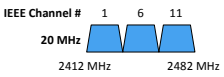
Access point placement

- Minimal overlap
  - Maximize coverage, minimize the number of access points
- Avoid interference
  - Electronic devices (microwaves)
  - Building materials
  - Third-party wireless networks
- Signal control
  - Place APs where the users are
  - Avoid excessive signal distance

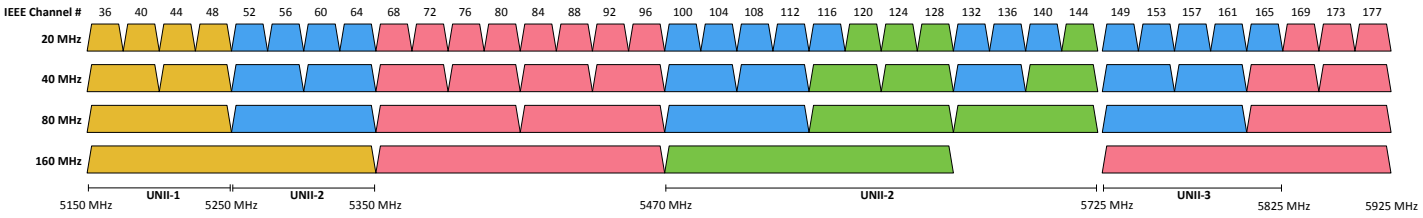
Wireless infrastructure security

- Wireless controllers
  - Centralized management of wireless access points
  - Manage system configuration and performance
- Securing wireless controllers
  - Control access to management console
  - Use strong encryption with HTTPS
  - Automatic logout after no activity
- Securing access points
  - Use strong passwords
  - Update to the latest firmware

2.4 GHz Spectrum for 802.11 - North America



5 GHz Spectrum for 802.11 - North America



3.5 - Mobile Networks

Point-to-point
- One-to-one connection
  - Conversation between two devices
- Connections between buildings
  - Point-to-point network links
- Wi-Fi repeaters
  - Extend the length of an existing network

Point-to-multipoint
- One of the most popular communication methods 802.11 wireless
- Does not imply full connectivity between nodes

Cellular networks
- Mobile devices
  - "Cell" phones
- Separate land into "cells"
  - Antenna coverages a cell with certain frequencies
- Security concerns
  - Traffic monitoring
  - Location tracking
  - Worldwide access to a mobile device

Wi-Fi
- Local network access
  - Local security problems
- Same security concerns as other Wi-Fi devices
- Data capture
  - Encrypt your data!
- On-path attack
  - Modify and/or monitor data
- Denial of service
  - Frequency interference

Bluetooth
- High speed communication over short distances
  - PAN (Personal Area Network)
- Connects our mobile devices
  - Smartphones, tethering, headsets and headphones, health monitors, automobile and phone integration, smartwatches, external speakers

RFID (Radio-frequency identification)
- It's everywhere
  - Access badges
  - Inventory/Assembly line tracking
  - Pet/Animal identification
  - Anything that needs to be tracked
- Radar technology
  - Radio energy transmitted to the tag
  - RF powers the tag, ID is transmitted back
  - Bidirectional communication
  - Some tag formats can be active/powered

Near field communication (NFC)
- Two-way wireless communication
  - Builds on RFID, which was one-way
- Payment systems
  - Google wallet, Apple Pay
- Bootstrap for other wireless
  - NFC helps with Bluetooth pairing
- Access token, identity "card"
  - Short range with encryption support

NFC security concerns
- Remote capture
  - It's a wireless network
  - 10 meters for active devices
- Frequency jamming - Denial of service
- Relay / Replay attack - Man in the middle
- Loss of RFC device control - Stolen/lost phone

IR (Infrared)
- Included on many smartphones, tablets, and smartwatches
  - Not really used much for printing
- Control your entertainment center
  - Almost exclusively IR
- File transfers are possible
- Other phones can be used to control your IR devices

USB (Universal Serial Bus)
- Physical connectivity to your mobile device
  - USB to your computer
  - USB, Lightning, or proprietary on your phone
- Physical access is always a concern
  - May be easier to gain access than over a remote connection
- A locked device is relatively secure
  - Always auto-lock
- Mobile phones can also exfiltrate
  - Phone can appear to be a USB storage device

Global Positioning System (GPS)
- Created by the U.S. Department of Defense
  - Over 30 satellites currently in orbit
- Precise navigation
  - Need to see at least 4 satellites
- Determines location based on timing differences
  - Longitude, latitude, altitude
- Mobile device location services and geotracking
  - Maps, directions
  - Determine physical location based on GPS,
  - WiFi, and cellular towers

3.5 - Mobile Device Management

Mobile Device Management (MDM)
- Manage company-owned and user-owned mobile devices
  - BYOD - Bring Your Own Device
- Centralized management of the mobile devices
  - Specialized functionality
- Set policies on apps, data, camera, etc.
  - Control the remote device
  - The entire device or a "partition"
- Manage access control
  - Force screen locks and PINs on these single user devices

Application management
- Managing mobile apps are a challenge
  - Mobile devices install apps constantly
- Not all applications are secure
  - And some are malicious
  - Android malware is a rapidly growing security concern
- Manage application use through whitelists
  - Only approved applications can be installed
  - Managed through the MDM
- A management challenge
  - New applications must be checked and added

Content management
- Mobile Content Management (MCM)
  - Secure access to data, protect data from outsiders
- File sharing and viewing
  - On-site content (Microsoft Sharepoint, file servers)
  - Cloud-based storage (Box, Office 365)
- Data sent from the mobile device
  - DLP (Data Loss Prevention) prevents copy/paste of sensitive data
  - Ensure data is encrypted on the mobile device
- Managed from the mobile device manager (MDM)

Remote wipe
- Remove all data from your mobile device
  - Even if you have no idea where it is
  - Often managed from the MDM
- Connect and wipe from the web
  - Nuke it from anywhere
- Need to plan for this
  - Configure your mobile device now
- Always have a backup
  - Your data can be removed at any time
  - As you are walking out the door

Geolocation
- Precise tracking details - Tracks within feet
- Can be used for good (or bad)
  - Find your phone, find you
- Most phones provide an option to disable
  - Limits functionality of the phones
- May be managed by the MDM

Geofencing
- Some MDMs allow for geofencing
  - Restrict or allow features when the device is in a particular area
- Cameras
  - Might only work when outside the office
- Authentication
  - Only allow logins when the device is located in a particular area

Screen lock
- All mobile devices can be locked
  - Keep people out of your data
- Simple passcode or strong passcode
  - Numbers vs. Alphanumeric
- Fail too many times?
  - Erase the phone
- Define a lockout policy
  - Create aggressive lockout timers
  - Completely lock the phone

Push notification services
- Information appears on the mobile device screen
  - The notification is "pushed" to your device
- No user intervention
  - Receive notifications from one app when using a completely different app
- Control of displayed notifications can be managed from the MDM
  - Or notifications can be pushed from the MDM

Passwords and PINs
- The universal help desk call
  - I need to reset my password
- Mobile devices use multiple authentication methods
  - Password/passphrase, PINs, patterns
- Recovery process can be initiated from the MDM
  - Password reset option is provided on the mobile device
  - "What is the name of your favorite car maiden cat's color?"
- MDM also has full control
  - Completely remove all security controls
  - Not the default or best practice

Biometrics
- You are the authentication factor
  - Fingerprint, face
- May not be the most secure authentication factor
  - Useful in some environments
  - Completely forbidden in others
- Availability is managed through the MDM
  - Organization determines the security of the device
- Can be managed per-app
  - Some apps require additional biometric authentication

3.5 - Mobile Device Management (continued)

Context-aware authentication
- Who needs 2FA?
  - The attackers can get around anything
- Authentication can be contextual
  - If it walks like a duck…
- Combine multiple contexts
  - Where you normally login (IP address
  - Where you normally frequent (GPS information)
  - Other devices that may be paired (Bluetooth, etc.)
- And others
  - An emerging technology
  - Another way to keep data safe

Containerization
- Difficult to separate personal from business
  - Especially when the device is BYOD
  - Owned by the employee
- Separate enterprise mobile apps and data
  - Create a virtual "container" for company data
  - A contained area - limit data sharing
  - Storage segmentation keeps data separate
- Easy to manage offboarding
  - Only the company information is deleted
  - Personal data is retained
  - Keep your pictures, video, music, email, etc.

Full device encryption
- Scramble all of the data on the mobile device
  - Even if you lose it, the contents are safe
- Devices handle this in different ways
  - Strongest/stronger/strong ?
- Encryption isn't trivial
  - Uses a lot of CPU cycles
  - Complex integration between hardware and software
- Don't lose or forget your password!
  - There's no recovery
  - Often backed up on the MDM

3.5 - Mobile Device Security

MicroSD HSM
- Shrink the PCI Express
  - Hardware Security Module - Now in a microSD card form
- Provides security services
  - Encryption, key generation, digital signatures, authentication
- Secure storage
  - Protect private keys - Cryptocurrency storage

Unified Endpoint Management (UEM)
- Manage mobile and non-mobile devices
  - An evolution of the Mobile Device Manager (MDM)
- End users use different types of devices
  - Their use has blended together
- Applications can be used across different platforms
  - Work on a laptop and a smartphone
- All of these devices can be used from anywhere
  - User's don't stay in one place

Mobile Application Management (MAM)
- Provision, update, and remove apps
  - Keep everyone running at the correct version
- Create an enterprise app catalog
  - Users can choose and install the apps they need
- Monitor application use
  - Apps used on a device, devices with unauthorized apps
- Remotely wipe application data
  - Securely manage remote data

SEAndroid
- Security Enhancements for Android
  - SELinux (Security-Enhanced Linux) in the Android OS
  - Supports access control security policies
- A project from the US National Security Agency (NSA)
  - Based on the NSA's SELinux
- Addresses a broad scope of system security
  - Kernel, userspace, and policy configuration
- Enabled by default with Android version 4.3
  - July 2013
  - Protect privileged Android system daemons
  - Prevent malicious activity
- Change from Discretionary Access Control (DAC) to Mandatory Access Control (MAC)
  - Move from user-assigned control to object labels and minimum user access
  - Isolates and sandboxes Android apps
- Centralized policy configuration
  - Manage Android deployments

3.5 - Mobile Device Enforcement

Third-party app stores
- Centralized app clearinghouses
  - Apple App Store
  - Google Play
- Not all applications are secure
  - Vulnerabilities, data leakage
- Not all applications are appropriate for business use
  - Games, instant messaging, etc.
- MDM can allow or deny app store use.

Rooting/jailbreaking
- Mobile devices are purpose-built systems
  - You don't need access to the operating system
- Gaining access - Android - Rooting / Apple iOS - Jailbreaking
- Install custom firmware
  - Replaces the existing operating system
- Uncontrolled access
  - Circumvent security features, sideload apps without using an app store
  - The MDM becomes relatively useless

Carrier unlocking
- Most phones are locked to a carrier
  - You can't use an AT&T phone on Verizon
  - Contract with a carrier subsidizes the cost of the phone
- You can unlock the phone
  - If your carrier allows it
  - A carrier lock may be illegal in your country
- Security revolves around connectivity
  - Moving to another carrier can circumvent the MDM
  - Preventing a SIM unlock may not be possible on a personal device

Firmware OTA updates
- The operating system of a mobile device is constantly changing - Similar to a desktop computer
- Updates are provided over the air (OTA)
  - No cable required
- Security patches or entire operating system updates
  - Significant changes without connecting the device
- This may not be a good thing
  - The MDM can manage what OTA updates are allowed

Camera use
- Cameras are controversial
  - They're not always a good thing
  - Corporate espionage, inappropriate use
- Almost impossible to control on the device
  - No good way to ensure the camera won't be used
- Camera use can be controlled by the MDM
  - Always disabled
  - Enabled except for certain locations (geo-fencing)

SMS/MMS
- Short Message Service / Multimedia Messaging Service
  - Text messages, video, audio
- Control of data can be a concern
  - Outbound data leaks, financial disclosures
  - Inbound notifications, phishing attempts
- MDM can enable or disable SMS/MMS
  - Or only allow during certain timeframes or locations

External media
- Store data onto external or removable drives
  - SD flash memory or USB/lightning drives
- Transfer data from flash
  - Connect to a computer to retrieve
- This is very easy to do
  - Limit data written to removable drives
  - Or prevent the use of them from the MDM

USB OTG
- USB On-The-Go - Connect devices directly together
  - No computer required, only a cable
- The mobile device can be both a host and a device
  - Read from an external device, then act as a storage device itself
  - No need for a third-party storage device
- A USB 2.0 standard - Commonly seen on Android devices
- Extremely convenient
  - From a security perspective, it's too convenient

Recording microphone
- Audio recordings
  - There are microphones on every mobile device
- Useful for meetings and note taking
  - A standard for college classes
- A legal liability
  - Every state has different laws
  - Every situation is different
- Disable or geo-fence - Manage from the MDM

Geotagging / GPS tagging
- Your phone knows where you are
  - Location Services, GPS
- Adds your location to document metadata
  - Longitude, latitude - Photos, videos, etc.
- Every document may contain geotagged information
  - You can track a user quite easily
- This may cause security concerns
  - Take picture, upload to social media

WiFi Direct/ad hoc
- We're so used to access points
  - SSID configurations
- The wireless standard includes an ad hoc mode
  - Connect wireless devices directly
  - Without an access point
- WiFi Direct simplifies the process
  - Easily connect many devices together
  - Common to see in home devices
- Simplicity can aid vulnerabilities
  - Invisible access to important devices

3.5 - Mobile Device Enforcement (continued)

Hotspot/tethering
- Turn your phone into a WiFi hotspot
  - Your own personal wireless router
  - Extend the cellular data network to all of your devices
- Dependent on phone type and provider
  - May require additional charges and data costs
- May provide inadvertent access to an internal network
  - Ensure proper security / passcode

Payment methods
- Send small amounts of data wirelessly over a limited area (NFC)
  - Built into your phone
  - Payment systems, transportation, in-person information exchange
- A few different standards
  - Apple Pay, Android Pay, Samsung Pay
- Bypassing primary authentication would allow payment
  - Use proper security - or disable completely

3.5 - Mobile Deployment Models

BYOD
- Bring Your Own Device / Bring Your Own Technology
- Employee owns the device
  - Need to meet the company's requirements
- Difficult to secure
  - It's both a home device and a work device
  - How is data protected?
  - What happens to the data when a device is sold or traded in?

COPE
- Corporate owned, personally enabled
  - Company buys the device
  - Used as both a corporate device and a personal device
- Organization keeps full control of the device
  - Similar to company-owned laptops and desktops
- Information is protected using corporate policies
  - Information can be deleted at any time
- CYOD - Choose Your Own Device
  - Similar to COPE, but with the user's choice of device

Corporate owned
- The company owns the device
  - And controls the content on the device
- The device is not for personal use
  - You'll need to buy your own device for home
- Very specific security requirements
  - Not able to mix business with home use

VDI/VMI
- Virtual Desktop Infrastructure / Virtual Mobile Infrastructure
  - The apps are separated from the mobile device
  - The data is separated from the mobile device
- Data is stored securely, centralized
- Physical device loss - Risk is minimized
- Centralized app development
  - Write for a single VMI platform
- Applications are managed centrally
  - No need to update all mobile devices

3.6 - Cloud Security Controls

HA across zones
- Availability zones (AZ)
  - Isolated locations within a cloud region (geographical location)
  - AZ commonly spans across multiple regions
  - Each AZ has independent power, HVAC, and networking
- Build applications to be highly available (HA)
  - Run as active/standby or active/active
  - Application recognizes an outage and moves to the other AZ
- Use load balancers to provide seamless HA
  - Users don't experience any application issues

Resource policies
- Identity and access management (IAM)
  - Who gets access, what they get access to
- Map job functions to roles
  - Combine users into groups
- Provide access to cloud resources
  - Set granular policies - Group, IP address, date and time
- Centralize user accounts, synchronize across all platforms

Secrets management
- Cloud computing includes many secrets
  - API keys, passwords, certificates
- This can quickly become overwhelming
  - Difficult to manage and protect
- Authorize access to the secrets
  - Limit access to the secret service
- Manage an access control policy
  - Limit users to only necessary secrets
- Provide an audit trail
  - Know exactly who accesses secrets and when

Integration and auditing
- Integrate security across multiple platforms
  - Different operating systems and applications
- Consolidate log storage and reporting
  - Cloud-based Security Information and Event Management (SIEM)
- Auditing - Validate the security controls
  - Verify compliance with financial and user data

3.6 - Securing Cloud Storage

Cloud storage
- Data is on a public cloud
  - But may not be public data
- Access can be limited
  - And protected
- Data may be required in different geographical locations
  - A backup is always required
- Availability is always important
  - Data is available as the cloud changes?

Permissions
- A significant cloud storage concern
  - One permission mistake can cause a data breach
  - Accenture, Uber, US Department of Defense
- Public access
  - Should not usually be the default
- Many different options
  - Identify and Access Management (IAM)
  - Bucket policies
  - Globally blocking public access
  - Don't put data in the cloud unless it really needs to be there

Encryption
- Cloud data is more accessible than non-cloud data
  - More access by more people
- Server-side encryption
  - Encrypt the data in the cloud
  - Data is encrypted when stored on disk
- Client-side encryption
  - Data is already encrypted when it's sent to the cloud
  - Performed by the application
- Key management is critical

Replication
- Copy data from one place to another
  - Real-time data duplication in multiple locations
- Disaster recovery, high availability
  - Plan for problems
  - Maintain uptime if an outage occurs
  - Hot site for disaster recovery
- Data analysis
  - Analytics, big data analysis
- Backups
  - Constant duplication of data

3.6 - Securing Cloud Networks

Cloud Networks
- Connect cloud components
  - Connectivity within the cloud
  - Connectivity from outside the cloud
- Users communicate to the cloud
  - From the public Internet
  - Over a VPN tunnel
- Cloud devices communicate between each other
  - Cloud-based network
  - East/west and north/south communication
  - No external traffic flows

Virtual networks
- A cloud contains virtual devices
  - Servers, databases, storage devices
- Virtual switches, virtual routers
  - Build the network from the cloud console
  - The same configurations as a physical device
- The network changes with the rest of the infrastructure
  - On-demand
  - Rapid elasticity

Public and private subnets
- Private cloud
  - All internal IP addresses
  - Connect to the private cloud over a VPN
  - No access from the Internet
- Public cloud
  - External IP addresses
  - Connect to the cloud from anywhere
- Hybrid cloud
  - Combine internal cloud resources with external
  - May combine both public and private subnets

Segmentation
- The cloud contains separate VPCs, containers, and microservices
  - Application segmentation is almost guaranteed
- Separation is a security opportunity
  - Data is separate from the application
  - Add security systems between application components
- Virtualized security technologies
  - Web Application Firewall (WAF)
  - Next-Generation Firewall (NGFW)
    - Intrusion Prevention System (IPS)

API inspection and integration
- Microservice architecture is the underlying application engine
  - A significant security concern
- API calls can include risk
  - Attempts to access critical data
  - Geographic origin
  - Unusual API calls
- API monitoring
  - View specific API queries
  - Monitor incoming and outgoing data

3.6 - Securing Compute Clouds

Compute cloud instances

- The IaaS component for the cloud computing environment
  - Amazon Elastic Compute Cloud (EC2)
  - Google Compute Engine (GCE)
  - Microsoft Azure Virtual Machines
- Manage computing resources
  - Launch a VM or container
  - Allocate additional resources
  - Disable/remove a VM or container

Security groups

- A firewall for compute instances
  - Control inbound and outbound traffic flows
- Layer 4 port number
  - TCP or UDP port
- Layer 3 address
  - Individual addresses
  - CIDR block notation
  - IPv4 or IPv6

Dynamic resource allocation

- Provision resources when they are needed
  - Based on demand - Provisioned automatically
- Scale up and down
  - Allocate compute resources where and when they are needed
  - Rapid elasticity
  - Pay for only what's used
- Ongoing monitoring
  - If CPU utilization hits a particular threshold, provision a new application instance

Instance awareness

- Granular security controls
  - Identify and manage very specific data flows
  - Each instance of a data flow is different
- Define and set policies
  - Allow uploads to the corporate box.com file share
    - Corporate file shares can contain PII
    - Any department can upload to the corporate file share
  - Deny certain uploads to a personal box.com file share
    - Allow graphics files
    - Deny any spreadsheet
    - Deny files containing credit card numbers
    - Quarantine the file and send an alert

Virtual private cloud endpoints

- Microservice architecture is the VPC gateway endpoints
  - Allow private cloud subnets to communicate to other cloud services
- Keep private resources private
  - Internet connectivity not required
- Add an endpoint to connect VPC resources

Container security

- Containers have similar security concerns as any other application deployment method
  - Bugs, insufficient security controls, misconfigurations
- Use container-specific operating systems
  - A minimalist OS designed for containers
- Group container types on the same host
  - The same purpose, sensitivity, and threat posture
  - Limit the scope of any intrusion

3.6 - Cloud Security Solutions

Cloud access security broker (CASB)

- Clients are at work, data is in the cloud
  - How do you keep everything secure?
  - The organization already has well-defined security policies
- How do you make your security policies work in the cloud?
  - Integrate a CASB
  - Implemented as client software, local security appliances, or cloud-based security solutions
- Visibility
  - Determine what apps are in use
  - Are they authorized to use the apps?
- Compliance
  - Are users complying with HIPAA? PCI?
- Threat prevention
  - Allow access by authorized users, prevent attacks
- Data security
  - Ensure that all data transfers are encrypted
  - Protect the transfer of PII with DLP

Application security

- Secure cloud-based applications
  - Complexity increases in the cloud
- Application misconfigurations
  - One of the most common security issues
  - Especially cloud storage
- Authorization and access
  - Controls should be strong enough for access from anywhere
- API security - Attackers will try to exploit interfaces and APIs

Next-Gen Secure Web Gateway (SWG)

- Protect users and devices
  - Regardless of location and activity
- Go beyond URLs and GET requests
  - Examine the application API
  - Dropbox for personal use or corporate use?
- Examine JSON strings and API requests
  - Allow or disallow certain activities
- Instance-aware security
  - A development instance is different than production

3.6 - Cloud Security Solutions (continued)

Firewalls in the cloud
- Control traffic flows in the cloud
  - Inside the cloud and external flows
- Cost
  - Relatively inexpensive compared to appliances
  - Virtual firewalls
  - Host-based firewalls
- Segmentation
  - Between microservices, VMs, or VPCs
- OSI layers
  - Layer 4 (TCP/UDP), Layer 7 (Application)

Security controls
- Cloud-native security controls
  - Integrated and supported by the cloud provider
  - Many configuration options
  - Security is part of the infrastructure
  - No additional costs
- Third-party solutions
  - Support across multiple cloud providers
  - Single pane of glass
  - Extend policies outside the scope of the cloud provider
  - More extensive reporting

3.7 - Identity Controls

Identity provider (IdP)
- Who are you?
  - A service needs to vouch for you
  - Authentication as a Service
- A list of entities
  - Users and devices
- Commonly used by SSO applications or an authentication process
  - Cloud-based services need to know who you are
- Uses standard authentication methods
  - SAML, OAuth, OpenID Connect, etc.

Attributes
- An identifier or property of an entity
  - Provides identification
- Personal attributes
  - Name, email address, phone number, Employee ID
- Other attributes
  - Department name, job title, mail stop
- One or more attributes can be used for identification
  - Combine them for more detail

Certificates
- Digital certificate - Assigned to a person or device
- Binds the identity of the certificate owner to a public and private key
  - Encrypt data, create digital signatures
- Requires an existing public-key infrastructure (PKI)
  - The Certificate Authority (CA) is the trusted entity
  - The CA digitally signs the certificates

Tokens and cards
- Smart card
  - Integrates with devices - may require a PIN
- USB token - Certificate is on the USB device
- Hardware or software tokens
  - Generates pseudo-random authentication codes
- Your phone - SMS a code to your phone

SSH keys
- Secure Shell (SSH) - Secure terminal communication
- Use a key instead of username and password
  - Public/private keys - Critical for automation
- Key management is critical
  - Centralize, control, and audit key use
- SSH key managers - Open source, Commercial

SSH key-based authentication
- Create a public/private key pair
  - `ssh-keygen`
- Copy the public key to the SSH server
  - `ssh-copy-id user@host`
- Try it out
  - `ssh user@host`
  - No password prompt!

3.7 - Account Types

User accounts
- An account on a computer associated with a specific person
  - The computer associates the user with a specific identification number
- Storage and files can be private to that user
  - Even if another person is using the same computer
- No privileged access to the operating system
  - Specifically not allowed on a user account
- This is the account type most people will use
  - Your user community

Shared and generic accounts
- Shared account
  - Used by more than one person
  - Guest login, anonymous login
- Very difficult to create an audit trail
  - No way to know exactly who was working
  - Difficult to determine the proper privileges
- Password management becomes difficult
  - Password changes require notifying everyone
  - Difficult to remember so many password changes
  - Just write it down on this yellow sticky paper
- Best practice: Don't use these accounts

3.7 - Account Types (continued)

Guest accounts
- Access to a computer for guests
  - No access to change settings, modify applications, view other user's files, and more
  - Usually no password
- This brings significant security challenges
  - Access to the userspace is one step closer to an exploit
- Must be controlled
  - Not the default - Removed from Windows 10 build 10159

Service accounts
- Used exclusively by services running on a computer
  - No interactive/user access (ideally)
  - Web server, database server, etc.
- Access can be defined for a specific service
  - Web server rights and permissions will be different than a database server
- Commonly use usernames and passwords
  - You'll need to determine the best policy for password updates

Privileged accounts
- Elevated access to one or more systems
  - Administrator, Root
- Complete access to the system
  - Often used to manage hardware, drivers, and software installation
- This account should not be used for normal administration
  - User accounts should be used
- Needs to be highly secured
  - Strong passwords, 2FA
  - Scheduled password changes

3.7 - Account Policies

Account policies
- Control access to an account
  - It's more than just username and password
  - Determine what policies are best for an organization
- The authentication process
  - Password policies, authentication factor policies, other considerations
- Permissions after login - Another line of defense

Perform routine audits
- Is everything following the policy?
  - You have to police yourself
- It's amazing how quickly things can change
  - Make sure the routine is scheduled
- Certain actions can be automatically identified
  - Consider a tool for log analysis

Auditing
- Permission auditing
  - Does everyone have the correct permissions?
  - Some Administrators don't need to be there
  - Scheduled recertification
- Usage auditing - How are your resources used?
  - Are your systems and applications secure?

Password complexity and length
- Make your password strong - Resist brute-force attack
- Increase password entropy
  - No single words, no obvious passwords
    - What's the name of your dog?
  - Mix upper and lower case and use special characters
    - Don't replace a o with a 0, t with a 7
- Stronger passwords are at least 8 characters
  - Consider a phrase or set of words
- Prevent password reuse
  - System remembers password history, requires unique passwords

Account lockout and disablement
- Too many incorrect passwords will cause a lockout
  - Prevents online brute force attacks
  - This should be normal for most user accounts
  - This can cause big issues for service accounts
    - You might want this
- Disabling accounts
  - Part of the normal change process
  - You don't want to delete accounts
    - At least not initially
    - May contain important decryption keys

Location-based policies
- Network location
  - Identify based on IP subnet
  - Can be difficult with mobile devices
- Geolocation - determine a user's location
  - GPS - mobile devices, very accurate
  - 802.11 wireless, less accurate
  - IP address, not very accurate
- Geofencing
  - Automatically allow or restrict access when the user is in a particular location
  - Don't allow this app to run unless you're near the office
- Geotagging
  - Add location metadata to a document or file
  - Latitude and longitude, distance, time stamps
- Location-based access rules
  - Your IP address is associated with an IP block in Russia
  - We don't have an office in Russia
  - You were in Colorado Springs an hour ago
  - Permission not granted
- Time-based access rules
  - Nobody needs to access the lab at 3 AM

3.8 - Authentication Management

Password keys
- Hardware-based authentication
  - Something you have
- Helps prevent unauthorized logins and account takeovers
  - The key must be present to login
- Doesn't replace other factors
  - Passwords are still important

Password vaults
- Password managers
  - All passwords in one location
  - A database of credentials
- Secure storage
  - All credentials are encrypted
  - Cloud-based synchronization options
- Create unique passwords
  - Passwords are not the same across sites
- Personal and enterprise options
  - Corporate access

Trusted Platform Module (TPM)
- A specification for cryptographic functions
  - Hardware to help with all of this encryption stuff
- Cryptographic processor
  - Random number generator, key generators
- Persistent memory
  - Comes with unique keys burned in during production
- Versatile memory
  - Storage keys, hardware configuration information
- Password protected
  - No dictionary attacks

Hardware Security Module (HSM)
- High-end cryptographic hardware
  - Plug-in card or separate hardware device
- Key backup
  - Secured storage
- Cryptographic accelerators
  - Offload that CPU overhead from other devices
- Used in large environments
  - Clusters, redundant powers

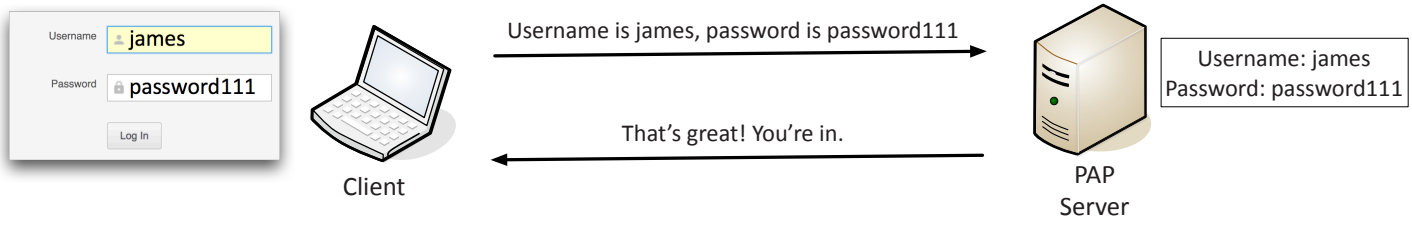
Knowledge-based authentication (KBA)
- Use personal knowledge as an authentication factor
  - Something you know
- Static KBA
  - Pre-configured shared secrets
  - Often used with account recovery
  - What was the make and model of your first car?
- Dynamic KBA
  - Questions are based on an identity verification service
  - What was your street number when you lived in Pembroke Pines, Florida?

3.8 - PAP and CHAP

PAP (Password Authentication Protocol)
- A basic authentication method
  - Used in legacy operating systems
  - Rare to see singularly used
- PAP is in the clear
  - Weak authentication scheme
  - Non-encrypted password exchange
  - We didn't require encryption on analog dialup lines
  - The application would need to provide any encryption

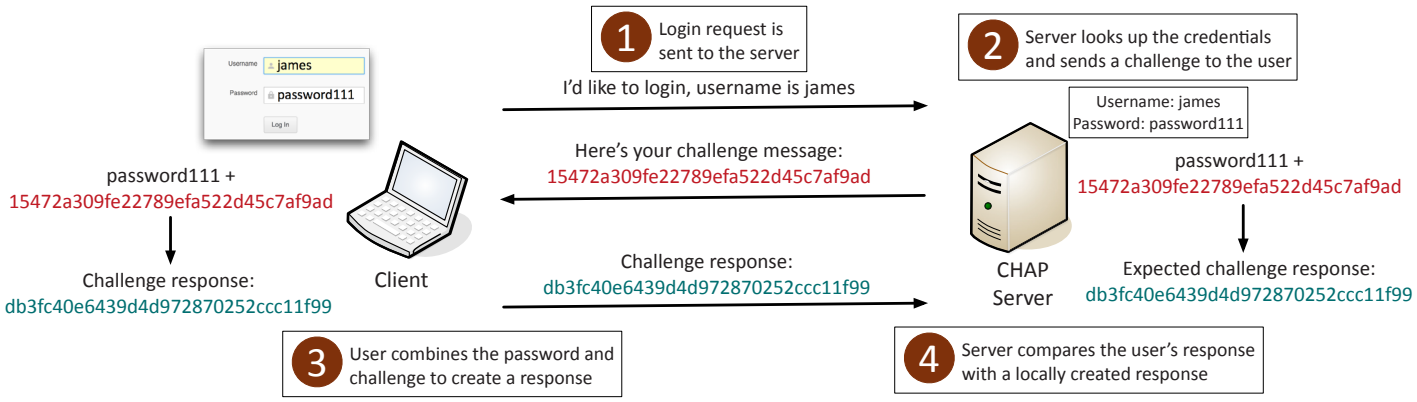
CHAP
- Challenge-Handshake Authentication Protocol
  - Encrypted challenge sent over the network
- Three-way handshake
  - After link is established, server sends a challenge
  - Client responds with a password hash calculated from the challenge and the password
  - Server compares received hash with stored hash
- Challenge-Response continues
  - Occurs periodically during the connection
  - User never knows it happens

PAP (Password Authentication Protocol) - Authentication process



3.8 - PAP and CHAP (continued)

MS-CHAP
- Microsoft's implementation of CHAP
  - Used commonly on Microsoft's
  - Point-to-Point Tunneling Protocol (PPTP)
  - MS-CHAP v2 is the more recent version
- Security issues related to the use of DES
  - Relatively easy to brute force the 256 possible keys to decrypt the NTLM hash
  - Don't use MS-CHAP!
  - Consider L2TP, IPsec, 802.1X or some other secure authentication method



3.8 - Identity and Access Services

RADIUS (Remote Authentication Dial-in User Service)
- One of the more common AAA protocols
  - Supported on a wide variety of platforms and devices
  - Not just for dial-in
- Centralize authentication for users
  - Routers, switches, firewalls, server authentication, remote VPN access, 802.1X network access
- RADIUS services available on almost any server OS

TACACS
- Terminal Access Controller
  - Access-Control System
  - Remote authentication protocol
  - Created to control access to dial-up lines to ARPANET
- XTACACS (Extended TACACS)
  - A Cisco-created (proprietary) version of TACACS
  - Additional support for accounting and auditing
- TACACS+
  - The latest version of TACACS, not backwards compatible
  - More authentication requests and response codes
  - Released as an open standard in 1993

Kerberos
- Network authentication protocol
  - Authenticate once, trusted by the system
  - No need to re-authenticate to everything
  - Mutual authentication - the client and the server
  - Protect against on-path or replay attacks
- Standard since the 1980s
  - Developed by the Massachusetts Institute of Technology (MIT)
- Microsoft starting using Kerberos in Windows 2000
  - Based on Kerberos 5.0 open standard
  - Compatible with other operating systems and devices

SSO with Kerberos
- Authenticate one time
  - Lots of backend ticketing
  - Cryptographic tickets
- No constant username and password input!
  - Save time
- Only works with Kerberos
  - Not everything is Kerberos-friendly
- There are many other SSO methods
  - Smart-cards, SAML, etc.

RADIUS, TACACS+, or Kerberos?
- Three different ways to communicate to an authentication server
  - More than a simple login process
- Often determined by what is at hand
  - VPN concentrator can talk to a RADIUS server
  - We have a RADIUS server
- TACACS+
  - Probably a Cisco device
- Kerberos
  - Probably a Microsoft network

IEEE 802.1X
- IEEE 802.1X
  - Port-based Network Access Control (NAC)
  - You don't get access to the network until you authenticate
- EAP integrates with 802.1X
  - Extensible Authentication Protocol
  - 802.1X prevents access to the network until the authentication succeeds
- Used in conjunction with an access database
  - RADIUS, LDAP, TACACS+

3.8 - Federated Identities

Federation
- Provide network access to others
  - Not just employees - Partners, suppliers, customers, etc.
  - Provides SSO and more
- Third-parties can establish a federated network
  - Authenticate and authorize between the two organizations
  - Login with your Facebook credentials
- The third-parties must establish a trust relationship
  - And the degree of the trust

Security Assertion Markup Language (SAML)
- Open standard for authentication and authorization
  - You can authenticate through a third-party to gain access
  - One standard does it all, sort of
- Not originally designed for mobile apps
  - This has been SAML's largest roadblock

OAuth
- Authorization framework
  - Determines what resources a user will be able to access
- Created by Twitter, Google, and many others
  - Significant industry support
- Not an authentication protocol
  - OpenID Connect handles the single sign-on authentication
  - OAuth provides authorization between applications
- Relatively popular
  - Used by Twitter, Google, Facebook,
  - LinkedIn, and more

3.8 - Access Control

Access control
- Authorization
  - The process of ensuring only authorized rights are exercised
    - Policy enforcement
  - The process of determining rights
    - Policy definition
- Users receive rights based on
  - Access Control models
  - Different business needs or mission requirements

Mandatory Access Control (MAC)
- The operating system limits the operation on an object
  - Based on security clearance levels
- Every object gets a label
  - Confidential, secret, top secret, etc.
- Labeling of objects uses predefined rules
  - The administrator decides who gets access to what security level
  - Users cannot change these settings

Discretionary Access Control (DAC)
- Used in most operating systems
  - A familiar access control model
- You create a spreadsheet
  - As the owner, you control who has access
  - You can modify access at any time
- Very flexible access control
  - And very weak security

Role-based access control (RBAC)
- You have a role in your organization
  - Manager, director, team lead, project manager
- Administrators provide access based on the role of the user
  - Rights are gained implicitly instead of explicitly
- In Windows, use Groups to provide role-based access control
  - You are in shipping and receiving, so you can use the shipping software
  - You are the manager, so you can review shipping logs

Attribute-based access control (ABAC)
- Users can have complex relationships to applications and data
  - Access may be based on many different criteria
- ABAC can consider many parameters
  - A "next generation" authorization model
  - Aware of context
- Combine and evaluate multiple parameters
  - Resource information, IP address, time of day, desired action, relationship to the data, etc.

Rule-based access control
- Generic term for following rules
  - Conditions other than who you are
- Access is determined through system-enforced rules
  - System administrators, not users
- The rule is associated with the object
  - System checks the ACLs for that object
- Rule examples
  - Lab network access is only available between 9 and 5
  - Only Chrome browsers may complete this web form

File system security
- Store files and access them
  - Hard drive, SSDs, flash drives, DVDs, part of most OSs
- Accessing information
  - Access control list
  - Group/user rights and permissions
  - Can be centrally administered and/or users can manage files they own
- The file system handles encryption and decryption

3.8 - Access Control (continued)

Conditional access
- Difficult to apply old methods of authentication to new methods of working
  - Mobile workforce, many different devices, constantly changing cloud
- Conditions
  - Employee or partner, location, type of application accessed, device
- Controls
  - Allow or block, require MFA, provide limited access, require password reset
- Administrators can build complex access rules
  - Complete control over data access

Privileged access management (PAM)
- Managing superuser access
  - Administrator and Root
  - You don't want this in the wrong hands
- Store privileged accounts in a digital vault
  - Access is only granted from the vault by request
  - These privileges are temporary
- PAM advantages
  - Centralized password management
  - Enables automation
  - Manage access for each user
  - Extensive tracking and auditing

3.9 - Public Key Infrastructure

Public Key Infrastructure (PKI)
- Policies, procedures, hardware, software, people
  - Digital certificates: create, distribute, manage, store, revoke
- This is a big, big, endeavor
  - Lots of planning
- Also refers to the binding of public keys to people or devices
  - The certificate authority
  - It's all about trust

The key management lifecycle
- Key generation
  - Create a key with the requested strength using the proper cipher
- Certificate generation
  - Allocate a key to a user
- Distribution
  - Make the key available to the user
- Storage
  - Securely store and protect against unauthorized use
- Revocation
  - Manage keys that have been compromised
- Expiration
  - A certificate may only have a certain "shelf life"

Digital certificates
- A public key certificate
  - Binds a public key with a digital signature
  - And other details about the key holder
- A digital signature adds trust
  - PKI uses Certificate Authority for additional trust
  - Web of Trust adds other users for additional trust
- Certificate creation can be built into the OS
  - Part of Windows Domain services
  - 3rd-party Linux options

Commercial certificate authorities
- Built-in to your browser
  - Any browser
- Purchase your web site certificate
  - It will be trusted by everyone's browser
- Create a key pair, send the public key to the CA to be signed
  - A certificate signing request (CSR)
- May provide different levels of trust and additional features
  - Add a new "tag" to your web site

Private certificate authorities
- You are your own CA
  - Build it in-house
  - Your devices must trust the internal CA
- Needed for medium-to-large organizations
  - Many web servers and privacy requirements
- Implement as part of your overall computing strategy
  - Windows Certificate Services, OpenCA

PKI trust relationships
- Single CA
  - Everyone receives their certificates from one authority
- Hierarchical
  - Single CA issues certs to intermediate CAs
  - Distributes the certificate management load
  - Easier to deal with the revocation of an intermediate CA than the root CA

Registration authority (RA)
- The entity requesting the certificate needs to be verified
  - The RA identifies and authenticates the requester
- Approval or rejection
  - The foundation of trust in this model
- Also responsible for revocations
  - Administratively revoked or by request
- Manages renewals and re-key requests
  - Maintains certificates for current cert holders

3.9 - Public Key Infrastructure (continued)

Important certificate attributes

- Common Name (CN)
  - The FQDN (Fully Qualified
  - Domain Name) for the certificate
- Subject alternative name
  - Additional host names for the cert
  - Common on web servers
  - professormesser.com and www.professormesser.com
- Expiration
  - Limit exposure to compromise
  - 398 day browser limit (13 months)

Key revocation

- Certificate Revocation List (CRL)
  - Maintained by the Certificate Authority (CA)
- Many different reasons
  - Changes all the time
- April 2014 - CVE-2014-0160
  - Heartbleed
  - OpenSSL flaw put the private key of affected web servers at risk
  - OpenSSL was patched, every web server certificate was replaced
  - Older certificates were moved to the CRL

Getting revocation details to the browser

- OCSP (Online Certificate Status Protocol)
  - The browser can check certificate revocation
- Messages usually sent to an OCSP responder via HTTP
  - Easy to support over Internet links
- Not all browsers/apps support OCSP
  - Early Internet Explorer versions did not support OCSP
  - Some support OCSP, but don't bother checking

3.9 - Certificates

Web server SSL certificates

- Domain validation certificate (DV)
  - Owner of the certificate has some control over a DNS domain
- Extended validation certificate (EV)
  - Additional checks have verified the certificate owner's identity
  - Browsers used to show a green name on the address bar
  - Promoting the use of SSL is now outdated
- Subject Alternative Name (SAN)
  - Extension to an X.509 certificate
  - Lists additional identification information
  - Allows a certificate to support many different domains
- Wildcard domain
  - Certificates are based on the name of the server
  - A wildcard domain will apply to all server names in a domain
  - *.professormesser.com

Code signing certificate

- Developers can provide a level of trust
  - Applications can be signed by the developer
- The user's operating system will examine the signature
  - Checks the developer signature
  - Validates that the software has not been modified
- Is it from a trusted entity?
  - The user will have the opportunity to stop the application execution

Root certificate

- The public key certificate that identifies the root CA (Certificate Authority)
  - Everything starts with this certificate
- The root certificate issues other certificates
  - Intermediate CA certificates
  - Any other certificates
- This is a very important certificate
  - Take all security precautions
  - Access to the root certificate allows for the creation of any trusted certificate

Self-signed certificates

- Internal certificates don't need to be signed by a public CA
  - Your company is the only one going to use it
  - No need to purchase trust for devices that already trust you
- Build your own CA
  - Issue your own certificates signed by your own CA
- Install the CA certificate/trusted chain on all devices
  - They'll now trust any certificates signed by your internal CA
  - Works exactly like a certificate you purchased

3.9 - Certificates (continued)

Machine and computer certificates
- You have to manage many devices
  - Often devices that you'll never physically see
- How can you truly authenticate a device?
  - Put a certificate on the device that you signed
- Other business processes rely on the certificate
  - Access to the remote access
  - VPN from authorized devices
  - Management software can validate the end device

Email certificates
- Use cryptography in an email platform
  - You'll need public key cryptography
- Encrypting emails
  - Use a recipient's public key to encrypt
- Receiving encrypted emails
  - Use your private key to decrypt
- Digital signatures
  - Use your private key to digitally sign an email
  - Non-repudiation, integrity

User certificates
- Associate a certificate with a user
  - A powerful electronic "id card"
- Use as an additional authentication factor
  - Limit access without the certificate
- Integrate onto smart cards
  - Use as both a physical and digital access card

3.9 - Certificate Formats

Certificate file formats
- X.509 digital certificates
  - The structure of the certification is standardized
  - The format of the actual certificate file can take many different forms
- There are many certificate file formats
  - You can convert between many of the formats
  - Use openssl or a similar application to view the certificate contents

DER (Distinguished Encoding Rules)
- Format designed to transfer syntax for data structures
  - A very specific encoding format
  - Perfect for an X.509 certificate
- Binary format
  - Not human-readable
- A common format
  - Used across many platforms
  - Often used with Java certificates

PEM (Privacy-Enhanced Mail)
- A very common format
  - BASE64 encoded DER certificate
  - Generally the format provided by CAs
  - Supported on many different platforms
- ASCII format
  - Letters and numbers
  - Easy to email, readable

PKCS #12
- Public Key Cryptography Standards #12
  - Personal Information Exchange Syntax Standard
  - Developed by RSA Security, now an RFC standard
- Container format for many certificates
  - Store many X.509 certificates in a single .p12 or .pfx file
  - Often used to transfer a private and public key pair
  - The container can be password protected
- Extended from Microsoft's .pfx format
  - Personal Information Exchange (PFX)
  - The two standards are very similar
  - Often referenced interchangeably

CER (Certificate)
- Primarily a Windows X.509 file extension
  - Can be encoded as binary DER format or as the ASCII PEM format
- Usually contains a public key
  - Private keys would be transferred in the .pfx file format
- Common format for Windows certificates
  - Look for the .cer extension

PKCS #7
- Public Key Cryptography Standards #7
- Cryptographic Message Syntax Standard
  - Associated with the .p7b file
- Stored in ASCII format
  - Human-readable
- Contains certificates and chain certificates
  - Private keys are not included in a .p7b file
- Wide platform support
  - Microsoft Windows
  - Java Tomcat

3.9 - Certificates (continued)

Email certificates
- Use cryptography in an email platform
  - You'll need public key cryptography
- Encrypting emails
  - Use a recipient's public key to encrypt
- Receiving encrypted emails
  - Use your private key to decrypt
- Digital signatures
  - Use your private key to digitally sign an email
  - Non-repudiation, integrity

User certificates
- Associate a certificate with a user
  - A powerful electronic "id card"
- Use as an additional authentication factor
  - Limit access without the certificate
- Integrate onto smart cards
  - Use as both a physical and digital access card

3.9 - Certificate Concepts

Online and offline CAs
- A compromised certificate authority
  - A very, very bad thing
  - No certificates issued by that CA can be trusted
- Distribute the load
  - Then take the root CA offline and protect it

OCSP stapling
- Online Certificate Status Protocol
  - Provides scalability for OCSP checks
- The CA is responsible for responding to all client OCSP requests
  - This does not scale well
- Instead, have the certificate holder verify their own status
  - Status information is stored on the certificate holder's server
- OCSP status is "stapled" into the SSL/TLS handshake
  - Digitally signed by the CA

Pinning
- You're communicating over TLS/SSL to a server
  - How do you really know it's a legitimate server?
- "Pin" the expected certificate or public key to an application
  - Compiled in the app or added at first run
- If the expected certificate or public key doesn't match, the application can decide what to do
  - Shut down, show a message

PKI trust relationships
- Single CA
  - Everyone receives their certificates from one authority
- Hierarchical
  - Single CA issues certs to intermediate CAs
- Mesh
  - Cross-certifying CAs - Doesn't scale well
- Web-of-trust
  - Alternative to traditional PKI
- Mutual Authentication
  - Server authenticates to the client and the client authenticates to the server

Key escrow
- Someone else holds your decryption keys
  - Your private keys are in the hands of a 3rd-party
- This can be a legitimate business arrangement
  - A business might need access to employee information
  - Government agencies may need to decrypt partner data

It's all about the process
- Need clear process and procedures
  - Keys are incredibly important pieces of information
- You must be able to trust your 3rd-party
  - Access to the keys is at the control of the 3rd-party
- Carefully controlled conditions
  - Legal proceedings and court orders

Certificate chaining
- Chain of trust
  - List all of the certs between the server and the root CA
- The chain starts with the SSL certificate
  - And ends with the Root CA certificate
- Any certificate between the SSL certificate and the root certificate is a chain certificate
  - Or intermediate certificate
- The web server needs to be configured with the proper chain
  - Or the end user may receive an error

4.1 - Reconnaissance Tools

traceroute
- Determine the route a packet takes to a destination
  - Map the entire path
- **tracert** (Windows) or **traceroute** (POSIX)
- Takes advantage of ICMP Time to Live Exceeded error message
  - The time in TTL refers to hops, not seconds or minutes
  - TTL=1 is the first router, TTL=2 is the second router, etc.
- Not all devices will reply with ICMP Time Exceeded messages
  - Some firewalls filter ICMP
  - ICMP is low-priority for many devices

nslookup and dig
- Lookup information from DNS servers
  - Canonical names, IP addresses, cache timers, etc.
- **nslookup**

-Both Windows and POSIX-based
  - Lookup names and IP addresses
  - Deprecated (use dig instead)
- **dig** or **DiG** (Domain Information Groper)
  - More advanced domain information
  - Probably your first choice
  - Install in Windows: https://professormesser.link/digwin

ipconfig and ifconfig
- Most of your troubleshooting starts with your IP address
  - Ping your local router/gateway
- Determine TCP/IP and network adapter information
  - And some additional IP details
- **ipconfig** – Windows TCP/IP configuration
- **ifconfig** – Linux interface configuration

Nmap
- Network mapper
  - Find and learn more about network devices
- Port scan
  - Find devices and identify open ports
- Operating system scan
  - Discover the OS without logging in to a device
- Service scan
  - What service is available on a device? Name, version, details
- Additional scripts
  - Nmap Scripting Engine (NSE)
    - Extend capabilities, vulnerability scans

ping
- Test reachability
  - Determine round-trip time
  - Uses Internet Control Message Protocol (ICMP)
- One of your primary troubleshooting tools
  - Can you ping the host?
- Written by Mike Muuss in 1983
  - The sound made by sonar
  - Not an acronym for Packet INternet Groper
  - A backronym

pathping
- Combine ping and traceroute
  - Included with Windows NT and later
- First phase runs a traceroute
  - Build a map
- Second phase
  - Measure round trip time and packet loss at each hop

hping
- TCP/IP packet assembler/analyzer
  - A ping that can send almost anything
- Ping a device
  - ICMP, TCP, UDP
  - **#hping3 --destport 80 10.1.10.1**
- Send crafted frames
  - Modify all IP, TCP, UDP, and ICMP values
- A powerful tool
  - It's easy to accidentally flood and DoS
  - Be careful!

netstat
- Network statistics
  - Many different operating systems
- **netstat -a**
  - Show all active connections
- **netstat -b**
  - Show binaries
- **netstat -n**
  - Do not resolve names

netcat
- "Read" or "write" to the network
  - Open a port and send or receive some traffic
- Many different functions
  - Listen on a port number
  - Transfer data
  - Scan ports and send data to a port
- Become a backdoor
  - Run a shell from a remote device
- Other alternatives and OSes - Ncat

IP scanners
- Search a network for IP addresses
  - Locate active devices
  - Avoid doing work on an IP address that isn't there
- Many different techniques
  - ARP (if on the local subnet)
  - ICMP requests (ping)
  - TCP ACK
  - ICMP timestamp requests
- A response means more recon can be done
  - Keep gathering information - Nmap, hping, etc.

4.1 - Reconnaissance Tools (continued)

Address Resolution Protocol
- Determine a MAC address based on an IP address
  - You need the hardware address to communicate

`arp -a`
- View local ARP table

`route`
- View the device's routing table
  - Find out which way the packets will go
- Windows: **`route print`**
- Linux and macOS: **`netstat -r`**

`curl`
- Client URL
  - Retrieve data using a URL
  - Uniform Resource Locator
  - Web pages, FTP, emails, databases, etc.
- Grab the raw data
  - Search
  - Parse
  - Automate

`theHarvester`
- Gather OSINT
  - Open-Source Intelligence
- Scrape information from Google or Bing
  - Find associated IP addresses
- List of people from LinkedIn
  - Names and titles
- Find PGP keys by email domain
  - A list of email contacts
- DNS brute force
  - Find those unknown hosts; vpn, chat, mail, partner, etc.

`sn1per`
- Combine many recon tools into a single framework
  - dnsenum, metasploit, nmap, theHarvester, and much more
- Both non-intrusive and very intrusive scanning options
  - You choose the volume
- Another tool that can cause problems
  - Brute force, server scanning, etc
  - Make sure you know what you're doing

`scanless`
- Run port scans from a different host
  - Port scan proxy
- Many different services
  - Choose the option for scan origination
  - Your IP is hidden as the scan source

`dnsenum`
- Enumerate DNS information
  - Find host names
- View host information from DNS servers
  - Many services and hosts are listed in DNS
- Find host names in Google
  - More hosts can probably be found in the index

Nessus
- Industry leader in vulnerability scanning
  - Extensive support
  - Free and commercial options
- Identify known vulnerabilities
  - Find systems before they can be exploited
- Extensive reporting
  - A checklist of issues
  - Filter out the false positives

Cuckoo
- A sandbox for malware
  - Test a file in a safe environment
- A virtualized environment
  - Windows, Linux, macOS, Android
- Track and trace
  - API calls, network traffic, memory analysis
  - Traffic captures
  - Screenshots

4.1 - File Manipulation Tools

`head`
- View the first part of a file
  - The head, or beginning, of the file
  - **`head [OPTION] … [FILE] …`**
- Use -n to specify the number of lines
  - **`head -n 5 syslog`**

`tail`
- View the last part of a file
  - The tail, or end, or the file
  - **`tail [OPTION] … [FILE] …`**
- Use -n to specify the number of lines
  - **`tail -n 5 syslog`**

`cat`
- Concatenate
  - Link together in a series
- Copy a file/files to the screen
  - **`cat file1.txt file2.txt`**
- Copy a file/files to another file
  - **`cat file1.txt file2.txt > both.txt`**

`grep`
- Find text in a file
  - Search through many files at a time
- **`grep PATTERN [FILE]`**
  - **`grep failed auth.log`**

4.1 - File Manipulation Tools (continued)

chmod

- Change mode of a file system object
  - r=read, w=write, x=execute
  - Can also use octal notation
  - Set for the file owner (u), the group(g), others(o), or all(a)
  - **chmod mode FILE**
  - **chmod 744 script.sh**
- **chmod 744 first.txt**
  - User; read, write execute
  - Group; read only
  - Other; read only
- **chmod a-w first.txt**
  - All users, no writing to first.txt
- **chmod u+x script.sh**
  - The owner of script.sh can execute the file

logger

- Add entries to the system log
  - syslog
- Adding to the local syslog file
  - **logger "This information is added to syslog"**
- Useful for including information in a local or remote syslog file
  - Include as part of an automation script
  - Log an important event

4.1 - Shell and Script Environments

SSH (Secure Shell)

- Encrypted console communication - tcp/22
- Looks and acts the same as Telnet

Windows PowerShell

- Command line for system administrators
  - .ps1 file extension
  - Included with Windows 8/8.1 and 10
- Extend command-line functions
  - Uses cmdlets (command-lets)
  - PowerShell scripts and functions
  - Standalone executables
- Automate and integrate
  - System administration
  - Active Domain administration

Python

- General-purpose scripting language
  - .py file extension
- Popular in many technologies
  - Broad appeal and support

OpenSSL

- A toolkit and crypto library for SSL/TLS
  - Build certificates, manage SSL/TLS communication
- Create X.509 certificates
  - Manage certificate signing requests (CSRs) and certificate revocation lists (CRLs)
- Message digests
  - Support for many hashing protocols
- Encryption and Decryption
  - SSL/TLS for services
- Much more

4.1 - Packet Tools

Tcpreplay

- A suite of packet replay utilities
  - Replay and edit packet captures
  - Open source
- Test security devices
  - Check IPS signatures and firewall rules
- Test and tune IP Flow/NetFlow devices
  - Send hundreds of thousands of traffic flows per second
- Evaluate the performance of security devices
  - Test throughput and flows per second

tcpdump

- Capture packets from the command line
  - Display packets on the screen
  - Write packets to a file

Wireshark

- Graphical packet analyzer
  - Get into the details
- Gathers frames on the network
  - Or in the air
- Sometimes built into the device
  - View traffic patterns
  - Identify unknown traffic
  - Verify packet filtering and security controls
- Extensive decodes
  - View the application traffic

4.1 - Forensic Tools

dd

- A reference to the DD command in
  - IBM mainframe JCL (Job Control Language)
  - Data Definition (ASCII to EBCDIC converter)
- Create a bit-by-bit copy of a drive
  - Used by many forensics tools
- Create a disk image
  - `dd if=/dev/sda of=/tmp/sda-image.img`
- Restore from an image
  - `dd if=/tmp/sda-image.img of=/dev/sda`

memdump

- Copy information in system memory to the standard output stream
  - Everything that happens is in memory
  - Many third-party tools can read a memory dump
- Copy to another host across the network
  - Use netcat, stunnel, openssl, etc.

Winhex

- A universal hexadecimal editor for Windows OS
- Edit disks, files, RAM
  - Includes data recovery features
- Disk cloning
  - Drive replication
- Secure wipe
  - Hard drive cleaning
- Much more
  - A full-featured forensics tool

FTK imager

- AccessData forensic drive imaging tool
  - Includes file utilities and read-only image mounting
  - Windows executable
- Widely supported in many forensics tools
  - Third-party analysis
- Support for many different file systems and full disk encryption methods
  - Investigator still needs the password
- Can also import other image formats
  - dd, Ghost, Expert Witness, etc.

Autopsy

- Perform digital forensics of hard drives, smartphones
  - View and recover data from storage devices
- Extract many different data types
  - Downloaded files
  - Browser history and cache
  - Email messages
  - Databases
  - Much more

Exploitation frameworks

- A pre-built toolkit for exploitations
  - Build custom attacks
  - Add more tools as vulnerabilities are found
  - Increasingly powerful utilities
- Metasploit
  - Attack known vulnerabilities
- The Social-Engineer Toolkit (SET)
  - Spear phishing, Infectious media generator

Password crackers

- The keys to the kingdom
  - Find the passwords
- Online cracking
  - Try username/password combinations
- Offline cracking
  - Brute force a hash file
- Limitations
  - Password complexity / strength (entropy)
  - Hashing method and CPU power
  - Graphics processors are useful hardware tools

Data sanitization

- Completely remove data
  - No usable information remains
- Many different use cases
  - Clean a hard drive for future use
  - Permanently delete a single file
- A one-way trip
  - Once it's gone, it's really gone
  - No recovery with forensics tools

4.2 - Incident Response Process

Security incidents

- User clicks an email attachment and executes malware
  - Malware then communicates with external servers
- DDoS
  - Botnet attack
- Confidential information is stolen
  - Thief wants money or it goes public
- User installs peer-to-peer software and allows external access to internal servers

Roles and responsibilities

- Incident response team
  - Specialized group, trained and tested
- IT security management
  - Corporate support
- Compliance officers
  - Intricate knowledge of compliance rules
- Technical staff
  - Your team in the trenches
- User community
  - They see everything

NIST SP800-61
- National Institute of Standards and Technology
  - NIST Special Publication 800-61 Rev. 2
  - Computer Security Incident
  - Handling Guide
- The incident response lifecycle:
  - Preparation
  - Detection and Analysis
  - Containment, Eradication, and Recovery
  - Post-incident Activity

Preparing for an incident
- Communication methods
  - Phones and contact information
- Incident handling hardware and software
  - Laptops, removable media, forensic software, digital cameras, etc.
- Incident analysis resources
  - Documentation, network diagrams, baselines, critical file hash values
- Incident mitigation software
  - Clean OS and application images
- Policies needed for incident handling
  - Everyone knows what to do

The challenge of detection
- Many different detection sources
  - Different levels of detail, different levels of perception
- A large amount of "volume"
  - Attacks are incoming all the time
  - How do you identify the legitimate threats?
- Incidents are almost always complex
  - Extensive knowledge needed

Incident precursors
- An incident might occur in the future
  - This is your heads-up
- Web server log
  - Vulnerability scanner in use
- Exploit announcement
  - Monthly Microsoft patch release,
  - Adobe Flash update
- Direct threats
  - A hacking group doesn't like you

Incident indicators
- An attack is underway
  - Or an exploit is successful
- Buffer overflow attempt
  - Identified by an intrusion detection/prevention system
- Anti-virus software identifies malware
  - Deletes from OS and notifies administrator
- Host-based monitor detects a configuration change
  - Constantly monitors system files
- Network traffic flows deviate from the norm
  - Requires constant monitoring

Isolation and containment
- Generally a bad idea to let things run their course
  - An incident can spread quickly
  - It's your fault at that point
- Sandboxes
  - An isolated operating system
  - Run malware and analyze the results
  - Clean out the sandbox when done
- Isolation can be sometimes be problematic
  - Malware or infections can monitor connectivity
  - When connectivity is lost, everything could be deleted/encrypted/damaged

Recovery after an incident
- Get things back to normal
  - Remove the bad, keep the good
- Eradicate the bug
  - Remove malware
  - Disable breached user accounts
  - Fix vulnerabilities
- Recover the system
  - Restore from backups
  - Rebuild from scratch
  - Replace compromised files
  - Tighten down the perimeter

Reconstitution
- A phased approach
  - It's difficult to fix everything at once
- Recovery may take months
  - Large-scale incidents require a large amount of work
- The plan should be efficient
  - Start with quick, high-value security changes
    - Patches, firewall policy changes
  - Later phases involve much "heavier lifting"
    - Infrastructure changes, large-scale security rollouts

Lessons learned
- Learn and improve
  - No system is perfect
- Post-incident meeting
  - Invite everyone affected by the incident
- Don't wait too long
  - Memories fade over time
  - Some recommendations can be applied to the next event

Answer the tough questions
- What happened, exactly?
  - Timestamp of the events
- How did your incident plans work?
  - Did the process operate successfully?
- What would you do differently next time?
  - Retrospective views provide context
- Which indicators would you watch next time?
  - Different precursors may give you better alerts

4.2 - Incident Response Planning

Exercise
- Test yourselves before an actual event
  - Scheduled update sessions (annual, semi-annual, etc.)
- Use well-defined rules of engagement
  - Do not touch the production systems
- Very specific scenario
  - Limited time to run the event
- Evaluate response
  - Document and discuss

Tabletop exercises
- Performing a full-scale disaster drill can be costly
  - And time consuming
- Many of the logistics can be determined through analysis
  - You don't physically have to go through a disaster or drill
- Get key players together for a tabletop exercise
  - Talk through a simulated disaster

Walkthrough
- Include responders
  - A step beyond a tabletop exercise
  - Many moving parts
- Test processes and procedures before an event
  - Walk through each step
  - Involve all groups
  - Reference actual response materials
- Identifies actual faults or missing steps
  - The walkthrough applies the concepts from the tabletop exercise

Simulation
- Test with a simulated event
  - Phishing attack, password requests, data breaches
- Going phishing
  - Create a phishing email attack
  - Send to your actual user community
  - See who bites
- Test internal security
  - Did the phishing get past the filter?
- Test the users
  - Who clicked?
  - Additional training may be required

Stakeholder management
- Keeping an good ongoing relationship with customers of IT
  - These can be internal or external customers
  - An incident response will require teamwork
  - Without the stakeholder, IT would not exist
- Most of this happens prior to an incident
  - Ongoing communication and meetings
  - Exercises should include the customers
- Continues after the incident
  - Prepare for the next event

Communication plan
- Get your contact list together
  - There are a lot of people in the loop
- Corporate / Organization
  - CIO / Head of Information Security / Internal Response Teams
- Internal non-IT
  - Human resources, public affairs, legal department
- External contacts
  - System owner, law enforcement
  - US-CERT (for U.S. Government agencies)

Disaster recovery plan
- If a disaster happens, IT should be ready
  - Part of business continuity planning
  - Keep the organization up and running
- Disasters are many and varied
  - Natural disasters
  - Technology or system failures
  - Human-created disasters
- A comprehensive plan
  - Recovery location
  - Data recovery method
  - Application restoration
  - IT team and employee availability

Continuity of operations planning (COOP)
- Not everything goes according to plan
  - Disasters can cause a disruption to the norm
- We rely on our computer systems
  - Technology is pervasive
- There needs to be an alternative
  - Manual transactions
  - Paper receipts
  - Phone calls for transaction approvals
- These must be documented and tested before a problem occurs

Incident response team
- Receives, reviews, and responds
  - A predefined group of professionals
- Determine what type of events require a response
  - A virus infection? Ransomware? DDoS?
- May or may not be part of the organizational structure
  - Pulled together on an as-needed basis
- Focuses on incident handling
  - Incident response, incident analysis, incident reporting

Retention policies
- Backup your data
  - How much and where? Copies, versions of copies, lifecycle of data, purging old data
- Regulatory compliance
  - A certain amount of data backup may be required
- Operational needs
  - Accidental deletion, disaster recovery
- Differentiate by type and application
  - Recover the data you need when you need it

4.2 - Attack Frameworks

Attacks and responses

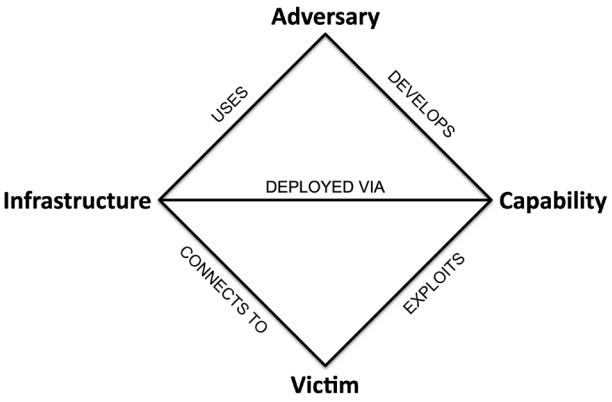
- A constantly moving chessboard
  - The rules are also constantly changing
- Response and intelligence teams need assistance
  - Gather and maintain ongoing reconnaissance
- Understand attacks
  - Many different vectors
- Assess the risk in an organization
  - Determine if a risk exists
  - Use appropriate mitigation

MITRE ATT&CK framework

- The MITRE corporation
  - US not-for-profit based in Massachusetts and Virginia
  - Supports several U.S. government agencies
- The MITRE ATT&CK framework
  - https://attack.mitre.org/
- Determine the actions of an attacker
  - Identify point of intrusion
  - Understand methods used to move around
  - Identify potential security techniques to block future attacks

Diamond Model of Intrusion Analysis

- Designed by the intelligence community
  - https://apps.dtic.mil/docs/citations/ADA586960
  - Guide analysts to help understand intrusions
  - Integrates well with other frameworks
- Apply scientific principles to intrusion analysis
  - Measurement, testability, and repeatability
  - Appears simple, but is remarkably complex
- An adversary deploys a capability over some infrastructure against a victim
  - Use the model to analyze and fill in the details



Cyber Kill Chain

- Seven phases of a cyber attack
  - A military concept

4.3 - Vulnerability Scan Output

Identify vulnerability

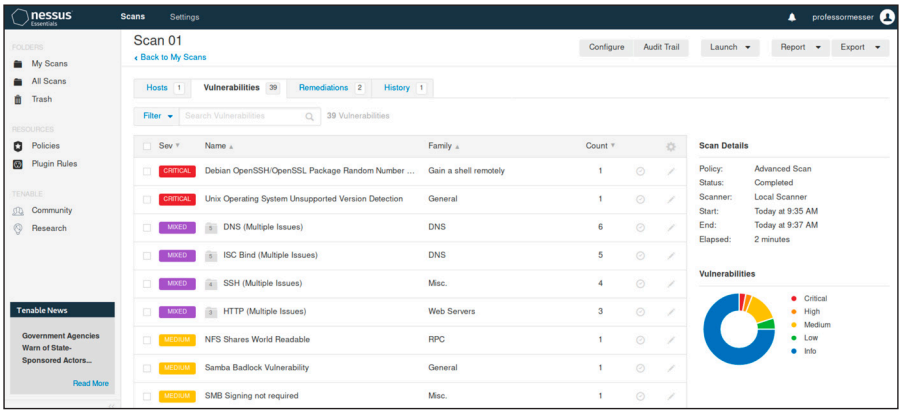
- The scanner looks for everything
  - Well, not _everything_
  - The signatures are the key
- The vulnerabilities can be cross-referenced online
  - Almost all scanners give you a place to go
  - National Vulnerability Database: http://nvd.nist.gov/
  - Microsoft Security Bulletins:
  - https://docs.microsoft.com/en-us/security-updates/
- Some vulnerabilities cannot be definitively identified
  - You'll have to check manually to see if a system is vulnerable
  - But the scanner gives you a heads-up

Vulnerability scan results

- Lack of security controls
  - No firewall
  - No anti-virus
  - No anti-spyware
- Misconfigurations
  - Open shares
  - Guest access
- Real vulnerabilities
  - Especially newer ones
  - Occasionally the old ones

Dealing with false positives

- False positives
  - A vulnerability is identified that doesn't really exist
- This is different than a low-severity vulnerability
  - It's real, but it may not be your highest priority
- False negatives
  - A vulnerability exists, but you didn't detect it
- Update to the latest signatures
  - If you don't know about it, you can't see it
- Work with the vulnerability detection manufacturer
  - They may need to update their signatures for your environment



4.3 - SIEM Dashboards

SIEM
- Security Information and Event Management
  - Logging of security events and information
- Security alerts
  - Real-time information
- Log aggregation and long-term storage
  - Usually includes advanced reporting features
- Data correlation
  - Link diverse data types
- Forensic analysis
  - Gather details after an event

Getting the data
- Sensors and logs
  - Operating systems
  - Infrastructure devices
  - NetFlow sensors
- Sensitivity settings
  - Easy to be overwhelmed with data
  - Some information is unnecessary
  - Informational, Warning, Urgent

Viewing the data
- Trends
  - Identify changes over time
  - Easily view constant attack metrics
- Alerts
  - Identify a security event
  - View raw data
  - Visualize the log information
- Correlation
  - Combine and compare
  - View data in different ways

4.3 - Log files

Network log files
- Switches, routers, access points, VPN concentrators
  - And other infrastructure devices
- Network changes
  - Routing updates
  - Authentication issues
  - Network security issues

System log files
- Operating system information
  - Extensive logs
  - File system information
  - Authentication details
- Can also include security events
  - Monitoring apps
  - Brute force, file changes
- May require filtering
  - Don't forward everything

Application log files
- Specific to the application
  - Information varies widely
- Windows - Event Viewer / Application Log
- Linux / macOS - /var/log
- Parse the log details on the SIEM
  - Filter out unneeded info

Security log files
- Detailed security-related information
  - Blocked and allowed traffic flows
  - Exploit attempts
  - Blocked URL categories
  - DNS sinkhole traffic
- Security devices
  - IPS, firewall, proxy
- Critical security information
  - Documentation of every traffic flow
  - Summary of attack info
  - Correlate with other logs

Web log files
- Web server access
  - IP address, web page URL
- Access errors
  - Unauthorized or non-existent folders/files
- Exploit attempts
  - Attempt to access files containing known vulnerabilities
- Server activity
  - Startup and shutdown notices
  - Restart messages

DNS log files
- View lookup requests
  - And other DNS queries
- IP address of the request
  - The request FQDN or IP
- Identify queries to known bad URLs
  - Malware sites, known command and control domains
- Block or modify known bad requests at the DNS server
  - Log the results
  - Report on malware activity

Authentication log files
- Know who logged in (or didn't)
  - Account names
  - Source IP address
  - Authentication method
  - Success and failure reports
- Identify multiple failures
  - Potential brute force attacks
- Correlate with other events
  - File transfers
  - Authentications to other devices
  - Application installation

4.3 - Log files (continued)

Dump files
- Store all contents of memory into a diagnostic file
  - Developers can use this info
- Easy to create from the
  - Windows Task Manager
  - Right-click, Create dump file
- Some applications have their own dump file process
  - Contact the appropriate support team for additional details

VoIP and Call Manager logs
- View inbound and outbound call info
  - Endpoint details, gateway communication
- Security information
  - Authentications, audit trail
- SIP traffic logs
  - Session Initiation Protocol
  - Call setup, management, and teardown
  - Inbound and outbound calls
  - Alert on unusual numbers or country codes

4.3 - Log Management

Syslog
- Standard for message logging
  - Diverse systems create a consolidated log
- Usually a central logging receiver
  - Integrated into the SIEM (Security Information and Event Manager)
- Each log entry is labeled
  - Facility code (program that created the log) and severity level
- Syslog daemon options
  - Rsyslog -"Rocket-fast System for log processing"
  - syslog-ng - A popular syslog daemon with additional filtering and storage options
  - NXLog - Collection from many diverse log types

Journalctl
- Linux has a lot of logs
  - The OS, daemons, applications, etc.
- System logs are stored in a binary format
  - Optimized for storage and queries
  - Can't read them with a text editor
- Journalctl provides a method for querying the system journal
  - Search and filter
  - View as plain text

Bandwidth monitors
- The fundamental network statistic
  - Percentage of network use over time
- Many different ways to gather this metric
  - SNMP, NetFlow, sFlow, IPFIX protocol analysis, software agent
- Identify fundamental issues
  - Nothing works properly if bandwidth is highly utilized

Metadata
- Metadata
  - Data that describes other data sources
- Email
  - Header details, sending servers, destination address
- Mobile - Type of phone, GPS location,
- Web - Operating system, browser type, IP address
- Files - Name, address, phone number, title

NetFlow
- Gather traffic statistics from all traffic flows
  - Shared communication between devices
- NetFlow
  - Standard collection method
  - Many products and options
- Probe and collector
  - Probe watches network communication
  - Summary records are sent to the collector
- Usually a separate reporting app
  - Closely tied to the collector

IPFIX
- IP Flow Information Export
  - A newer, NetFlow-based standard
  - Evolved from NetFlow v9
- Flexible data support
  - Templates are used to describe the data

sFlow
- sFlow (Sampled Flow)
  - Only a portion of the actual network traffic
  - So, technically not a flow
- Usually embedded in the infrastructure
  - Switches, routers
  - Sampling usually occurs in hardware/ASICs
- Relatively accurate statistics
  - Useful information regarding video streaming and high-traffic applications

Protocol analyzer output
- Solve complex application issues
  - Get into the details
- Gathers packets on the network
  - Or in the air
  - Sometimes built into the device
- View detailed traffic information
  - Identify unknown traffic
  - Verify packet filtering and security controls
  - View a plain-language description of the application data

4.4 - Endpoint Security Configuration

The endpoint
- The end user device
  - Desktop PC, laptop, tablet, phone, etc.
- Many ways to exploit a system
  - OS vulnerability, malware, user intervention
- Security team has to cover all of the bases
  - Recognize and react to any malicious activity

Application approved/deny lists
- Any application can be dangerous
  - Vulnerabilities, trojan horses, malware
  - Security policy can control app execution
- Approved list
  - Nothing runs unless it's approved
  - Very restrictive
- Blocklist / deny list
  - Nothing on the "bad list" can be executed
  - Anti-virus, anti-malware
- Quarantine
  - Anything suspicious can be moved to a safe area

Examples of application approval lists
- Decisions are made in the operating system
  - Often built-in to the operating system management
  - Application hash
- Only allows applications with this unique identifier
- Certificate
  - Allow digitally signed apps from certain publishers
- Path
  - Only run applications in these folders
- Network zone
  - The apps can only run from this network zone

4.4 - Security Configurations

Configuration changes
- Firewall rules
  - Manage application flows
  - Block dangerous applications
- Mobile Device Manager (MDM)
  - Enable or disable phone and tablet functionality
  - Regardless of physical location
- Data Loss Prevention (DLP)
  - Block transfer of personally identifiable information (PII) or sensitive data
  - Credit card numbers, social security numbers, etc.
- Content filter/URL filter
  - Limit access to untrusted websites
  - Block known malicious sites
  - Large blocklists are used to share suspicious site URLs
- Updating or revoking certificates
  - Manage device certificates to verify trust
  - Revoking a certificate effectively removes access

Isolation
- Administratively isolate a compromised device from everything else
  - Prevent the spread of malicious software
  - Prevent remote access or C2 (Command and Control)
- Network isolation
  - Isolate to a remediation VLAN
  - No communication to other devices
- Process isolation
  - Limit application execution
  - Prevent malicious activity but allow device management

Containment
- Application containment
  - Run each application in its own sandbox
  - Limit interaction with the host operating system and other applications
  - Ransomware would have no method of infection
- Contain the spread of a multi-device security event, i.e., ransomware
  - Disable administrative shares
  - Disable remote management
  - Disable local account access and change local administrator password

Segmentation
- Separate the network
  - Prevent unauthorized movement
  - Limit the scope of a breach

SOAR
- Security Orchestration, Automation, and Response
  - Integrate third-party tools and data sources
  - Make security teams more effective
- Runbooks
  - Linear checklist of steps to perform
  - Step-by-step approach to automation
  - Reset a password, create a website certificate, back up application data
- Playbooks
  - Conditional steps to follow; a broad process
  - Investigate a data breach, recover from ransomware

4.5 - Digital Forensics

Digital forensics
- Collect and protect information relating to an intrusion
  - Many different data sources and protection mechanisms
- RFC 3227 - Guidelines for
  - Evidence Collection and Archiving
  - A good set of best practices
- Standard digital forensic process
  - Acquisition, analysis, and reporting
- Must be detail oriented
  - Take extensive notes

Legal hold
- A legal technique to preserve relevant information
  - Prepare for impending litigation
  - Initiated by legal counsel
- Hold notification
  - Records custodians are instructed to preserve data
- Separate repository for electronically stored information (ESI)
  - Many different data sources and types
  - Unique workflow and retention requirements
- Ongoing preservation
  - Once notified, there's an ongoing obligation to preserve data

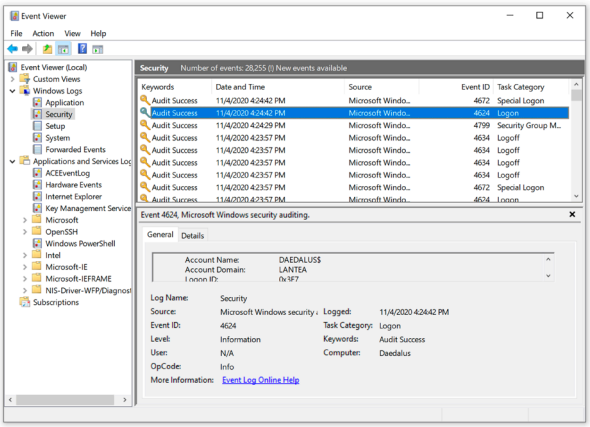
Capture video
- A moving record of the event
  - Gathers information external to the computer and network
- Captures the status of the screen and other volatile information
  - Today's mobile video devices are remarkable
- Don't forget security cameras and your phone
- The video content must also be archived
  - May have some of the most important record of information

Admissibility
- Not all data can be used in a court of law
  - Different rules in different jurisdictions
- Legal authorization
  - Search and seizure of information
- Procedures and tools
  - The correct tools used the correct way
- Laboratories
  - Proper scientific principles used to analyze the evidence
- Technical and academic qualifications
  - Competence and qualifications of experts

Chain of custody
- Control evidence
  - Maintain integrity
- Everyone who contacts the evidence
  - Use hashes
  - Avoid tampering
- Label and catalog everything
  - Digitally tag all items for ongoing documentation
  - Seal and store

Recording time offsets
- The time zone determines how the time is displayed
  - Document the local device settings
- Different file systems store timestamps differently
  - FAT: Time is stored in local time
  - NTFS: Time is stored in GMT
- Record the time offset from the operating system
  - The Windows Registry
  - Many different values (daylight saving time, time change information, etc.)

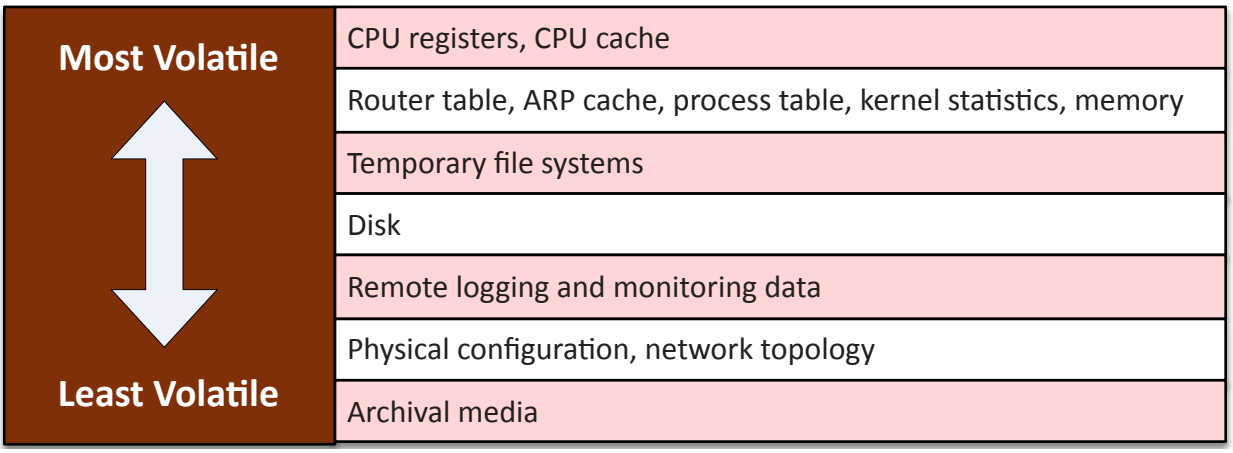
Event logs
- System logs
  - Documents important operating system and application events
- Export and store for future reference
  - Filter and parse
- Log store
  - Linux: /var/log
  - Windows: Event Viewer



Interviews
- Who might have seen this?
  - You won't know until you ask
- Interview and document
  - These folks might not be around later
- Not all witness statements are 100% accurate
  - Humans are fallible

Reports
- Document the findings
  - For Internal use, legal proceedings, etc.
- Summary information
  - Overview of the security event
- Detailed explanation of data acquisition
  - Step-by-step method of the process
- The findings
  - An analysis of the data
- Conclusion
  - Professional results, given the analysis

4.5 - Forensics Data Acquisition



Order of volatility
- How long does data stick around?
  - Some media is much more volatile than others
  - Gather data in order from the most volatile to less volatile

Disk
- Copy everything on a storage drive
  - Hard drive, SSD, flash drive
- Drive image preparation
  - Power down to prevent changes
  - Remove storage drive
- Connect to imaging device
  - With write-protection
- Forensic clone
  - Bit-for-bit copy
  - Preserve all data (even the "deleted" data)

Random access memory (RAM)
- A difficult target to capture
  - Changes constantly
  - Capturing data changes the data
- Memory dump
  - Grab everything in active RAM
  - Many third-party tools
- Important data
  - Browsing history
  - Clipboard information
  - Encryption keys
  - Command history

Swap/pagefile
- Used by different operating systems
  - Slightly different usage in each
- A place to store RAM when memory is depleted
  - There's a lot more space on the storage drive
  - Transfer pages of RAM to a storage drive
- Can also contain portions of an application
  - Page out portions that aren't in use
- Contains data similar to a RAM dump
  - Anything active on the system

Operating system
- OS files and data
  - May have been modified
- Core operating system
  - Executable files and libraries
  - Can be compared later to known-good files
  - Usually captured with a drive image
- Other OS data
  - Logged in users
  - Open ports
  - Processes currently running
  - Attached device list

Device
- Mobile devices and tablets
  - A more challenging forensics task
- Capture data
  - Use an existing backup file
  - Transfer image over USB
- Data
  - Phone calls
  - Contact information
  - Text messages
  - Email data
  - Images and movies

Firmware
- Extract the device firmware
  - Rootkits and exploited hardware device
  - A reprogrammed firmware or ROM
- Specific to the platform
  - Firmware implementations vary widely
- Attacker gains access to the device
  - Maintains access through OS updates
- Data discovery
  - Exploit data
  - Firmware functionality
  - Real-time data

4.5 - Forensics Data Acquisition (continued)

Snapshot
- Generally associated with virtual machines (VMs)
  - A point-in-time system image
- Incremental between snapshots
  - Original image is the full backup
  - Each snapshot is incremented from the last
  - Restoring requires the original and all snapshots
- Contains all files and information about a VM
  - Similar to a system image
  - Operating system, applications, user data, etc.

Cache
- Store data for use later
  - Often used to increase performance
  - Many different caches (CPU, disk, Internet, etc.)
- Can contain specialized data
  - CPU cache is very short-term instruction storage
- Some data may never be used
  - Erased after a specified timeframe or when the cache is full
  - Browser caches are often long-lived
- Data
  - URL locations
  - Browser page components (text, images)

Network
- Gather information about and from the network
  - Network connections, packet captures
- Inbound and outbound sessions
  - OS and application traffic
- Packet data
  - Capture raw network data
  - May include long-term packet captures
- Third-party packet captures
  - Firewalls, IPS, etc.

Artifacts
- Digital items left behind
  - Every contact leaves a trace
  - May not be obvious to access
- Artifact locations
  - Log information
  - Flash memory
  - Prefetch cache files
  - Recycle Bin
  - Browser bookmarks and logins

4.5 - On-Premises vs. Cloud Forensics

Forensics in the cloud
- Adding complexity to the digital forensics process
  - Cloud technologies
- Technical challenges
  - Devices are not totally in your control
  - There may be limited access
  - Associate data with a specific user
- Legal issues
  - Laws are different around the world
  - The rules may not be immediately obvious

Right to audit clauses
- Common to work with business partners
  - Data sharing
  - Outsourcing
- Cloud computing providers
  - Can hold all of the data
  - Manage Internet access
  - Are they secure?
- Right-to-audit should be in the contract
  - A legal agreement to have the option to perform a security audit at any time
  - Everyone agrees to the terms and conditions
  - Ability to verify security before a breach occurs

Regulatory/jurisdiction
- Cloud computing technology appeared relatively quickly
  - The legal world is scrambling to catch up
- Forensics professionals must know their legal rights
  - Data in a different jurisdiction may be bound by very different regulations
- Data stored in cloud may not be located in the same country
  - Location of the data center may determine how data can be treated
- Location of the data is critical
  - Legal frameworks vary widely between countries
  - Some countries don't allow electronic searches outside of their borders

Data breach notification laws
- Notification laws
  - If consumer data is breached, the consumer must be informed
- Many data breach notification laws
  - Vary widely across countries and localities
  - If you're in the cloud, you're a global entity
- Notification requirements also vary
  - Type of data breached
  - Who gets notified
  - How quickly

4.5 - Managing Evidence

Integrity
- Hashing
  - Cryptographic integrity verification
  - A digital "fingerprint"
- Checksums
  - Protects against accidental changes during transmission
  - A relatively simple integrity check
  - Not designed to replace a hash
- Provenance
  - Documentation of authenticity
  - A chain of custody for data handling
  - Blockchain technology

Preservation
- Handling evidence
  - Isolate and protect the data
  - Analyze the data later without any alterations
- Manage the collection process
  - Work from copies
  - Manage the data collection from mobile devices
- Live collection has become an important skill
  - Data may be encrypted or difficult to collect after powering down
- Follow best practices to ensure admissibility of data in court
  - What happens now affects the future

E-discovery
- Electronic discovery
  - Collect, prepare, review, interpret, and produce electronic documents
- E-discovery gathers data required by the legal process
  - Does not generally involve analysis
  - There's no consideration of intent
- Works together with digital forensics
  - The e-discovery process obtains a storage drive
  - Data on the drive is smaller than expected
  - Forensics experts determine that data was deleted and attempt to recover the data

Data recovery
- Extract missing data without affecting the integrity of the data
  - Requires training and expertise
- The recovery process can vary
  - Deleted files
  - Hidden data
  - Hardware or software corruption
  - Storage device is physically damaged

Non-repudiation
- Proof of data integrity and the origin of the data
  - The data is unchanged and really did come from the sender
  - Hashing the data
- Authentication that is genuine with high confidence
  - The only person who could have sent the data is the sender
- Message Authentication Code (MAC)
  - The two parties can verify non-repudiation
- Digital Signature
  - The non-repudiation can be publicly verified

Strategic intelligence/counterintelligence
- Strategic intelligence
  - A focus on key threat activity for a domain
  - Business sectors, geographical regions, countries
  - Gather information from internal threat reports, third-party data sources, and other data inputs
  - Determine the threat landscape based on the trends
- Strategic counterintelligence (CI)
  - Prevent hostile intelligence operations
  - Discover and disrupt foreign intelligence threats
  - Gather threat information on foreign intelligence operations

5.1 - Security Controls

Security controls
- Security risks are out there
  - Many different types to consider
- Assets are also varied
  - Data, physical property, computer systems
- Prevent security events, minimize the impact, and limit the damage
  - Security controls

Control categories
- Managerial controls
  - Controls that address security design and implementation
  - Security policies, standard operating procedures
- Operational controls
  - Controls that are implemented by people
  - Security guards, awareness programs
- Technical controls
  - Controls implemented using systems
  - Operating system controls
  - Firewalls, anti-virus

Control types
- Preventive
  - Physically control access
  - Door lock
  - Security guard
  - Firewall
- Detective
  - May not prevent access
  - Identifies and records any intrusion attempt
  - Motion detector, IDS/IPS

5.1 - Security Controls (continued)

- Corrective
  - Designed to mitigate damage
  - IPS can block an attacker
  - Backups can mitigate a ransomware infection
  - A backup site can provide options when a storm hits
- Deterrent
  - May not directly prevent access
  - Discourages an intrusion attempt
  - Warning signs, login banner
- Compensating
  - Doesn't prevent an attack
  - Restores using other means
  - Re-image or restore from backup
  - Hot site
  - Backup power system
- Physical
  - Fences, locks, mantraps
  - Real-world security

5.2 - Security Regulations and Standards

Compliance

- Compliance
  - Meeting the standards of laws, policies, and regulations
- A healthy catalog of regulations and laws
  - Across many aspects of business and life
  - Many are industry-specific or situational
- Penalties
  - Fines, incarceration, loss of employment
- Scope
  - Covers national, territory, or state laws
  - Domestic and international requirements

GDPR - General Data Protection Regulation

- European Union regulation
  - Data protection and privacy for individuals in the EU
  - Name, address, photo, email address, bank details, posts on social networking websites, medical information, a computer's IP address, etc.
- Controls export of personal data
  - Users can decide where their data goes
- Gives individuals control of their personal data
  - A right to be forgotten
- Site privacy policy
  - Details all of the privacy rights for a user

PCI DSS

- Payment Card Industry
  - Data Security Standard (PCI DSS)
  - A standard for protecting credit cards
- Six control objectives
  - Build and maintain a secure network and systems
  - Protect cardholder data
  - Maintain a vulnerability management program
  - Implement strong access control measures
  - Regularly monitor and test networks
  - Maintain an information security policy

5.2 - Security Frameworks

Security frameworks

- Secure your data.
  - Where do you start? What are the best practices?
  - If only there was a book.
- Often a complex problem
  - Unique organizational requirements
  - Compliance and regulatory requirements
  - Many different processes and tools are available
- Use a security framework
  - Documented processes
  - A guide for creating a security program
  - Define tasks and prioritize projects

Center for Internet Security (CIS)

- Center for Internet Security
  - Critical Security Controls for
  - Effective Cyber Defense
  - CIS CSC
- Improve cyber defenses
  - Twenty key actions (the critical security controls)
  - Categorized for different organization sizes
- Designed for implementation - Written for IT professionals
  - Includes practical and actionable tasks

NIST RMF

- National Institute of Standards and Technology
  - Risk Management Framework (RMF)
  - Mandatory for US federal agencies and organizations that handle federal data
- Six step process
  - Step 1: Categorize - Define the environment
  - Step 2: Select - Pick appropriate controls
  - Step 3: Implement - Define proper implementation
  - Step 4: Assess - Determine if controls are working
  - Step 5: Authorize - Make a decision to authorize a system
  - Step 6: Monitor - Check for ongoing compliance

NIST CSF

- National Institute of Standards and Technology
  - Cybersecurity Framework (CSF)
  - A voluntary commercial framework
- Framework Core
  - Identify, Protect, Detect, Respond, and Recover
- Framework Implementation Tiers
  - An organization's view of cybersecurity risk and processes to manage the risk
- Framework Profile - The alignment of standards, guidelines, and practices to the Framework Core

5.2 - Security Frameworks (continued)

ISO/IEC frameworks
- International Organization for Standardization / International Electrotechnical Commission
- ISO/IEC 27001
  - Standard for an Information Security Management System (ISMS)
- ISO/IEC 27002
  - Code of practice for information security controls
- ISO/IEC 27701
  - Privacy Information Management Systems (PIMS)
- ISO 31000
  - International standards for risk management practices

SSAE SOC 2 Type I/II
- The American Institute of Certified Public Accountants (AICPA) auditing standard Statement on Standards for Attestation Engagements number 18 (SSAE 18)
- SOC 2 - Trust Services Criteria (security controls)
  - Firewalls, intrusion detection, and multi-factor authentication
- Type I audit
  - Tests controls in place at a particular point in time
- Type II
  - Tests controls over a period of at least six consecutive months

Cloud Security Alliance (CSA)
- Security in cloud computing
  - Not-for-profit organization
- Cloud Controls Matrix (CCM)
  - Cloud-specific security controls
  - Controls are mapped to standards, best practices, and regulations
- Enterprise Architecture
  - Methodology and tools
  - Assess internal IT groups and cloud providers
  - Determine security capabilities
  - Build a roadmap

5.2 - Secure Configurations

Secure configurations
- No system is secure with the default configurations
  - You need some guidelines to keep everything safe
- Hardening guides are specific to the software or platform
  - Get feedback from the manufacturer or Internet interest group
  - They'll have the best details
- Other general-purpose guides are available online

Web server hardening
- Access a server with your browser
  - The fundamental server on the Internet
  - Microsoft Internet Information Server, Apache HTTP Server, et al.
- Huge potential for access issues
  - Data leaks, server access
- Secure configuration
  - Information leakage: Banner information, directory browsing
  - Permissions: Run from a non-privileged account, configure file permissions
  - Configure SSL: Manage and install certificates
  - Log files: Monitor access and error logs

Operating system hardening
- Many and varied - Windows, Linux, iOS, Android, et al.
- Updates
  - Operating system updates/service packs, security patches
- User accounts
  - Minimum password lengths and complexity
  - Account limitations
- Network access and security
  - Limit network access
- Monitor and secure
  - Anti-virus, anti-malware

Application server
- Programming languages, runtime libraries, etc.
  - Usually between the web server and the database
  - Middleware
- Very specific functionality
  - Disable all unnecessary services
- Operating system updates
  - Security patches
- File permissions and access controls
  - Limit rights to what's required
  - Limit access from other devices

Network infrastructure devices
- Switches, routers, firewalls, IPS, etc.
  - You never see them, but they're always there
- Purpose-built devices
  - Embedded OS, limited OS access
- Configure authentication
  - Don't use the defaults
- Check with the manufacturer
  - Security updates
  - Not usually updated frequently
  - Updates are usually important

5.3 - Personnel Security

Acceptable use policies (AUP)
- What is acceptable use of company assets?
  - Detailed documentation
  - May be documented in the Rules of Behavior
- Covers many topics
  - Internet use, telephones, computers, mobile devices, etc.
- Used by an organization to limit legal liability
  - If someone is dismissed, these are the well-documented reasons why

Business policies
- Job rotation
  - Keep people moving between responsibilities
  - No one person maintains control for long periods of time
- Mandatory vacations
  - Rotate others through the job
  - The longer the vacation, the better chance to identify fraud
  - Especially important in high-security environments
- Separation of duties
  - Split knowledge
    - No one person has all of the details
    - Half of a safe combination
  - Dual control
    - Two people must be present to perform the business function
    - Two keys open a safe (or launch a missile)
- Clean desk policy
  - When you leave, nothing is on your desk
  - Limit the exposure of sensitive data to third-parties

Least privilege
- Rights and permissions should be set to the bare minimum
  - You only get exactly what's needed to complete your objective
- All user accounts must be limited
  - Applications should run with minimal privileges
- Don't allow users to run with administrative privileges
  - Limits the scope of malicious behavior

Background checks
- Background checks
  - Pre-employment screening
  - Verify the applicant's claims
  - Discover criminal history, workers compensation claims, etc.
  - Legalities vary by country
- Adverse actions
  - An action that denies employment based on the background check
  - May require extensive documentation
  - Can also include existing employees

Personnel security procedures
- NDA (Non-disclosure agreement)
  - Confidentiality agreement / Legal contract
  - Prevents the use and dissemination of confidential information
- Social media analysis
  - Gather data from social media
  - Facebook, Twitter, LinkedIn, Instagram
  - Build a personal profile
  - Another data point when making a hiring decision

On-boarding
- Bring a new person into the organization
  - New hires or transfers
- IT agreements need to be signed
  - May be part of the employee handbook or a separate AUP
- Create accounts
  - Associate the user with the proper groups and departments
- Provide required IT hardware
  - Laptops, tablets, etc. - Preconfigured and ready to go

Off-boarding
- All good things… (But you knew this day would come)
- This process should be pre-planned
  - You don't want to decide how to do things at this point
- What happens to the hardware and the data?
- Account information is usually deactivated
  - But not always deleted

User training
- Gamification
  - Score points, compete with others, collect badges
- Capture the flag (CTF)
  - Security competition
  - Hack into a server to steal data (the flag)
  - Can involve highly technical simulations
  - A practical learning environment
- Phishing simulation
  - Send simulated phishing emails
  - Make vishing calls
  - See which users are susceptible to phishing attacks without being a victim of phishing
- Computer-based training (CBT)
  - Automated pre-built training
  - May include video, audio, and Q&A
  - Users all receive the same training experience

Role-based security awareness training
- Before providing access, train your users
  - Detailed security requirements
- Specialized training
  - Each user role has unique security responsibilities
- Also applies to third-parties
  - Contractors, partners, suppliers
- Detailed documentation and records
  - Problems later can be severe for everyone

5.3 - Third-party Risk Management

Vendors
- Every organization works with vendors
  - Payroll, customer relationship management, email marketing, travel, raw materials
- Important company data is often shared
  - May be required for cloud-based services
- Perform a risk assessment
  - Categorize risk by vendor and manage the risk
- Use contracts for clear understanding
  - Make sure everyone understands the expectations
  - Use the contract to enforce a secure environment

Target credit card breach - November 2013
- Every point of sale terminal infected
  - A third-party was allowed in through lapses in security policy
- A vendor was infected through an email attachment
  - The vendor didn't have or follow a security policy for their workstations
- Target didn't segment the vendor network from the corporate
  - The attackers jumped from the vendor to the Target network
- The corporate network was not segmented from point of sale (POS) terminals
  - Once on the inside, it was relatively easy to get to your credit card numbers
  - (110 million card numbers)

Supply chain
- The system involved when creating a product
  - Involves organizations, people, activities, and resources
- Supply chain assessment
  - Get a product or service from supplier to customer
  - Evaluate coordination between groups
  - Identify areas of improvement
  - Assess the IT systems supporting the operation
  - Document the business process changes
- New laptops arrive with bundled malware
  - Lenovo, August 2014 through early 2015
  - Superfish software added a self-signed root cert (!)
  - Allowed for on-path attacks when browsing any site, including over HTTPS

Business partners
- Much closer to your data than a vendor
  - May require direct access
  - May be a larger security concern than an outside hacker
- Often involves communication over a trusted connection
  - More difficult to identify malicious activity
- Partner risk management should be included
  - Requirements for best practices, data handling, intellectual property
- Include additional security between partners
  - Firewalls and traffic filters

Common agreements
- Service Level Agreement (SLA)
  - Minimum terms for services provided
  - Uptime, response time agreement, etc.
  - Commonly used between customers and service providers
- Memorandum of Understanding (MOU)
  - Both sides agree on the contents of the memorandum
  - Usually includes statements of confidentiality
  - Informal letter of intent; not a signed contract
- Measurement system analysis (MSA)
  - Don't make decisions based on incorrect data!
  - Used with quality management systems, i.e., Six Sigma
  - Assess the measurement process
  - Calculate measurement uncertainty
- Business Partnership Agreement (BPA)
  - Going into business together
  - Owner stake
  - Financial contract
  - Decision-making agreements
  - Prepare for contingencies

Product support lifetime
- End of life (EOL)
  - Manufacturer stops selling a product
  - May continue supporting the product
  - Important for security patches and updates
- End of service life (EOSL)
  - Manufacturer stops selling a product
  - Support is no longer available for the product
  - No ongoing security patches or updates
  - May have a premium-cost support option
- Technology EOSL is a significant concern
  - Security patches are part of normal operation

Non-disclosure agreement (NDA)
- Confidentiality agreement between parties
  - Information in the agreement should not be disclosed
- Protects confidential information
  - Trade secrets
  - Business activities
  - Anything else listed in the NDA
- Unilateral or bilateral (or multilateral)
  - On-way NDA or mutual NDA
- Formal contract
  - Signatures are usually required

5.3 - Managing Data

Data governance

- Rules, processes, and accountability associated with an organization's data
  - Data is used in the right ways
- Data steward
  - Manages the governance processes
  - Responsible for data accuracy, privacy, and security
  - Associates sensitivity labels to the data
  - Ensures compliance with any applicable laws and standards
- Formal rules for data
  - Everyone must know and follow the processes

Data classification

- Identify data types
  - Personal, public, restricted, etc.
  - Use and protect data efficiently
- Associate governance controls to the classification levels
  - How the data class should be managed
- Data compliance
  - Laws and regulations regarding certain types of data
  - GDPR - General Data Protection Regulation

Data retention

- Keep files that change frequently for version control
  - Files change often
  - Keep at least a week, perhaps more
- Recover from virus infection
  - Infection may not be identified immediately
  - May need to retain 30 days of backups
- Often legal requirements for data retention
  - Email storage may be required over years
  - Some industries must legally store certain data types
  - Different data types have different storage requirements
  - Corporate tax information, customer PII, tape backups, etc.

5.3 - Credential Policies

Credential management

- All that stands between the outside world and all of the data
  - The data is everything
- Passwords must not be embedded in the application
  - Everything needs to reside on the server, not the client
- Communication across the network should be encrypted
  - Authentication traffic should be impossible to see

Personnel accounts

- An account on a computer associated with a specific person
  - The computer associates the user with a specific identification number
- Storage and files can be private to that user
  - Even if another person is using the same computer
- No privileged access to the operating system
  - Specifically not allowed on a user account
- This is the account type most people will use
  - Your user community

Third-party accounts

- Access to external third-party systems
  - Cloud platforms for payroll, enterprise resource planning, etc.
- Third-party access to corporate systems
  - Access can come from anywhere
- Add additional layers of security
  - 2FA (two factor authentication)
  - Audit the security posture of third-parties
- Don't allow account sharing
  - All users should have their own account

Device accounts

- Access to devices
  - Mobile devices
- Local security
  - Device certificate
  - Require screen locks and unlocking standards
  - Manage through a Mobile Device Manager (MDM)
- Add additional security
  - Geography-based
  - Include additional authentication factors
  - Associate a device with a user

Service accounts

- Used exclusively by services running on a computer
  - No interactive/user access (ideally)
  - Web server, database server, etc.
- Access can be defined for a specific service
  - Web server rights and permissions will be different than a database server
- Commonly use usernames and passwords
  - You'll need to determine the best policy for password updates

Administrator/root accounts

- Elevated access to one or more systems
  - Super user access
- Complete access to the system
  - Often used to manage hardware, drivers, and software installation
- This account should not be used for normal administration
  - User accounts should be used
- Needs to be highly secured
  - Strong passwords, 2FA
  - Scheduled password changes

5.3 - Organizational Policies

Change management
- How to make a change
  - Upgrade software, change firewall configuration, modify switch ports
- One of the most common risks in the enterprise
  - Occurs very frequently
- Often overlooked or ignored
  - Did you feel that bite?
- Have clear policies
  - Frequency, duration, installation process, fallback procedures
- Sometimes extremely difficult to implement
  - It's hard to change corporate culture

Change control
- A formal process for managing change
  - Avoid downtime, confusion, and mistakes
- Nothing changes without the process
  - Determine the scope of the change
  - Analyze the risk associated with the change
  - Create a plan
  - Get end-user approval
  - Present the proposal to the change control board
  - Have a backout plan if the change doesn't work
  - Document the changes

Asset management
- Identify and track computing assets
  - Usually an automated process
- Respond faster to security problem
  - You know who, what, and where
- Keep an eye on the most valuable assets
  - Both hardware and data
- Track licenses
  - You know exactly how many you'll need
- Verify that all devices are up to date
  - Security patches, anti-malware signature updates, etc.

5.4 - Risk Management Types

Risk assessment
- Identify assets that could be affected by an attack
  - Define the risk associated with each asset
  - Hardware, customer data, intellectual property
- Identify threats
  - Loss of data, disruption of services, etc.
- Determine the risk - High, medium, or low risk
- Assess the total risk to the organization
  - Make future security plans

Risk assessments
- External threats
  - Outside the organization
  - Hacker groups, former employees
- Internal threats
  - Employees and partners
  - Disgruntled employees
- Legacy systems
  - Outdated, older technologies
  - May not be supported by the manufacturer
  - May not have security updates
  - Depending on the age, may not be easily accessible

Multi-party risk
- Breaches involving multiple parties
  - Often trusted business relationships
  - Events often involve many different parties
- May 2019 - American Medical Collection Agency
  - Provided debt collection for many different organizations
  - Data breach disclosed personal information on 24 million individuals
  - Twenty-three healthcare organizations affected by this single breach
  - A single breach can cause a ripple effect

Risk assessments
- Intellectual Property (IP) theft
  - Theft of ideas, inventions, and creative expressions
  - Human error, hacking, employees with access, etc.
  - Identify and protect IP
  - Educate employees and increase security
- Software compliance/licensing
  - Operational risk with too few licenses
  - Financial risk with budgeting and over-allocated licenses
  - Legal risk if proper licensing is not followed

Risk management strategies
- Acceptance
  - A business decision; we'll take the risk!
- Risk-avoidance
  - Stop participating in a high-risk activity
- Transference
  - Buy some cybersecurity insurance
- Mitigation
  - Decrease the risk level
  - Invest in security systems

5.4 - Risk Analysis

Evaluating risk
- Risk register
  - Every project has a plan, but also has risk
  - Identify and document the risk associated with each step
  - Apply possible solutions to the identified risks
  - Monitor the results
- Risk matrix / risk heat map
  - View the results of the risk assessment
  - Visually identify risk based on color
  - Combines the likelihood of an event with the potential impact
  - Assists with making strategic decisions

		Consequence				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost Certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Audit risk model
- Inherent risk
  - Impact + Likelihood
  - Risk that exists in the absence of controls
  - Some models include the existing set of controls
- Residual risk
  - Inherent risk + control effectiveness
  - Risk that exists after controls are considered
  - Some models base it on including additional controls
- Risk appetite
  - The amount of risk an organization is willing to take

Risk control assessment
- Risk has been determined
  - Heat maps have been created
- Time to build cybersecurity requirements
  - Based on the identified risks
- Find the gap
  - Often requires a formal audit
  - Self-assessments may be an option
- Build and maintain security systems based on the requirements
  - The organizational risk determines the proper controls
- Determine if existing controls are compliant or non-compliant
  - Make plans to bring everything into compliance

Risk awareness
- A constantly changing battlefield
  - New risks, emerging risks
  - A nearly overwhelming amount of information
  - Difficult to manage a defense
- Knowledge is key
  - Part of every employee's daily job role
  - Part of the onboarding process for employees and partners
- Maintaining awareness
  - Ongoing group discussions
  - Presentations from law enforcement
  - Attend security conferences and programs

Regulations that affect risk posture
- Many of them
  - Regulations tend to regulate
- Regulations directly associated to cybersecurity
  - Protection of personal information, disclosure of information breaches
  - Requires a minimum level of information security
- HIPAA - Health Insurance Portability and Accountability Act
  - Privacy of patient records
  - New storage requirements, network security, protect against threats
- GDPR - General Data Protection Regulation
  - European Union data protection and privacy
  - Personal data must be protected and managed for privacy

Qualitative risk assessment
- Identify significant risk factors
  - Ask opinions about the significance
  - Display visually with traffic light grid or similar method

Quantitative risk assessment
- Likelihood
  - Annualized Rate of Occurrence (ARO)
  - How likely is it that a hurricane will hit? In Montana? In Florida?
- SLE (Single Loss Expectancy)
  - What is the monetary loss if a single event occurs?
  - Laptop stolen (asset value or AV) = $1,000
- ALE (Annualized Loss Expectancy)
  - ARO x SLE
  - Seven laptops stolen a year (ARO) x $1,000 (SLE) = $7,000
- The business impact can be more than monetary
  - Quantitative vs. qualitative

Disaster types
- Environmental threats
  - Tornado, hurricane, earthquake, severe weather
- Person-made threats
  - Human intent, negligence, or error
  - Arson, crime, civil disorder, fires, riots, etc.
- Internal and external
  - Internal threats are from employees
  - External threats are from outside the organization

5.4 - Business Impact Analysis

Recovery
- Recovery time objective (RTO)
  - Get up and running quickly
  - Get back to a particular service level
- Recovery point objective (RPO)
  - How much data loss is acceptable?
  - Bring the system back online; how far back does data go?
- Mean time to repair (MTTR)
  - Time required to fix the issue
- Mean time between failures (MTBF)
  - Predict the time between outages

Functional recovery plans
- Recover from an outage
  - Step-by-step guide
- Contact information
  - Someone is on-call
  - Keep everyone up to date
- Technical process
  - Reference the knowledge base
  - Follow the internal processes
- Recover and test
  - Confirm normal operation

Removing single points of failure
- A single event can ruin your day
  - Unless you make some plans
- Network configuration
  - Multiple devices (the "Noah's Ark" of networking)
- Facility / Utilities
  - Backup power, multiple cooling devices
- People / Location
  - A good hurricane can disrupt personnel travel
- There's no practical way to remove all points of failure
  - Money drives redundancy

Disaster recovery plan (DRP)
- Detailed plan for resuming operations after a disaster
  - Application, data center, building, campus, region, etc.
- Extensive planning prior to the disaster
  - Backups
  - Off-site data replication
  - Cloud alternatives
  - Remote site
- Many third-party options
  - Physical locations
  - Recovery services

Impact
- Life - The most important consideration
- Property - The risk to buildings and assets
- Safety - Some environments are too dangerous to work
- Finance - The resulting financial cost
- Reputation
  - An event can cause status or character problems

Mission-essential functions
- If a hurricane blew through, what functions would be essential to the organization?
  - That's where you start your analysis
  - These are broad business requirements
- What computing systems are required for these mission-essential business functions?
  - Identify the critical systems

Site risk assessment
- All locations are a bit different
  - Even those designed to be similar
- Recovery plans should consider unique environments
  - Applications
  - Personnel
  - Equipment
  - Work environment

5.5 - Privacy and Data Breaches

Information life cycle
- Creation and receipt
  - Create data internally or receive data from a third-party
- Distribution - Records are sorted and stored
- Use
  - Make business decisions, create products and services
- Maintenance
  - Ongoing data retrieval and data transfers
- Disposition
  - Archiving or disposal of data

Consequences
- Reputation damage
  - Opinion of the organization becomes negative
  - Can have an impact on products or services
  - Can impact stock price
- Identity theft
  - Company and/or customers information becomes public
  - May require public disclosure
  - Credit monitoring costs
- Fines
  - Uber
    - Data breach in 2016 wasn't disclosed
    - Uber paid the hackers $100,000 instead
    - Lawsuit settlement was $148 million
  - Equifax
    - 2017 data breach
    - Government fines were approximately $700 million
- Intellectual Property (IP) theft
  - Stealing company secrets
  - Can put an organization out of business

5.5 - Privacy and Data Breaches (continued)

Notification
- Internal escalation process
  - Breaches are often found by technicians
  - Provide a process for making those findings known
- External escalation process
  - Know when to ask for assistance from external resources
  - Security experts can find and stop an active breach
- Public notifications and disclosures
  - Refer to security breach notification laws
  - All 50 US states, EU, Australia, etc.
  - Delays might be allowed for criminal investigations

Privacy impact assessment (PIA)
- Almost everything can affect privacy
  - New business relationships, product updates, website features, service offering
- Privacy risk needs to be identified in each initiative
  - How could the process compromise customer privacy?
- Advantages
  - Fix privacy issues before they become a problem
  - Provides evidence of a focus on privacy
  - Avoid data breach
  - Shows the importance of privacy to everyone

Notices
- Terms of service
  - Terms of use, terms and conditions (T&C)
  - Legal agreement between service provider and user
  - User must agree to the terms to use the service
- Privacy notice, privacy policy
  - May be required by law
  - Documents the handling of personal data
  - May provide additional data options and contact information

5.5 - Data Classifications

Labeling sensitive data
- Not all data has the same level of sensitivity
  - License tag numbers vs. health records
- Different levels require different security and handling
  - Additional permissions
  - A different process to view
  - Restricted network access

Data classifications
- Proprietary
  - Data that is the property of an organization
  - May also include trade secrets
  - Often data unique to an organization
- PII - Personally Identifiable Information
  - Data that can be used to identify an individual
  - Name, date of birth, mother's maiden name, biometric information
- PHI - Protected Health Information
  - Health information associated with an individual
  - Health status, health care records, payments for health care, and much more
- Public / Unclassified
  - No restrictions on viewing the data
- Private / Classified / Restricted / Internal use only
  - Restricted access, may require a non-disclosure agreement (NDA)
- Sensitive - Intellectual property, PII, PHI
- Confidential - Very sensitive, must be approved to view
- Critical - Data should always be available
- Financial information
  - Internal company financial information
  - Customer financial details
- Government data
  - Open data
  - Transfer between government entities
  - May be protected by law
- Customer data
  - Data associated with customers
  - May include user-specific details
  - Legal handling requirements

5.5 - Enhancing privacy

Tokenization
- Replace sensitive data with a non-sensitive placeholder
  - SSN 266-12-1112 is now 691-61-8539
- Common with credit card processing
  - Use a temporary token during payment
  - An attacker capturing the card numbers can't use them later
- This isn't encryption or hashing
  - The original data and token aren't mathematically related
  - No encryption overhead

Data minimization
- Minimal data collection
  - Only collect and retain necessary data
- Included in many regulations
  - HIPAA has a "Minimum Necessary" rule
  - GDPR - "Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed."
- Some information may not be required
  - Do you need a telephone number or address?
- Internal data use should be limited
  - Only access data required for the task

5.5 - Enhancing privacy (continued)

Anonymization

- Make it impossible to identify individual data from a dataset
  - Allows for data use without privacy concerns
- Many different anonymization techniques
  - Hashing, masking, etc.
- Convert from detailed customer purchase data
  - Remove name, address, change phone number to ### ### ####
  - Keep product name, quantity, total, and sale date
- Anonymization cannot be reversed
  - No way to associate the data to a user

Data masking

- Data obfuscation
  - Hide some of the original data
- Protects PII
  - And other sensitive data
- May only be hidden from view
  - The data may still be intact in storage
  - Control the view based on permissions
- Many different techniques
  - Substituting, shuffling, encrypting, masking out, etc.

Pseudo-anonymization

- Pseudonymization
  - Replace personal information with pseudonyms
  - Often used to maintain statistical relationships
- May be reversible
  - Hide the personal data for daily use or in case of breach
  - Convert it back for other processes
- Random replacement
  - James Messer -> Jack O'Neill -> Sam Carter -> Daniel Jackson
- Consistent replacements
  - James Messer is always converted to George Hammond

5.5 - Data Roles and Responsibilities

Data responsibility

- High-level data relationships
  - Organizational responsibilities, not always technical
- Data owner
  - Accountable for specific data, often a senior officer
  - VP of Sales owns the customer relationship data
  - Treasurer owns the financial information

Data roles

- Data controller
  - Manages the purposes and means by which personal data is processed
- Data processor
  - Processes data on behalf of the data controller
  - Often a third-party or different group
- Payroll controller and processor
  - Payroll department (data controller) defines payroll amounts and timeframes
  - Payroll company (data processor) processes payroll and stores employee information

Additional data roles

- Data custodian/steward
  - Responsible for data accuracy, privacy, and security
  - Associates sensitivity labels to the data
  - Ensures compliance with any applicable laws and standards
  - Manages the access rights to the data
  - Implements security controls
- Data protection officer (DPO)
  - Responsible for the organization's data privacy
  - Sets policies, implements processes and procedures

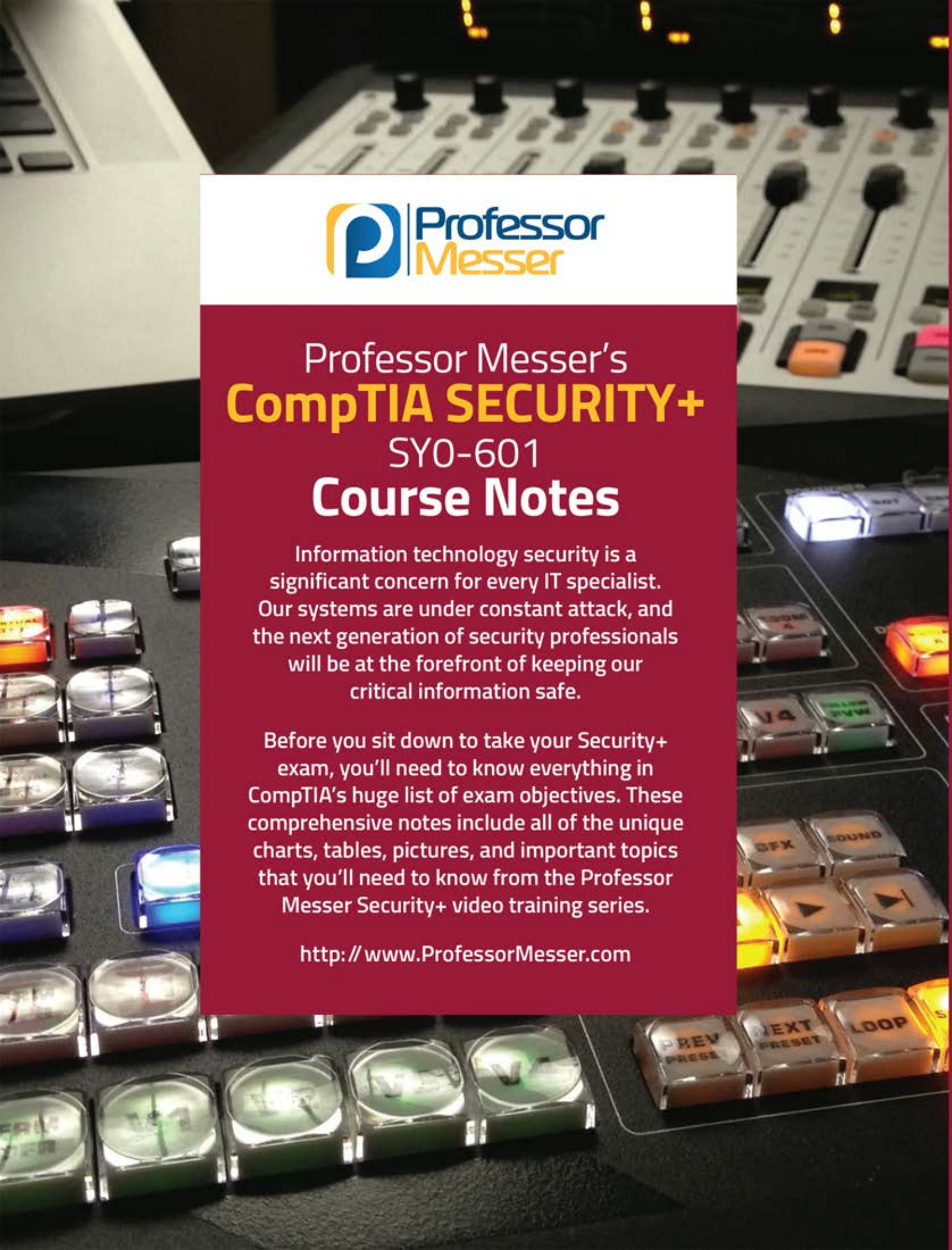
Continue your journey on
ProfessorMesser.com:

Professor Messer's Free
SY0-601 CompTIA Security+ Training Course

Monthly Security+ Study Group Live Streams

24 x 7 Live Chat

Professor Messer's
SY0-601 CompTIA Security+ Success Bundle



Professor Messer's

CompTIA SECURITY+

SY0-601

Course Notes

Information technology security is a significant concern for every IT specialist. Our systems are under constant attack, and the next generation of security professionals will be at the forefront of keeping our critical information safe.

Before you sit down to take your Security+ exam, you'll need to know everything in CompTIA's huge list of exam objectives. These comprehensive notes include all of the unique charts, tables, pictures, and important topics that you'll need to know from the Professor Messer Security+ video training series.

http://www.ProfessorMesser.com