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 1.05

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

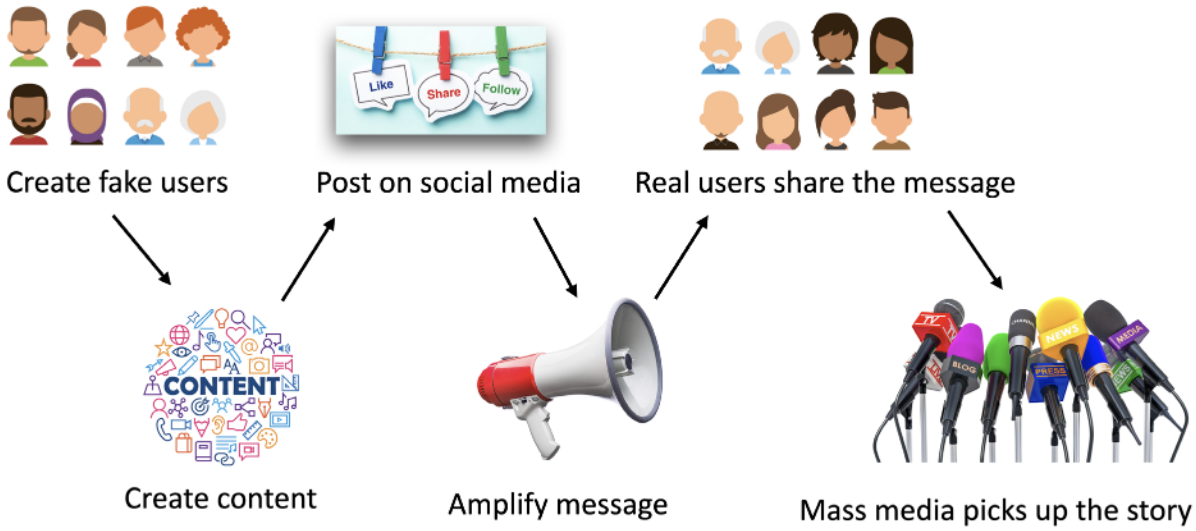
1.1 - Influence Campaigns

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

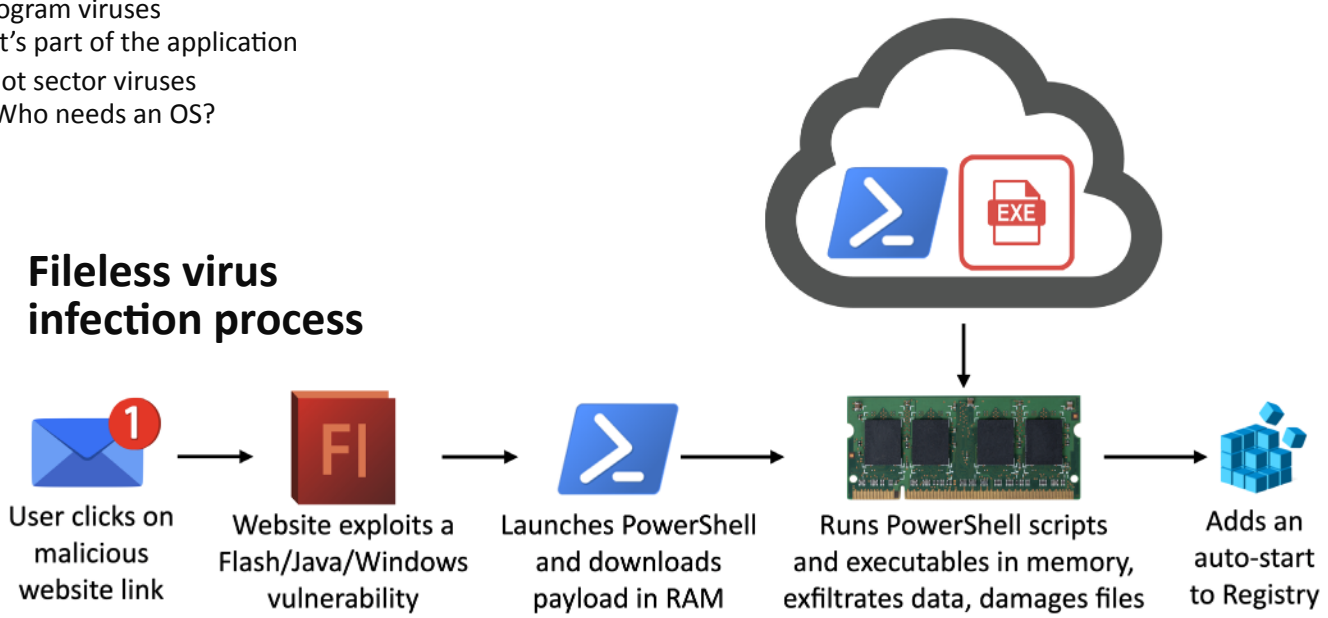
- These all work together
  - A worm takes advantage of a vulnerability
  - Installs malware that includes a remote access backdoor
  - Bot may be installed later
- Your computer must run a program
  - Email link - Don't click links
  - Web page pop-up
  - Drive-by download
  - Worm
- Your computer is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

1.2 - Viruses and Worms

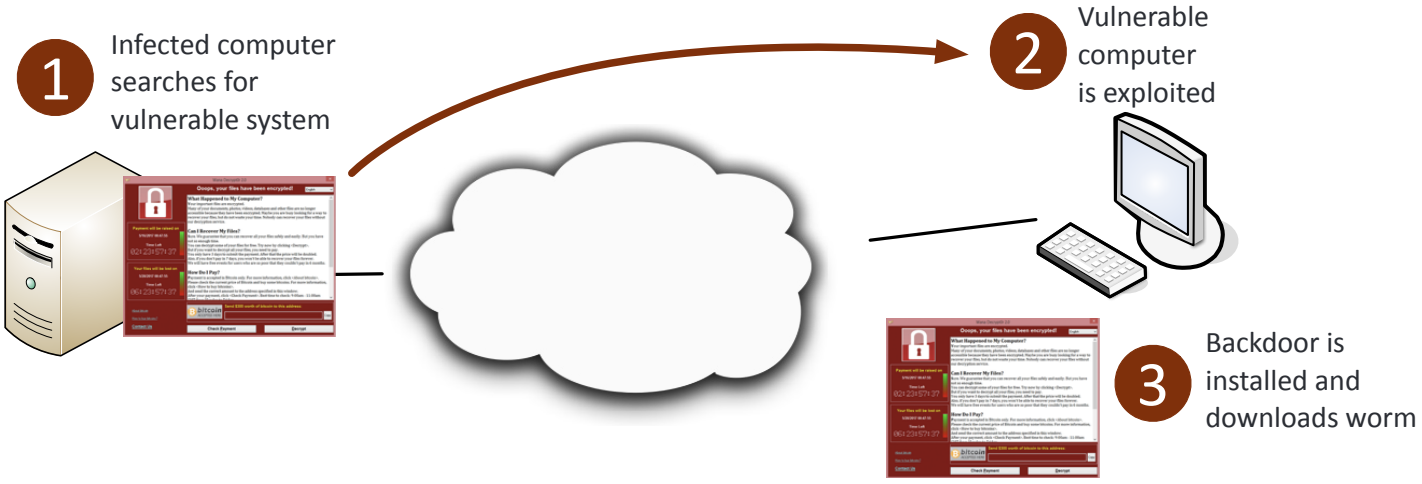
Virus
- Malware that can reproduce itself
  - It needs you to execute a program
- Reproduces through file systems or the network
  - Just running a program can spread a virus
- May or may not cause problems
  - Some viruses are invisible, some are annoying
- Anti-virus is very common
  - Thousands of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

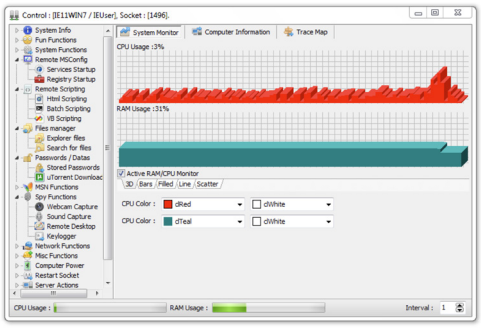
- Identified by anti-virus/anti-malware
  - Potentially undesirable software
  - Often installed along with other software
- Overly aggressive browser toolbar
- A backup utility that displays ads
- Browser search engine hijacker

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

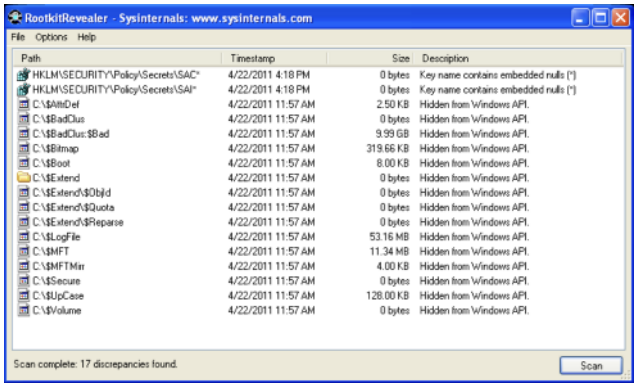
- Don't run unknown software
  - Consider the consequences
- Keep anti-virus/anti-malware signatures updated
  - There are always new attacks
- Always have a backup
  - You may need to quickly recover

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

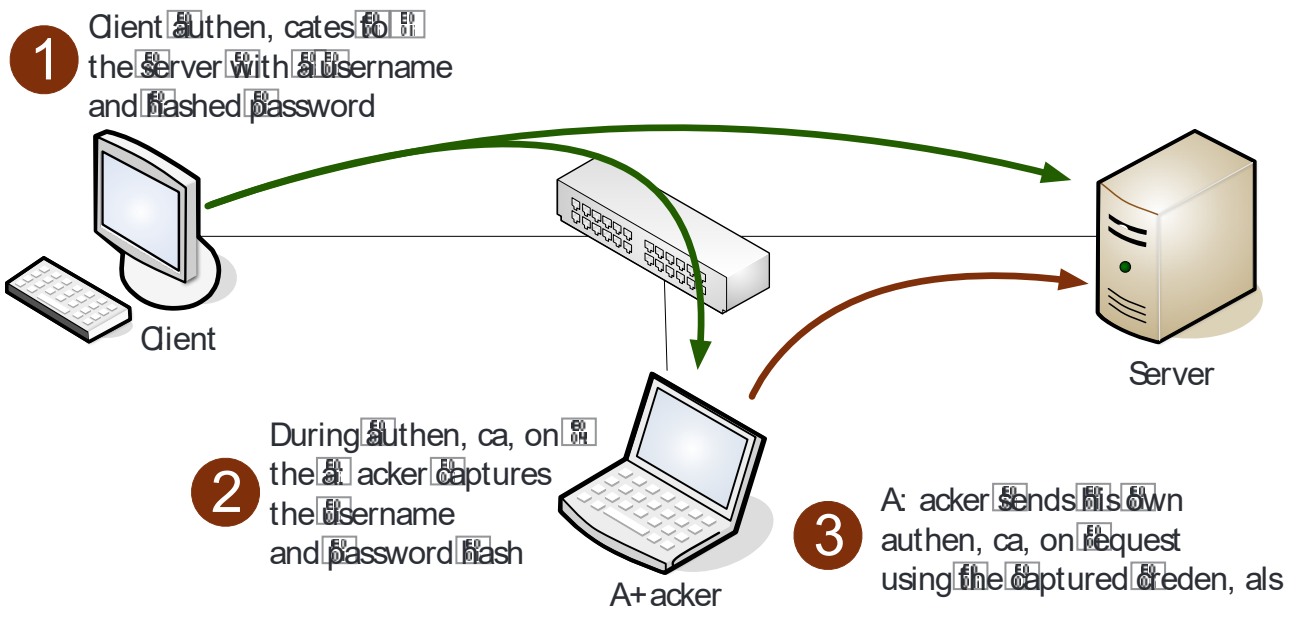
Variable(Name	A								B	
Value	'e'	'x'	'c'	'e'	's'	's'	'i'	'v'	25856	
Hex(Value	65	78	63	65	73	73	69	76	65	00

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

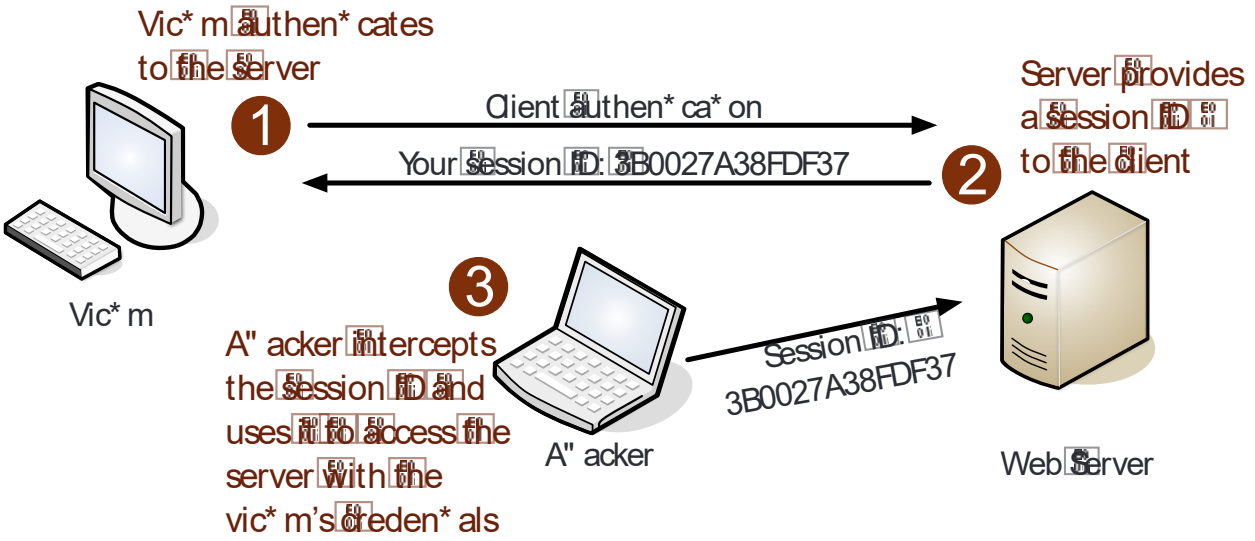
- Encrypt end-to-end
  - They can't capture your session ID if they can't see it
  - Additional load on the web server (HTTPS)
  - Firefox extension: HTTPS Everywhere, Force-TLS
  - Many sites are now HTTPS-only
- Encrypt end-to-somewhere
  - At least avoid capture over a local wireless network
  - Still 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

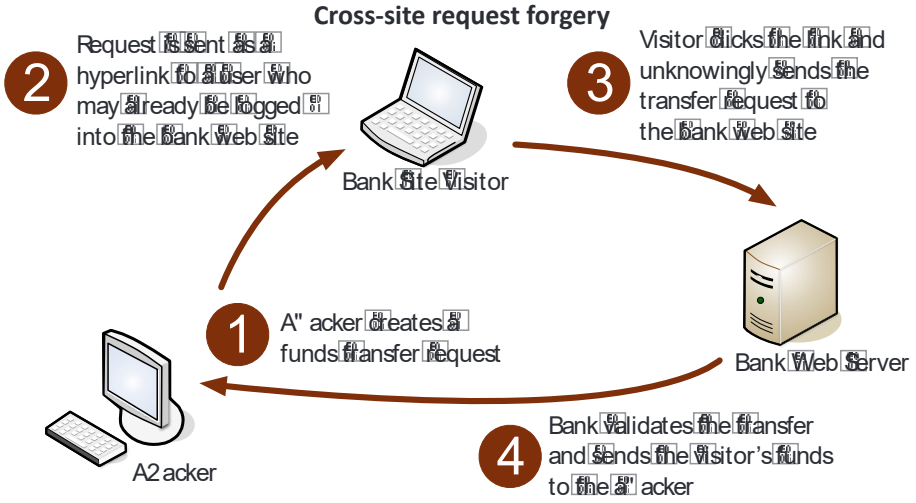
- Cross-site requests are common and legitimate
  - You visit ProfessorMesser.com
  - Your browser loads text from the ProfessorMesser.com server
  - Your browser loads a video from YouTube
  - Your browser loads pictures from Instagram
- HTML on ProfessorMesser.com directs requests from your browser
  - 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)

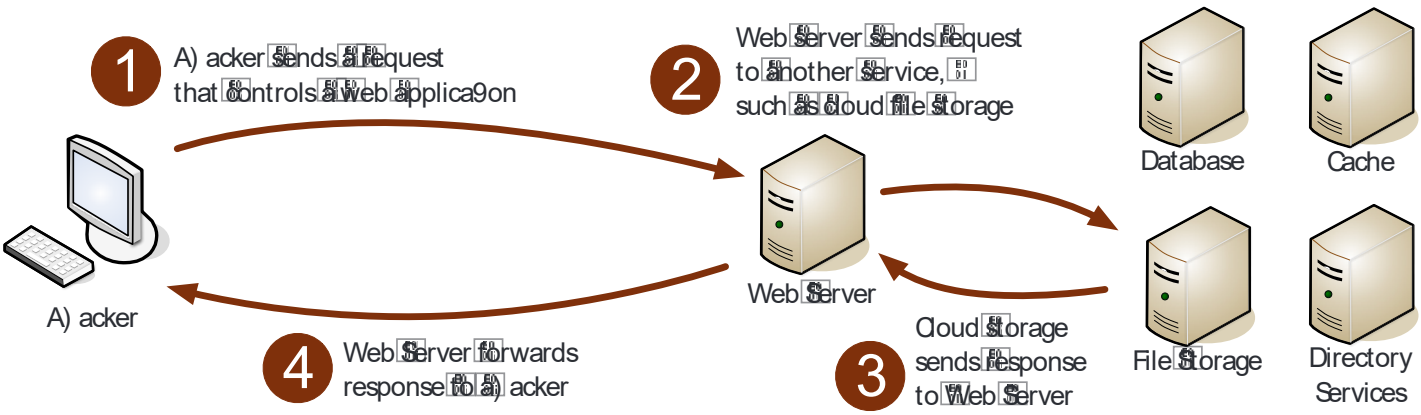
Server-side request forgery (SSRF)

- 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

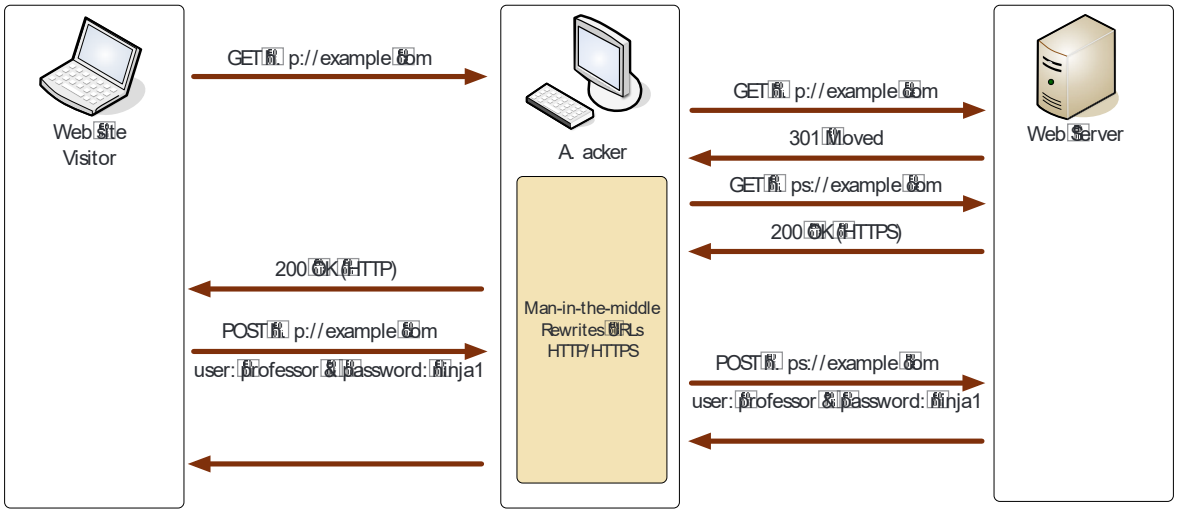
SSL stripping / HTTP downgrade

- 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



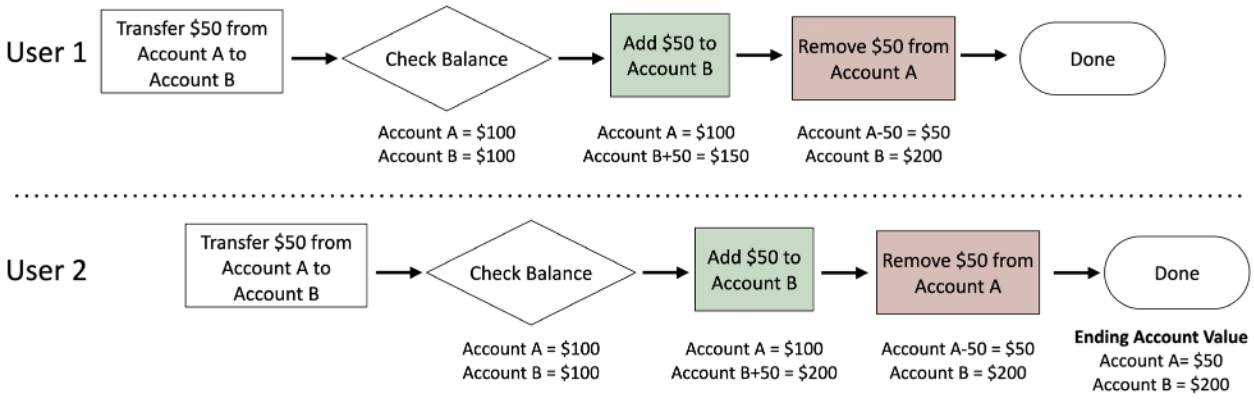
1.3 - Race Conditions

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

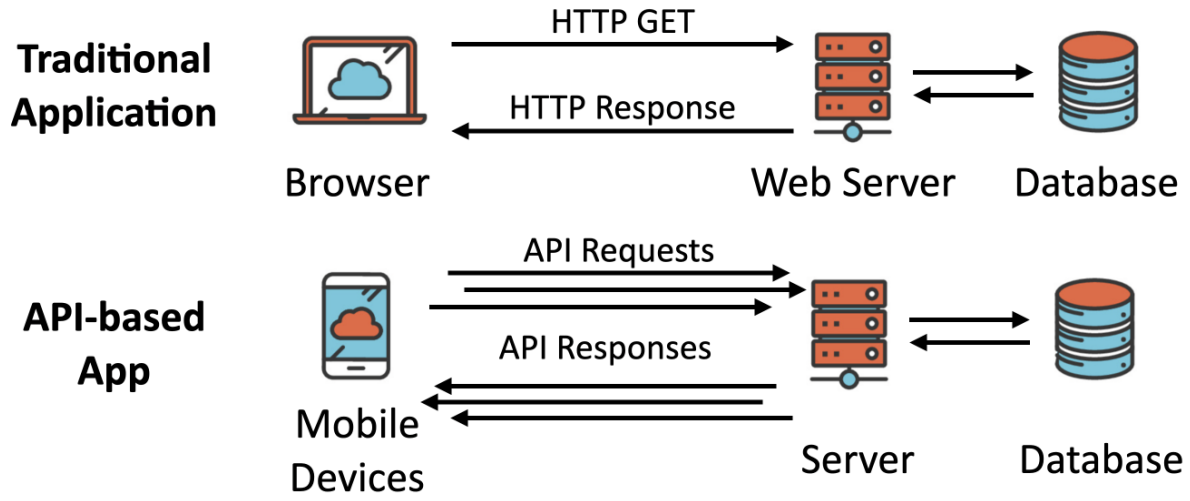
API attacks

- 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

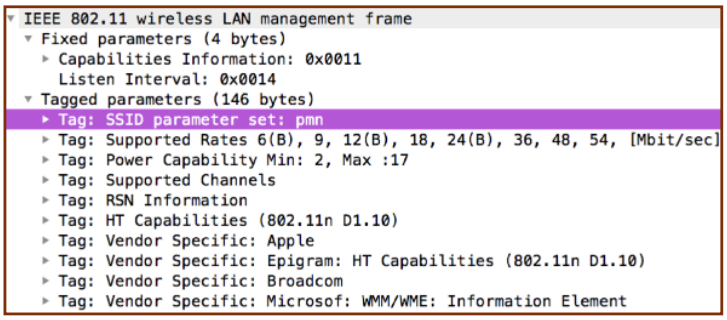
- Surfing along on your wireless network
  - And then you're not
- And then it happens again
  - And again
- You may not be able to stop it
  - There's (almost) nothing you can do
  - Time to get a long patch cable
- Wireless disassociation
  - A significant wireless denial of service (DoS) attack

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 NFC 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

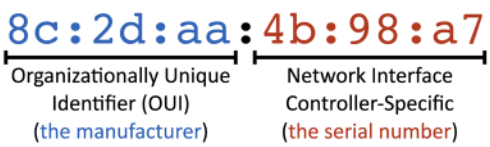
On-path browser attack

- 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 (CVSS)
  - Quantitative scoring of a vulnerability - 0 to 10
  - The scoring standards change over time
  - Different scoring for CVSS 2.0 vs CVSS 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 known and unknown
  - 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 digital 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

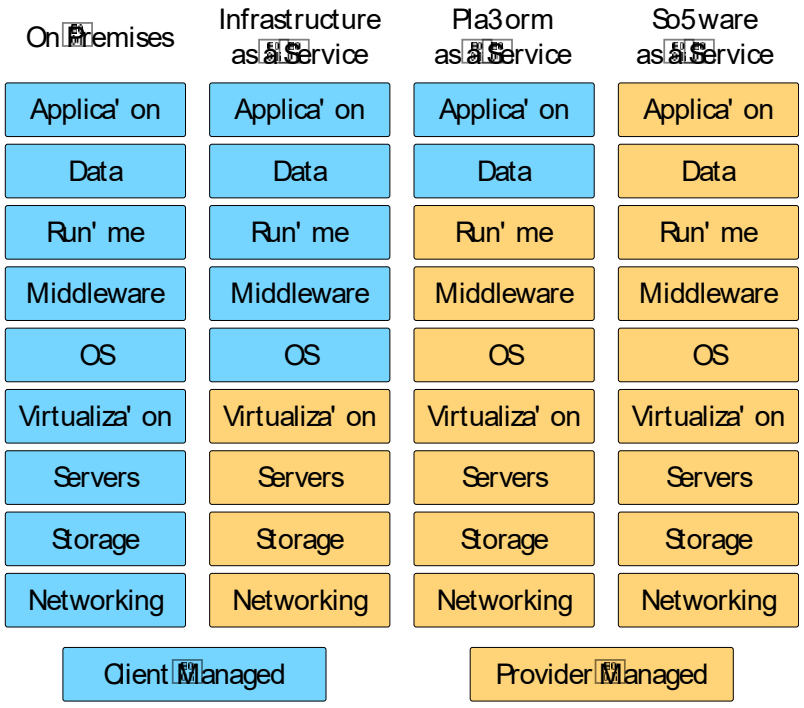
2.2 - Cloud Models

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

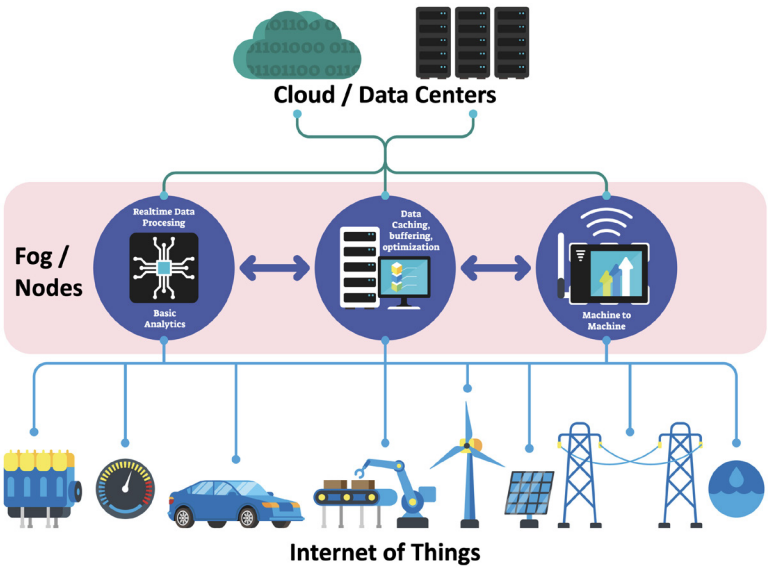
Cloud deployment models
- Public
  - Available to everyone over the Internet
- Community
  - Several organizations share the same resources
- Private
  - Your own virtualized local data center
- Hybrid
  - A mix of public and private

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