COMP 150: Cyber Attacks

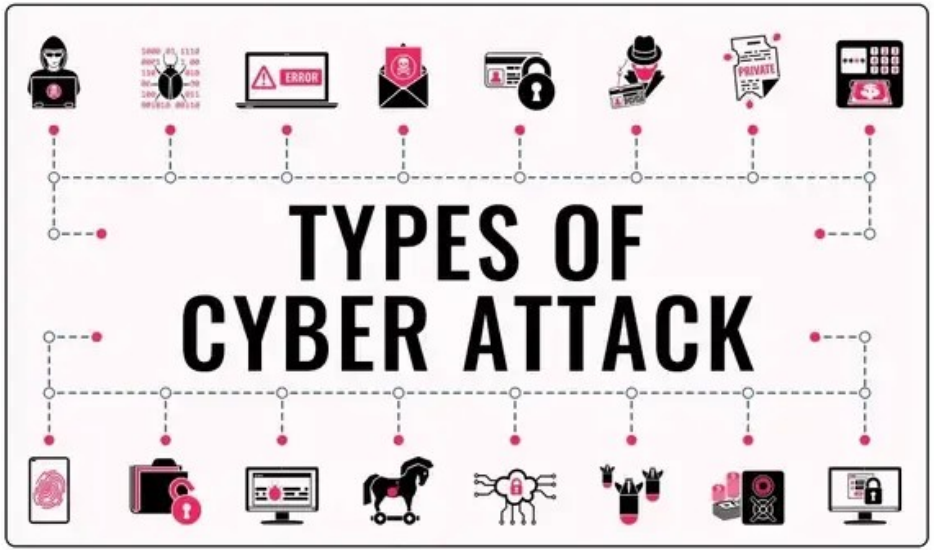
Week 10, Lecture 15

Agenda

- What is a cyber attack?
- Types of hackers
- Types of attacks
- Historic attacks

What is a cyber attack?

- Unauthorized access to computer or data system
- Intentional and directed
- Goal is to:
  - Identify problems (best-case)
  - Steal
  - Damage
  - Ransom
  - Disrupt



Types of Hackers

The Hats

- Black Hat
  - Malicious intent
  - Not given permission
  - No warning
- White Hat
  - Honorable intent
  - *Are* given permission
  - Intentionally work to inform manufacturers *before* attacks are known
- Grey Hat
  - Generally honorable intent
  - Not given permission, *but*
  - Intentionally work to inform manufacturers *before* attacks are known

The 6 Different Types of Hackers

Black Hat Hackers: Bad hackers who use cyber attacks to gain money or to achieve another agenda.

These hackers penetrate systems without permission to exploit known or zero-day vulnerabilities.

White Hat Hackers: Ethical hackers who protect your systems from black hat hackers.

Penetrate the system with the owner's permission to find and fix security vulnerabilities and mitigate cyberattacks.

Grey Hat Hackers: Hackers who cruise the line between being good and bad. Penetrate systems without permission but typically don't cause harm.

Draw attention to vulnerabilities and often offer a solution to patch them by charging fees.

Red Hat Hackers: Hackers who use cyber attacks to attack black hat hackers.

Their intentions are noble, but these hackers often take unethical or illegal routes to take down bad hackers.

Blue Hat Hackers: Hackers who seek to take personal revenge, or outside security professionals that companies hire to test new software & other products to find vulnerabilities prior to release.

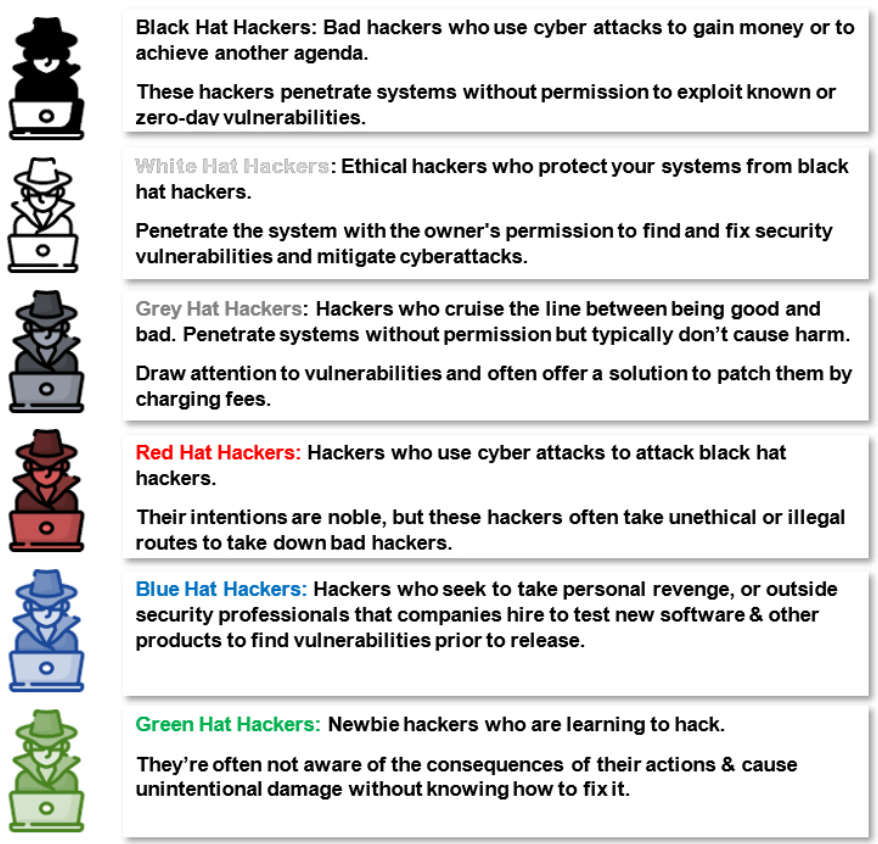
Green Hat Hackers: Newbie hackers who are learning to hack.

They're often not aware of the consequences of their actions & cause unintentional damage without knowing how to fix it.

Types of Hackers

The Hats

- Red Hat
  - Malicious intent, but only at Black Hats
  - Robin Hood hackers
- Blue Hat
  - Revenge-seeking, *or*
  - Hired by companies (Microsoft uses this term)
- Green Hat
  - “Oops I broke the stock exchange”
  - New hackers who are learning
  - Something like a term of endearment

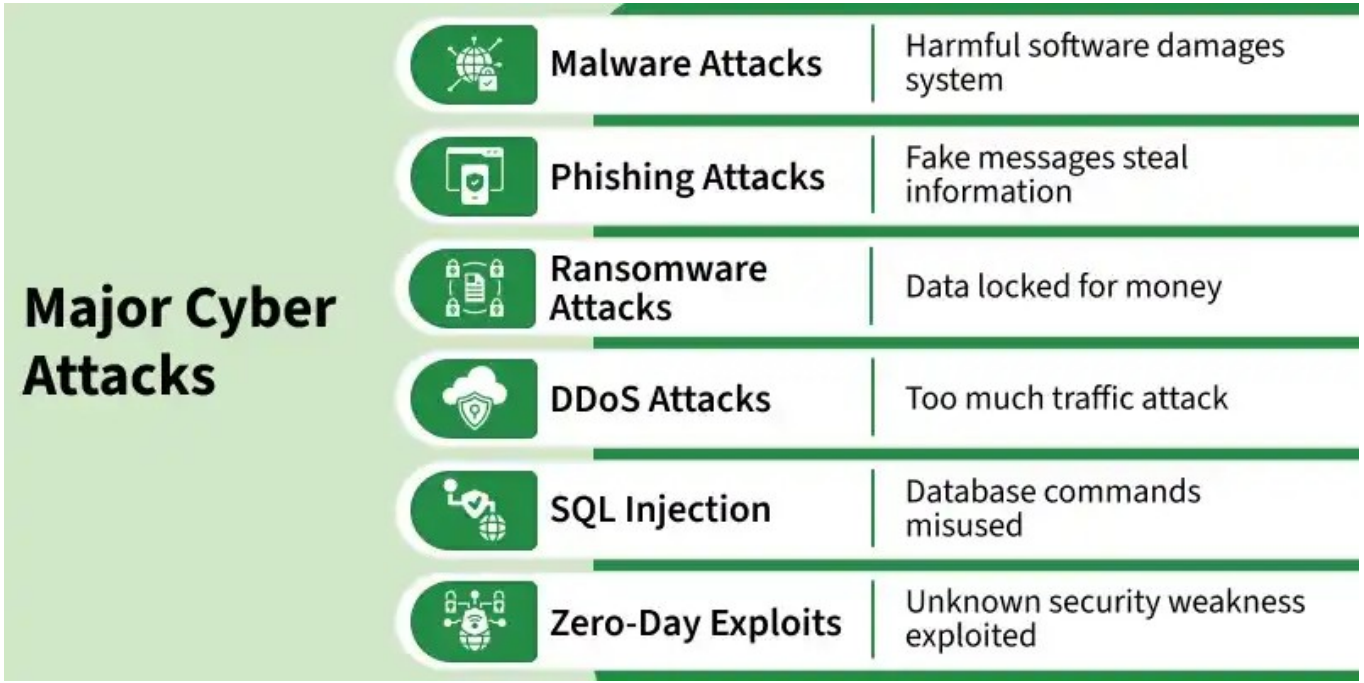


Types of Hackers

Other Roles

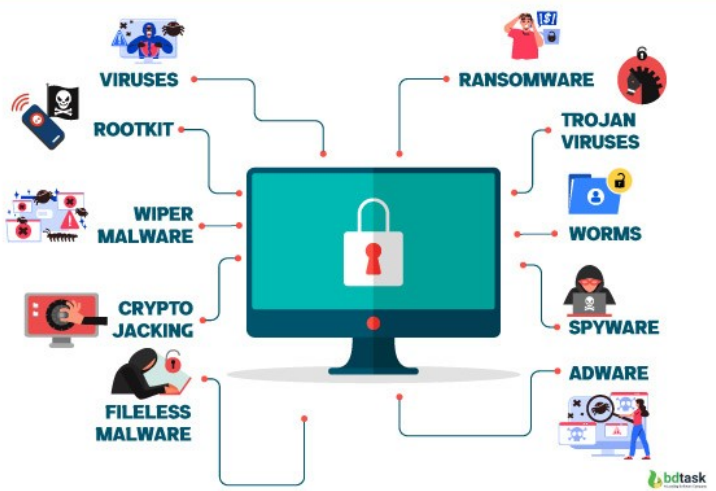
- “Script kiddies”
  - People who are new at or uninformed about hacking
  - Combine existing attacks
- “Hacktivists”
  - Motivations often political, but awareness-focused
  - Hack to make changes that draw attention - basically, digital protesters
- Cyber terrorism
  - Motivations often political or national
  - Hack to disrupt or damage
- State-sponsored or Nation-state hackers
  - Employees of governments
  - Take part in espionage via cyber attacks

Types of Attacks



Malware Attacks

- Malicious software
  - “Worms”, “viruses”
- Installed through infected files, software downloads, or email attachments
- Steal personal information, passwords, or financial data



Example:

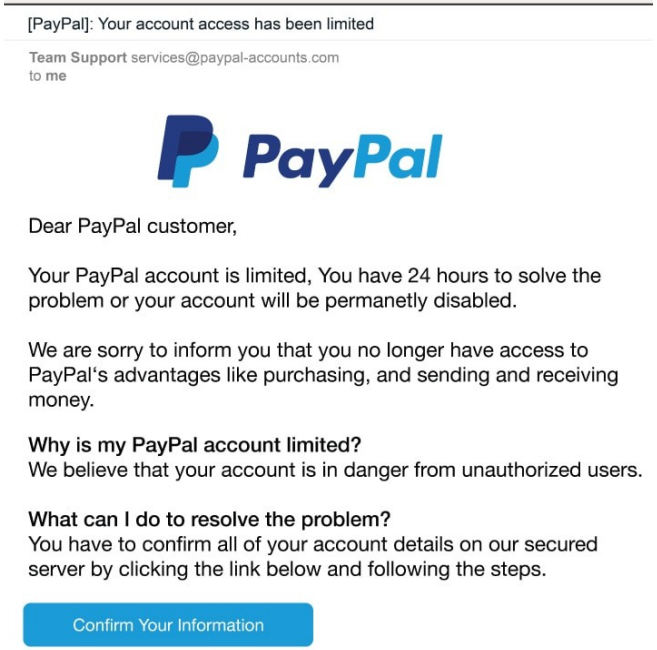
A user downloads free software from an untrusted website. The software secretly installs malware that records the user's keystrokes and steals login credentials.

Phishing Attacks

- Social engineering, not programming
- Trick users into revealing credentials or downloading malware
- Without a doubt: the most common type of cyber attack

Example:

A user receives an email claiming to be from a bank asking them to verify their account. The email includes a link to a fake website that looks exactly like the bank's login page. When the user enters their username and password, the attacker steals the credentials.


[PayPal]: Your account access has been limited

Team Support services@paypal-accounts.com
to **me**

PayPal

Dear PayPal customer,

Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanetly disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

Why is my PayPal account limited?
We believe that your account is in danger from unauthorized users.

What can I do to resolve the problem?
You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

Confirm Your Information

Ransomware Attacks

- Specific type of malware
  - Encrypts (locks) a user's system until they pay some bounty
  - Often target individuals, but some target only large enterprise environments
- Often spread via other malware or via phishing emails
- Common and devastating

Example:

Ryuk, likely Russian-made ransomware that is only used in enterprise environments, as with the Baltimore County (Maryland) school system in 2018

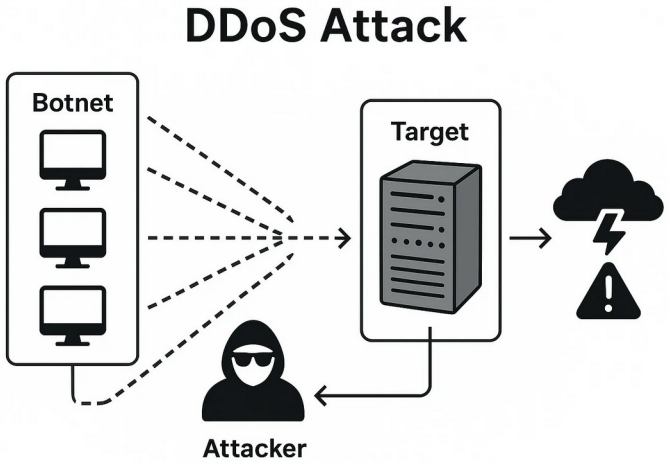
```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but
not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
KurtSchweickardt@protonmail.com
or
KurtSchweickardt@tutanota.com

BTC wallet:
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk

Ryuk
No system is safe
```

DDoS Attack

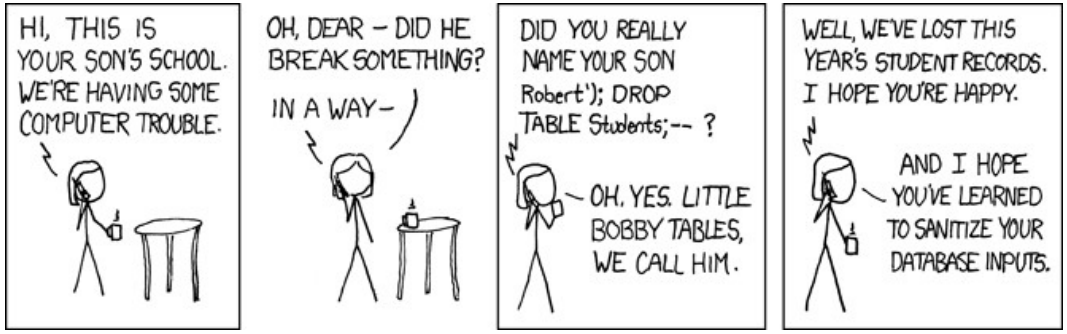
- Distributed Denial of Service (DDoS) Attack
- Flood an online service with traffic from multiple requesters
  - Legitimate users can no longer access the system
- Extremely common!

Example:

Thousands of infected computers send requests to a website at the same time, causing the server to slow down or completely crash.



SQL Injection



- Structured Query Language:
  - Databases!
- SQL injection attacks:
  - Put malicious SQL queries into parts of a website
  - Hope it hits the database
- Example of raw security vulnerability; programmers must protect their work against this kind of attack

Example:

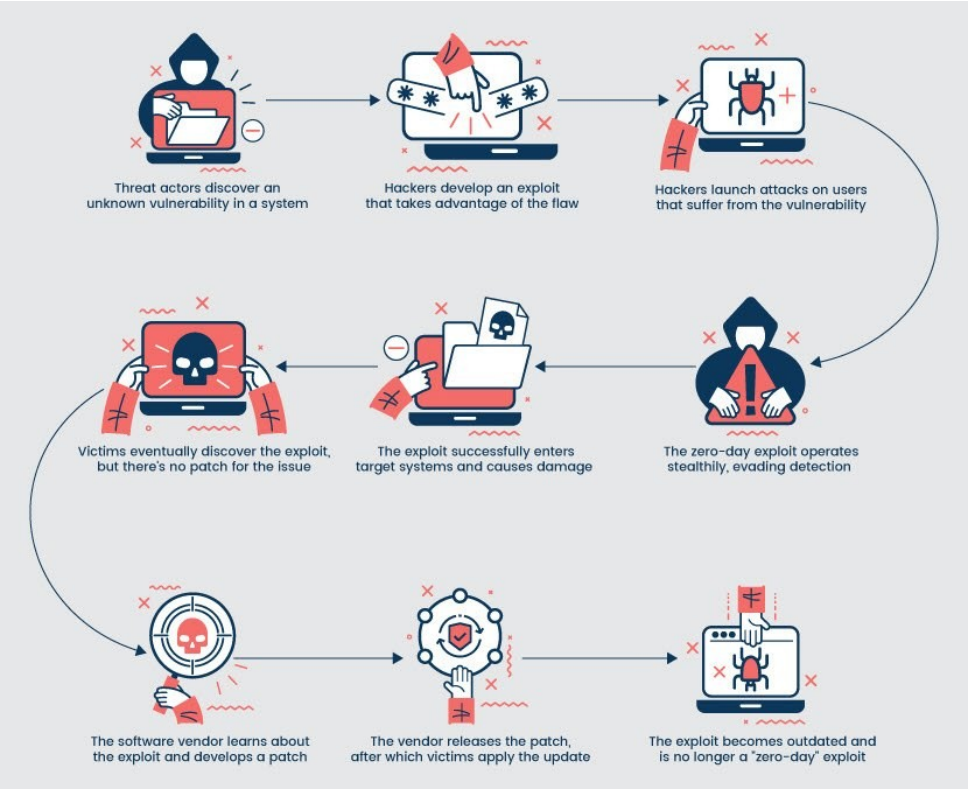
An attacker enters a specially crafted SQL command into a login form to bypass authentication and access the database.

Zero-Day Exploits

- Previously-unknown vulnerability used by malicious actors
- *Detection*, let alone defense, might not yet exist

Example:

- Hackers discover a vulnerability in a web browser and exploit it to install malware on users' systems before the browser company releases a security update.

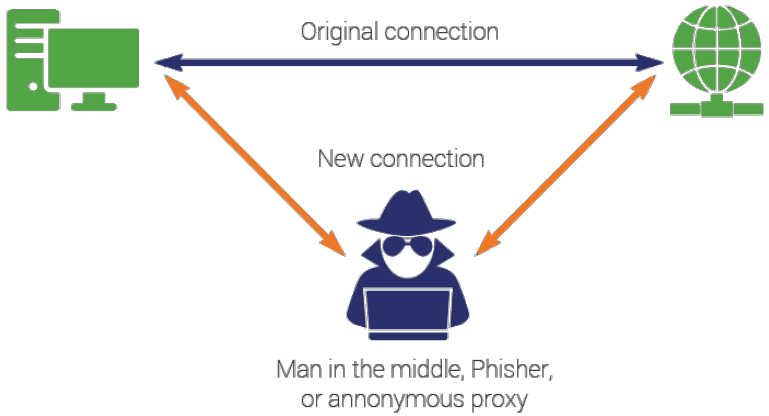


Man-In-The-Middle Attacks

- A listener intercepts communication between two parties
- Data (such as credentials) can be stolen
- Similar to phishing, but less reliant on social engineering

Example:

A user connects to free public Wi-Fi in a café and logs into their bank account while the attacker intercepts the login data.

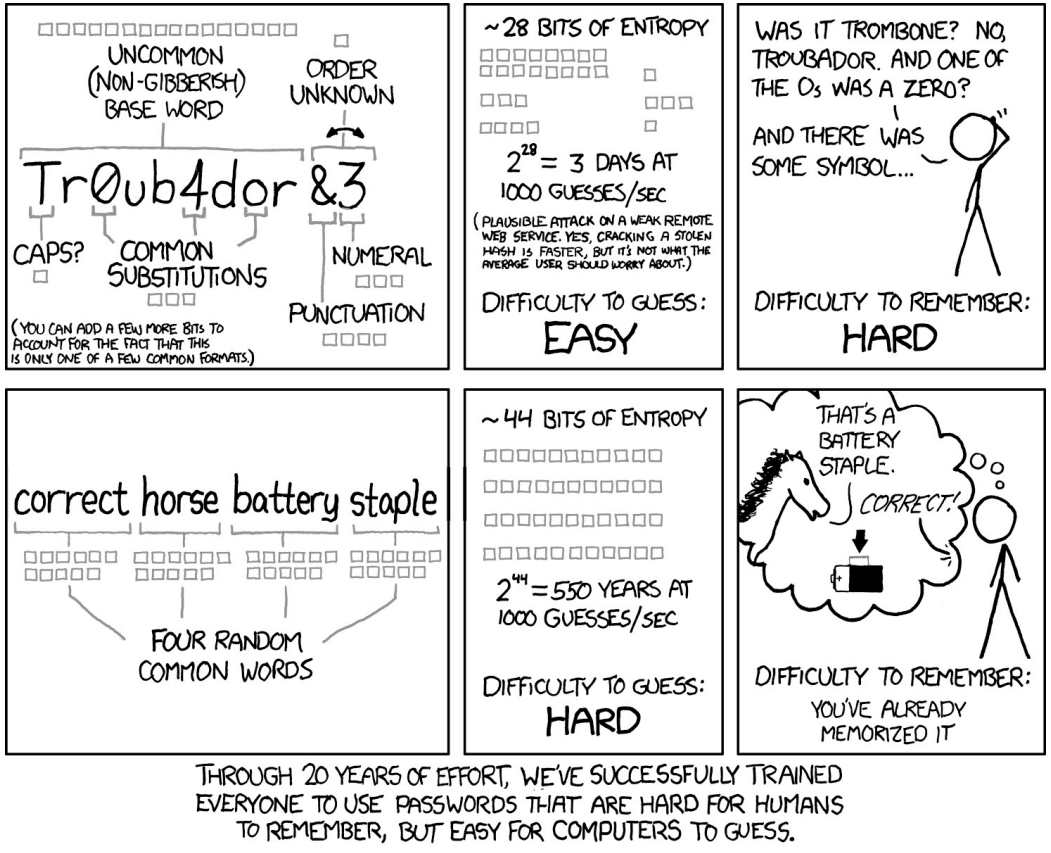


Password Attacks

- Tools are used to guess passwords
- The strength of a password is key!

Example:

An attacker uses a program that tries thousands of password combinations on a login page until the correct password is found.



How are cyber attacks prevented?

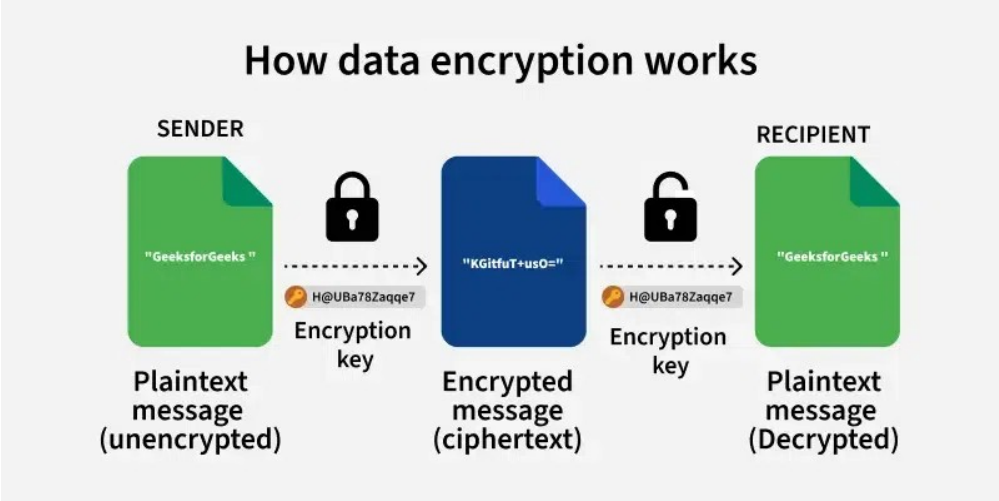
- You!
  - Strong passwords
  - MFA
  - Keep your devices and browsers updated
  - Don't click weird links
  - Don't use cables or USB drives offered by people you don't trust
  - **Do not, for the love of all that is good, give an AI access to your file system**

How are cyber attacks prevented?

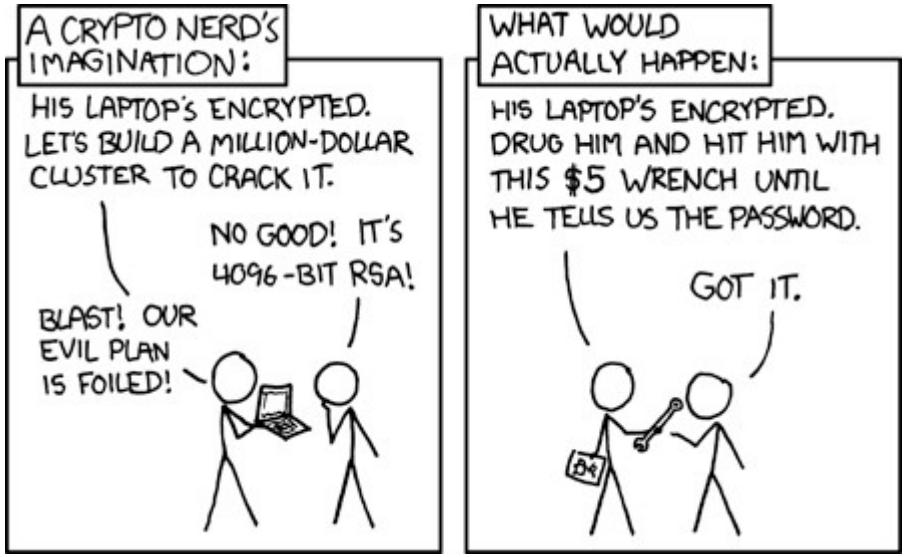
- Network
  - Antivirus/Anti-malware software
  - Monitoring and threat detection software
  - Updates, updates, updates
- Operating system
  - Access control
  - Automatic security updates
  - System monitoring
- Encryption

What is Encryption?

- Pass data through a special, two-way algorithm
- Store or send only gibberish
- Without the key, the actual data remains hidden!
- Types:
  - Symmetric
  - Asymmetric
- Issues
  - Only as good as the encryption algorithm
  - Only as secure as the key
  - Takes *time*



What is Encryption?



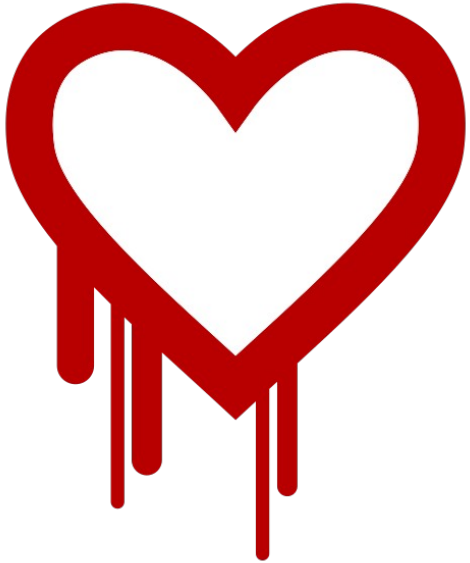
Famous Attacks

- Range from the trivial to the deadly
- Target the everyday or the exceptional

Not to be dramatic, but it's a battlefield out there.

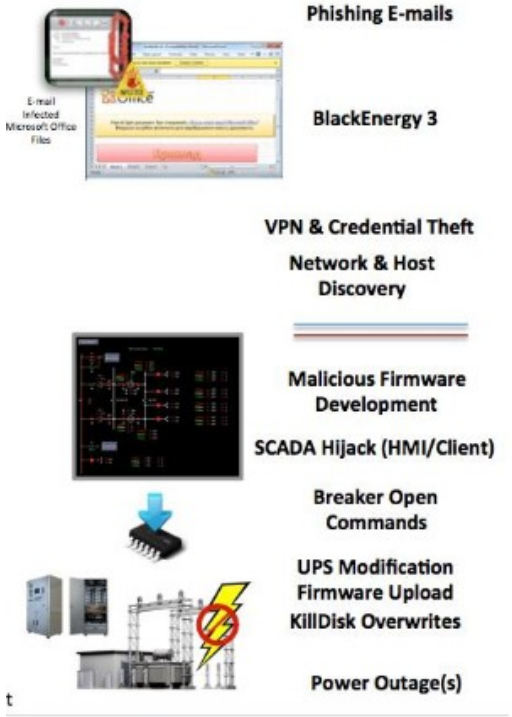
2012: Heartbleed Vulnerability

- Vulnerability in OpenSSL
  - Encryption tool for client/server communications
  - Allowed leakage of private keys
  - Led to endless exploits and loss of data
- Widely considered one of the worst cyber infrastructure vulnerabilities ever
  - Tor Project:
  - “If you need strong anonymity or privacy on the Internet, you might want to stay away from the Internet entirely for the next few days while things settle.”



2015: Ukraine Power Grid Hack

- Russian hacking group “Sandworm”
- Took down power grid in western Ukraine for 6 hours
- BlackEnergy3
  - Phishing
  - Malware
  - Intercept then re-write the code on the breakers
  - DDoS the phone lines to delay response



2017: Spectre and Meltdown

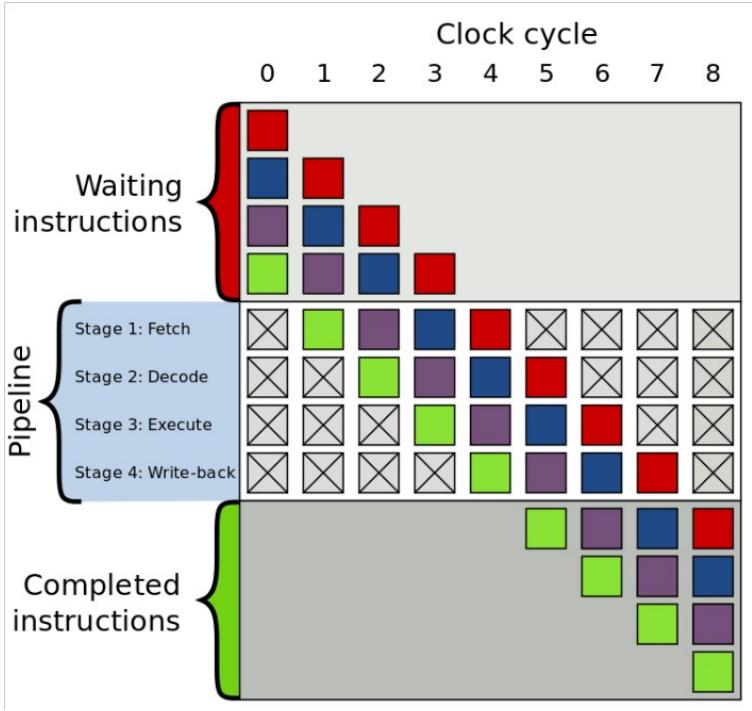
- *Thankfully* found by grey/white hats
- Exploits nature of CPUs to leak data or escalate permission
  - Terrifying in its reach
- Fixing it required
  - Patching all CPUs, especially Intel, at a 30-60% time cost
  - Re-working instructions
  - Re-designing entire portions of the OS
  - Re-designing hardware

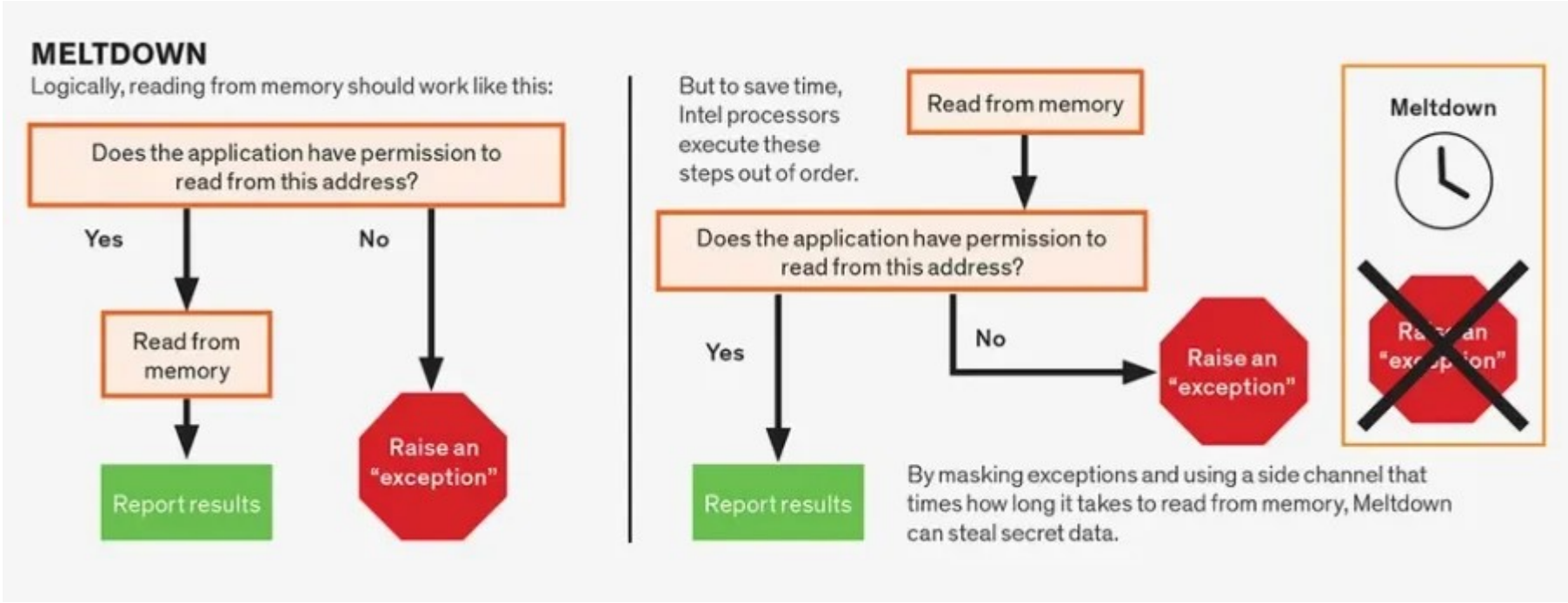
Some Speculative Executions Vulnerabilities

VULNERABILITY	WHAT'S EXPLOITED?	DISCLOSED
Spectre Variant 1	Branch-direction predictor	1/2018
Spectre Variant 2	Branch-target buffer	1/2018
Branchscope	Branch-direction predictor	3/2018
Spectre Variant 4	Speculative store bypass	5/2018
Spectre RSB/ Ret2Spec	Return stack buffer	6/2018
Lazy FPU	Lazy restore of floating-point unit registers	6/2018
TLBleed	Translation-lookaside buffer	6/2018
NetSpectre	Branch-direction predictor	7/2018
Meltdown	Page-permission check	01/2018
Foreshadow/L1TFl	Address translation	08/2018

2017: Spectre and Meltdown

- CPUs “think ahead”
  - Execute multiple instructions at a time
  - Make a best-guess on what the code will do next, then
  - Start executing it
  - If wrong, no harm done
  - If right, major performance gain!
- Spectre and Meltdown exploited this
  - Used prediction to manufacture branch speculation failure
  - Combined with other attacks to leak data



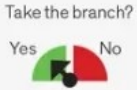

MELTDOWN
Logically, reading from memory should work like this:
Does the application have permission to read from this address?
Yes
No
Read from memory
Report results
Raise an "exception"
But to save time, Intel processors execute these steps out of order.
Read from memory
Does the application have permission to read from this address?
Yes
No
Raise an "exception"
Report results
Meltdown
By masking exceptions and using a side channel that times how long it takes to read from memory, Meltdown can steal secret data.

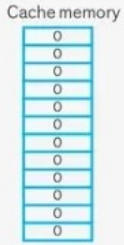
SPECTRE VARIANT 1

Spectre v1 can be summed up in the following piece of code:

```
If (x<256){
        secret=array1[x]
        y=array2[secret]
}
```

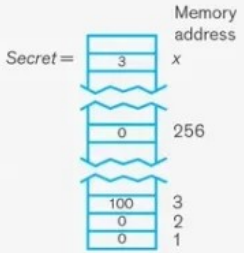
1. The code is run several times with *x* less than 256. This primes the branch predictor to expect *x* to be less than 256 the next time.

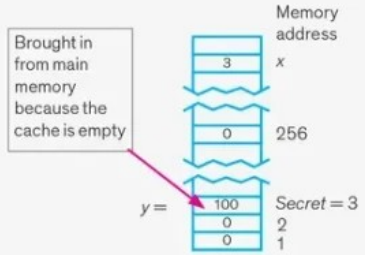




2. The attacker empties the processor's cache using flush instructions, so that any data read by the program must be brought in from main memory.

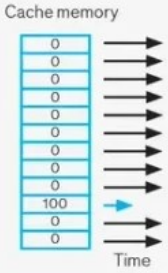
3. The attacker runs the code with *x* set to a value greater than 256. The processor begins to "speculatively" execute the rest of the code as if *x* were less than 256. The memory address at *x* contains secret data the attacker wants. The software assigns this data to the variable *secret*.





4. Next, the code uses the value of *secret* as a memory address. It reads the data at that address, bringing that data into the cache from main memory

5. Eventually, the processor realizes that it should not have taken the branch. It does not make the values *secret* and *y* visible to the program.



6. The attacker accesses each address in the cache systematically. Because the memory address equal to the secret is the only one whose data has already been brought in from main memory, it takes less time to access than all the others, thereby revealing the secret.

2017: WannaCry Ransomware

- Propagated using EternalBlue
  - Developed by the NSA - and they didn't tell Microsoft for *5 years*
  - Targets servers in a multi-server system network
  - Released by The Shadow Brokers
- Spread using DoublePulsar
  - Also developed by the NSA
  - Also released by The Shadow Brokers
- Infected more than 300,000 machines
- Cost more than $1B in damages

2025: Crosswalk Voice Actors

- Menlo Park, Palo Alto, and Redwood City, CA
- Audio-enabled crosswalk buttons offered AI recordings of Mark Zuckerberg and Elon Musk
- Achieved through the use of repeated and default passwords