Introduction to Cybersecurity

04/08/2024

By:
Nick Polanco

Instructor:
Dr. Betty H.C. Cheng

How do we want software to work?

What do you want to happen when you send money via Venmo?

- Money is safely transferred when you attempt to complete the transaction
- The correct amount is sent (nothing more, nothing less)
- Viewing by others is either enabled or disabled

How do we want software to work?

What don’t you want to happen?

- Bank information leaked
- Amount sent to wrong person
- More than expected
- Message gets sent to all your contacts

Terminology

"A computer is *secure* if you can depend on it and its software to behave as you expect (intent)."

'*Trust* describes our level of confidence that a computer system will behave as expected.' (intended)

[Garfinkel & Spafford, Kasten]

Slide taken from Dr. Cheng

What are industries who rely heavily on software?

Banking and e-commerce

- Debit card, credit cards, banking applications

Governments

- National defense-related system that processes classified information, power grids, military assets

Health

- Pacemakers, medical records, robotic surgery arms

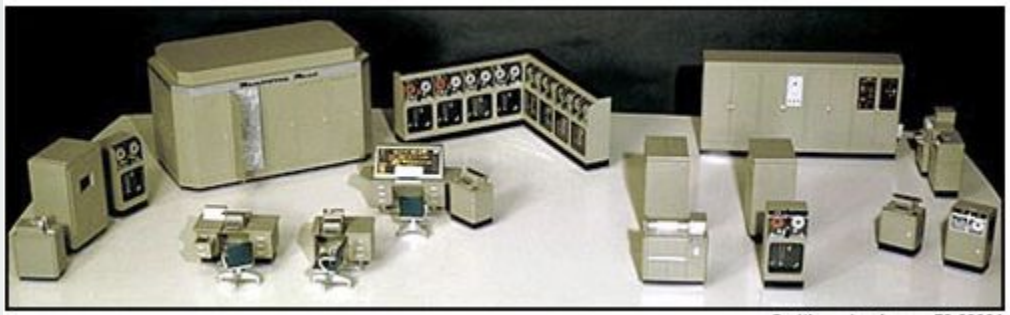
Autonomous Vehicles

- Hacking an automatic vacuum versus an autonomous vehicle
  - This is a larger problem, a cyber-physical system

Is security always considered?

The Internet

- In the 1960's, the internet was a tool for sharing research
  - Security was originally **not** the main focus
- U.S defense department created ARPANET (Advanced Research Projects Agency Network) in the Cold War
  - This is the network that ultimately evolved into what we now know as the Internet



[https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml#:~:text=Sharing%20Resources,government%20researchers%20to%20share%20information.]

Is security always considered?

Now, we can order entire houses and manage our bank account.

- Security is often, and was, an **afterthought**
  - Added onto a system, but it may not fully address the underlying issue
  - Lots of patches to an issue, causes inefficiency and **chasing**

[https://ecocor.us/portfolio/azalea/]

Outline

1. Terminology
2. Why does security matter?
3. What can we do?
4. Threat types
5. Sample attacks
6. Malware
7. Risk assessment
8. Key takeaways

Terminology

Terminology

Security Policy: The set of rules, practices, strategies, that specify or regulate how a system provides security services

Vulnerability: A flaw, weakness, area prone to attack in a system that *can* be exploited

[https://managex.ae/wp-content/uploads/2022/05/What-are-the-seven-types-of-cyber-security-threats.jpg]

Terminology

Threat: A possible security exploit or violation. A danger that might exploit a vulnerability.

Attack: The act of carrying out a threat, an exploit on the system that derives from a threat.

Asset: The part of a system that has the value. This can be something like the function of a system or data.

Why does security matter?

Why does security matter?

What is the value of the **asset** that is being targeted?

- What if it is changed? Altered? Viewed?
  - Example: Information
    - FERPA, HIPPA

https://www.hipaajournal.com/what-is-hipaa/
https://www.lex2.org/apps/pages/index.jsp?uREC_ID=991481&type=d&pREC_ID=2477745

Why does security matter?

What if someone uses an **asset** when not authorized

- What happens if the wrong party gains access to this asset?
  - Ex. Gaining access to restricted area, cameras, “computer person” heist movie

[https://us.amazon.com/Original-Movie-Prop-National-Authentic/dp/B00IRMGF2AI]

What can we do?

What can we do?

Avoid 3 common failures:

1. Organization has no **formal policy**. Thus, personnel cannot consistently make necessary decisions.
2. Organization has no **reasonable response** plans for violations, incidents, and disasters.
3. Plans don't work when needed because they haven't been regularly **tested**, updated, and rehearsed. (e.g., failure of operational security)

[Spafford]

Slide taken from Dr. Cheng

What can we do?

Build in security from the start

- Have a plan, think about your system and how security can be implemented.
- Understand differences in your security policy
- When something occurs, how do we handle the situation?

[Spafford, https://www.etsy.com/listing/1239850637/fire-safety-fire-drill-routine-classroom]

Pause: What about patches?

What are patches used for?

- Bug-fixes, improvements, new features, security fixes, updating our system

These are fixes for emergency situations

- They should **not be** relied upon
- Why?
  - Can cause further issues
  - User can ignore if too frequent (or any other reason)

Pause: What about patches?

How do we avoid using patches?

- Goal should be **design**, not patch
- You need to define in original design
- Be preventative and plan! We do not want to play catch up.
- A “band-aid solution” can only take you so far

[Spafford]

[https://www.connectwise.com/blog/cybersecurity/why-is-a-patch-management-solution-important-for-cybersecurity]

What can we do?

Capture requirements for design and validation

- Validate and verify
- Need a good grasp of our requirements
  - What about your projects?

Design with care using good tools and methods

- Be proactive, think about strategies prior to implementation

[Spafford]

Slide taken from Dr. Cheng

What can we do?

Understand the users

- What is the asset that needs to be protected for the users?
  - Narrow focus better than broad, expanding capabilities too much can cause some issues
- Understand that there is no “average user”
  - Account for different types of users
    - How does this alter how we think about the project?

[Spafford, https://www.ivanti.com/blog/user-education-cybersecurity-yes-worth]

Pause: Can security impact the user experience?

Yes! We need to be careful.

- Do not want to deter users from using our product
  - Two-factor authentication?

The software should still be

- Easy to use, false alarms should be avoided
- Frequent changes and updates are bad (can cause more issues)
- Should not require great expertise to get correct usage

[Spafford]

What can we do?

Understand balance between features and security

- Find the middle ground between safety and customer satisfaction.
- Manage complexity and change
  - Easy to test/verify its strength, fewer flaws
- Design of security should be as small and simple as needed

Employ better testing

- We have lots of tools to help with testing now
  - Could we use AI?

[Spafford]

What can we do?

The Principle of open design

- Our security mechanism should not be a secret!
  - Why?
    - Experts can review and point to flaws
    - Reverse engineering can expose your software
    - You will not know if your software have been compromised

Slide taken from Kira Chan

What can we do?

Set security goals

Confidentiality: Assets are accessible only by authorized parties

- Read-type access: read, view, print, existence secrecy and privacy

Integrity: Modified only by authorized parties in authorized ways

- Modification: write, change, change status, delete, create

Availability: Assets accessible to authorized parties

[Spafford]

Slide taken from Dr. Cheng

What can we do?

Set security goals

Consistency: The property to ensure that a consistent view of each data item is shown to every user

Control: The processes in place to protect from dangerous network vulnerabilities and data hacks

Audit: A comprehensive analysis and review of your IT infrastructure

[Spafford]

Slide taken from Dr. Cheng

What can we do?

[https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA]

What can we do?

Seek good security means

1. Limiting what happens
2. Limiting who can make it happen
3. Limiting how it happens
4. Limiting who can change the system

[Spafford]

Slide taken from Dr. Cheng

What can we do?

Set a security plan

1. Risk assessment
2. Cost-benefit analysis
3. Creating policies to reflect your needs
4. Implementation
5. Audit and incident response

Slide taken from Dr. Cheng

What can we do?

Know when software is secure

- Does not disclose information
- Does not allow unauthorized access
- Does not allow unauthorized change
- Maintains quality of service despite input and load
- Preserves audit, authenticity, control
- No surprises!

[Spafford]

Slide taken from Dr. Cheng

Threat Types

Types of Threats

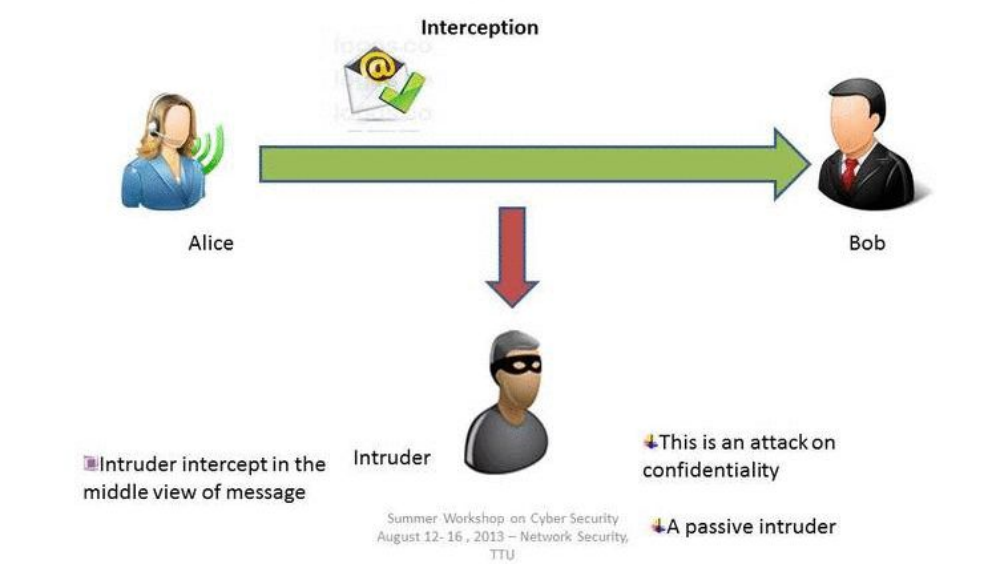
The basic types of threats are:

- Interception
- Interruption
- Fabrication
- Modification

Types of Threats

Interception

- Copying files, packet sniffing, wiretapping, eavesdropping

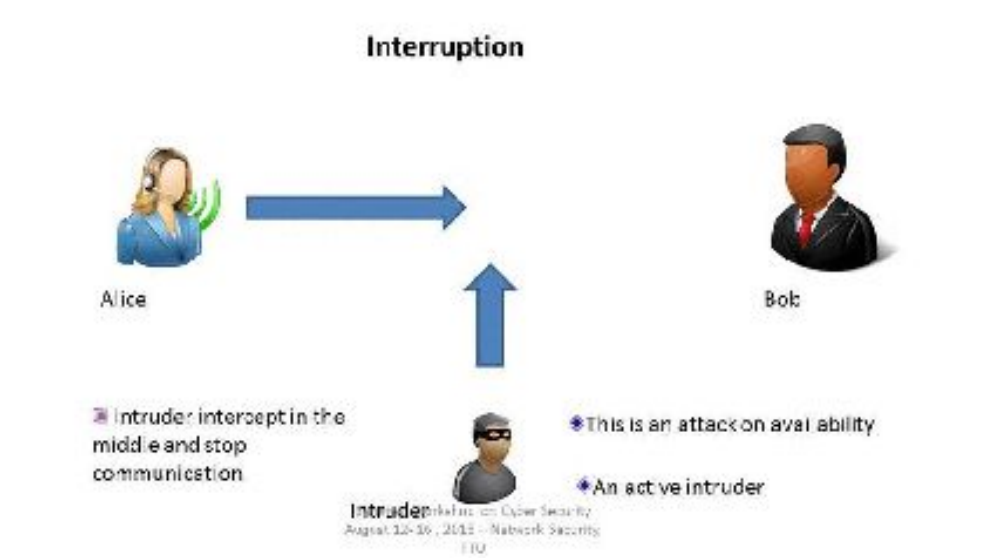


https://eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.4_Attacks_-_Types_of_Attacks

Types of Threats

Interruption

- Severing a communication line, DDoS, destroying software/hardware

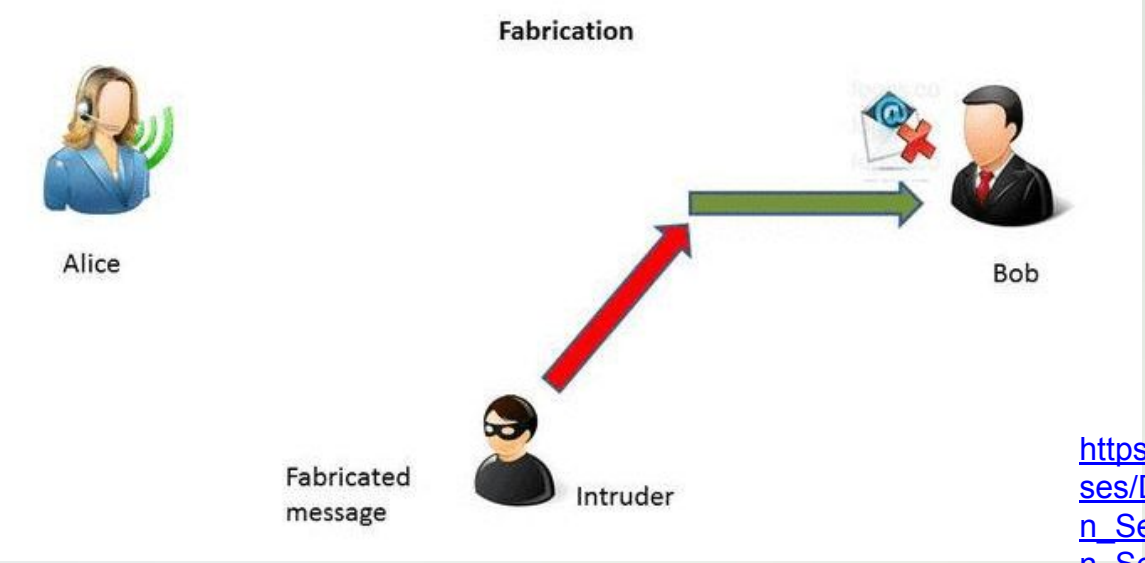


https://eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.4_Attacks_-_Types_of_Attacks

Types of Threats

Fabrication

- Spoofing, user falsification, SQL injection,
- email spoofing

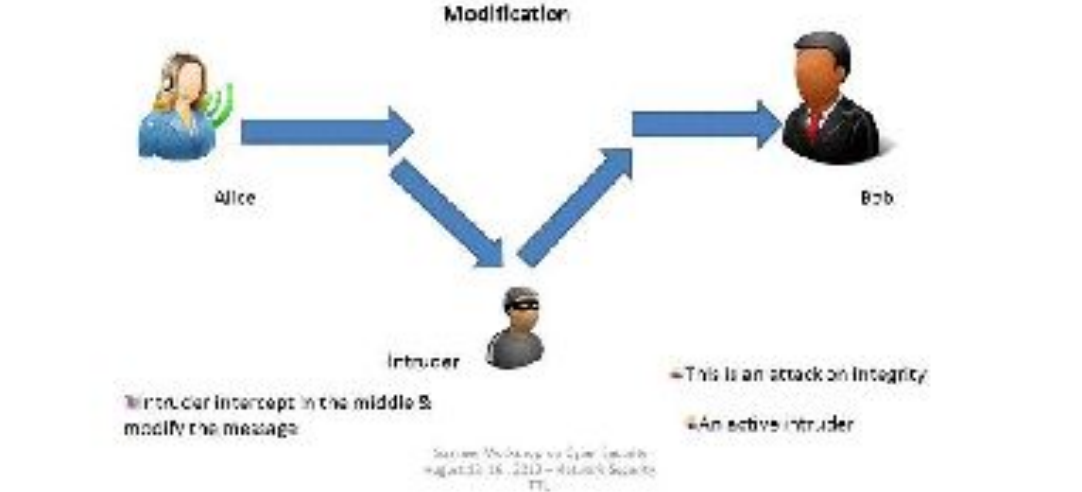


https://eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.4_Attacks_-_Types_of_Attacks

Types of Threats

Modification

- Changing files, reconfigure hardware, altering programs



https://eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.4_Attacks_-_Types_of_Attacks

Sample Attacks

DDoS Attack

Distributed denial of service attack (DDoS)

- The goal is to deny users access to a given website, resource, etc.
  - The **availability** is being attacked
  - Attempt to floods a server with traffic
  - Often uses multiple connected devices (botnets, can be coordinated)

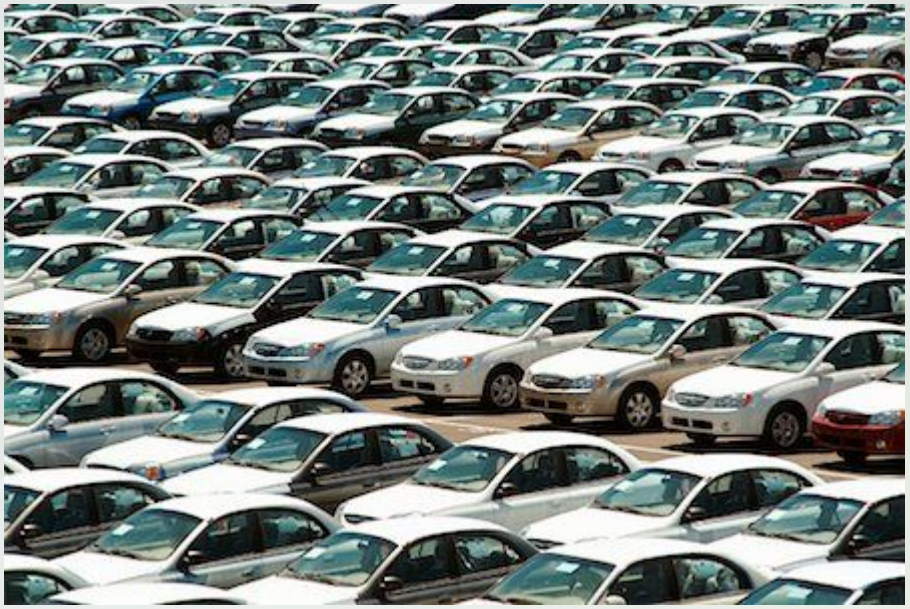
DDoS Attack - Example

Simple Parking Lot (from Kira Chan)

- Want to go to the mall, but we need to park in the lot first
  - Each parking spot (socket) can hold 1 car (computer)
- No fee or registration
- Let anyone in when they show up at the gate
- Only one car can pass through the gate at a time

DDoS Attack - Example

A bunch of cars (same model, year, and color) flood the lot and take all the spots



https://www.masterfile.com/search/en/parking+lot+with+the+same+cars

DDoS in AVs

CAN-Bus (Controller Area Network)

- Enables communication between different ECU's (Electrical Control Units) on the vehicle
- The data being sent along the CAN-Bus contains information for different subsystems
  - What if we flooded the system?
    - Stop communication between safety-critical systems
    - We could lose functionality of entire subsystems

[https://journal-home.s3.ap-northeast-2.amazonaws.com/site/2020kics/presentation/0128.pdf]

DDoS Defense

What is the problem with defending DDoS Attacks?

- High volumes of traffic may be real.
  - Amazon on cyber monday, Ticketmaster with any Taylor Swift Concert, etc., NFL Sunday ticket on first week of the season

Here are some ways to defend:

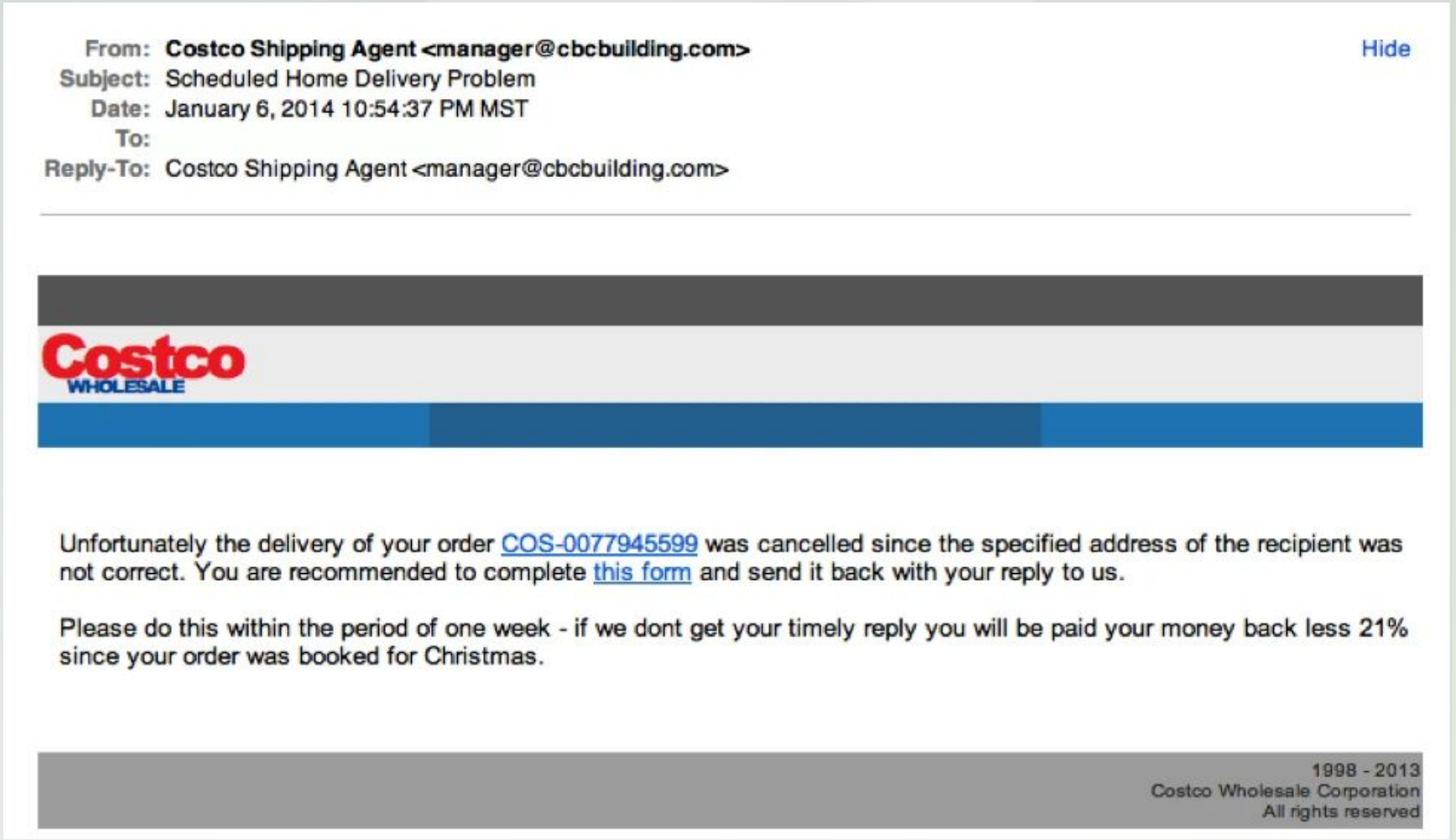
- Defenses at multiple layer
  - TCP connections: use modified TCP connection code.
    - Use TCP syn cookies
    - Drop an entry for incomplete connection from TCP connection table when overflowing
  - Use of captcha
  - Rate Limiting
    - Amount of requests in a certain window

Phishing Attack

Social engineering attack

- This is a type of attack that manipulates users to share or take actions they shouldn't
  - Phone calls, emails, texts, etc.
- The goal is to gain access or get users to compromise their own system
  - These can be very difficult to defend, why?
    - Often appear as a trusted source
      - Time is running out, reset your password soon
    - Spear-phishing: email specifically crafted for a target

Phishing Attack



From: **Costco Shipping Agent <manager@cbcbuilding.com>** Hide
Subject: Scheduled Home Delivery Problem
Date: January 6, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent <manager@cbcbuilding.com>

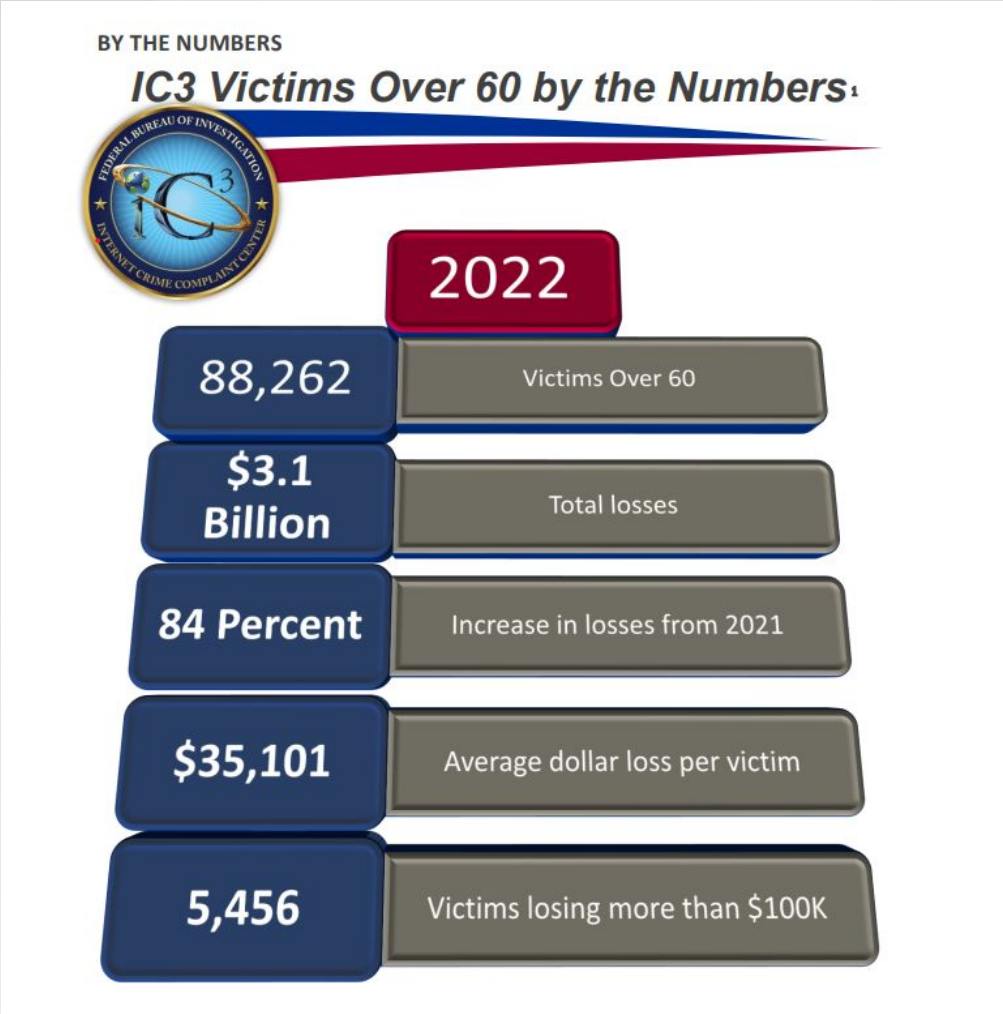
Costco WHOLESALE

Unfortunately the delivery of your order COS-0077945599 was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

Please do this within the period of one week - if we dont get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.

https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

Phishing Attack



https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf

Phishing in AVs

Who could be targeted for phishing attacks? Why is this problematic?

- Example, CD is corrupted
  - Present the user with a cryptic message, if appropriate button is not pressed
  - Reflash software on-board

S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, et al., “Comprehensive experimental analyses of automotive attack surfaces.,” in USENIX Security Symposium, San Francisco, 2011.

Phishing defense

The more we know, the better we can defend against these types of attacks

- Check domain name of email (e.g. www.chasebank.com, no-reply@bank.xyz.com)
- “We will never ask for your password” from companies, be aware
- Call company phone number before responding to “urgent” emails
- Reset passwords through the official website
- Do not click links, or proceed carefully

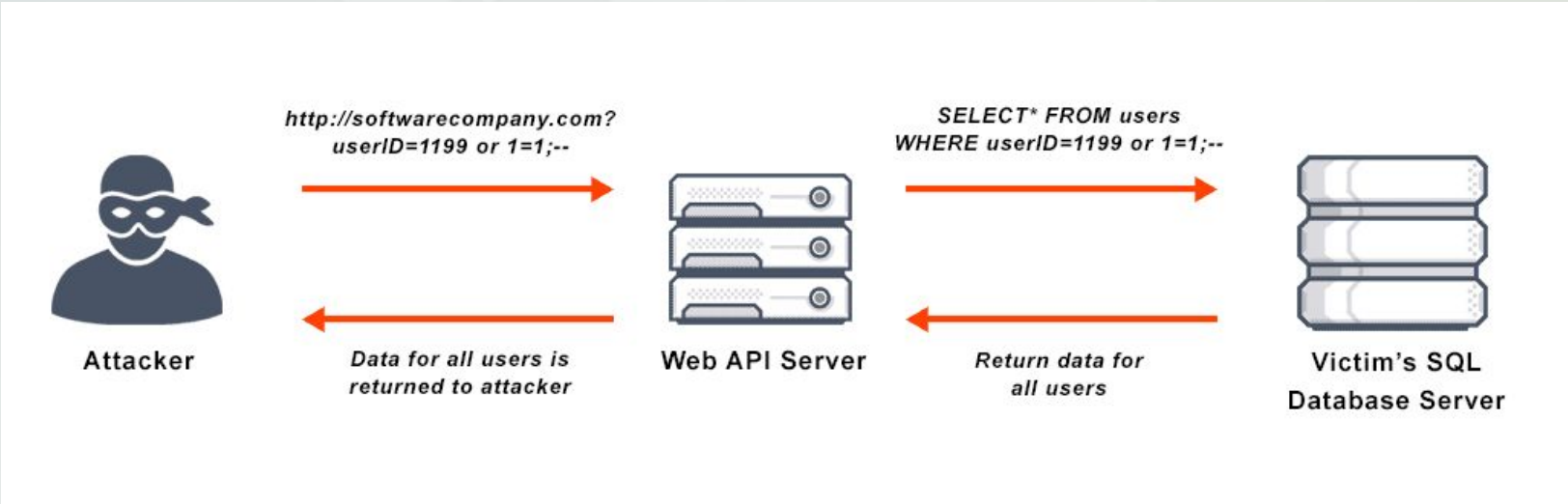
What is the challenge with implementing these defenses?

Slide taken from Kira Chan

SQL Injection attack

User enters code into the input boxes of an application and that code is executed by the application

- The damage may vary from unauthorized login, changes to table, or even drop tables
  - As of 2017, 51% of cyber attacks on web apps are from SQLi



https://www.akamai.com/de/de/multimedia/documents/state-of-the-internet/q2-2017-state-of-the-internet-security-report.pdf
https://avinetworks.com/glossary/sql-injection-attack/

SQL Injection attack

Turkish government

- Attackers used an SQLi attack to breach the system and drop debt data from other agencies

GhostShell attack

- APT group Team GhostShell targeted 53 universities using SQL injection stole and published 36,000 personal records belonging to students, faculty, and staff.

7-11

- 130 million credit card numbers were stolen by a group of attackers using SQLi attack

https://brightsec.com/blog/sql-injection-attack/#:~:text=7%2DEleven%20breach%E2%80%94a%20team,the%20IT%20security%20company's%20website.

SQL Injection in AV's

What types of damage could be done with this attack in vehicles?

This was attempted:

- SQLi attacks to clear user data from people who speed
- The goal is to have a simple statement written for when a license plate is flagged as "speeding", the SQL statement deletes the entry from the table.

https://www.cpr.org/2022/09/16/colorado-speed-cameras-traffic-bill/

SQL Injection defense

Have a cybersecurity plan, assume the worst

Sanitize input (a function provided by php)

- consists of removing any unsafe characters from user inputs

Make sure that input conforms to expected input

Parameterized queries

- Separates the query from user inputs
  - The user input values are passed as parameters
- The database will distinguish between code and data, regardless of is input.

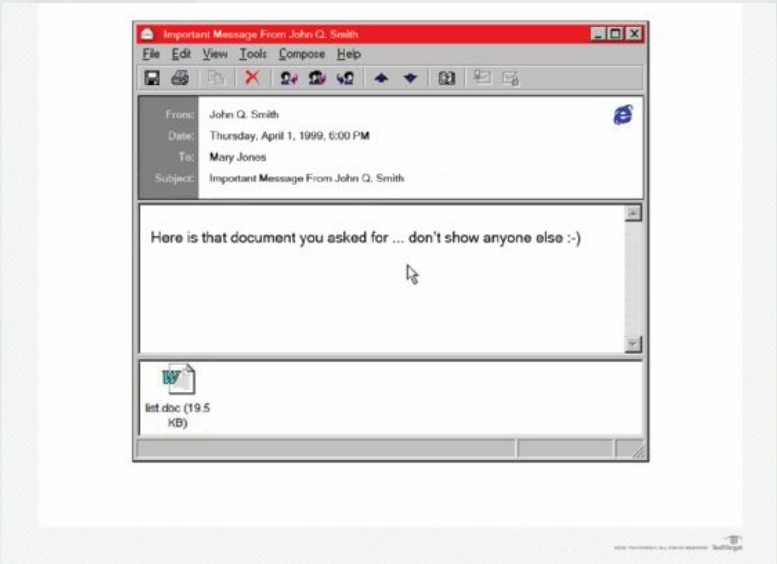
Malware

Virus

This operates similar to a virus in people

Needs a host to infect (usually executable) and when attached to an executable (.exe file), a virus can do a number of things

- Cause damage to data or software
- Can spread to other computers

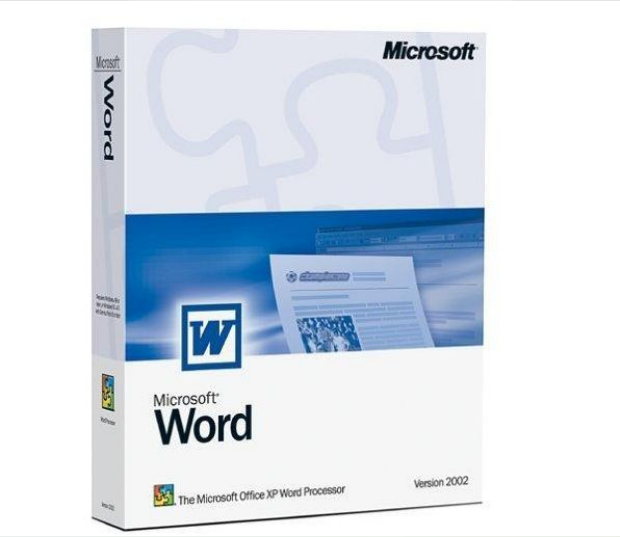


https://www.techtarget.com/searchsecurity/definition/Melissa-virus

Virus

The Melissa Virus

- Spotted in March 1999, spreading to the public via internet forums / emails
- It was a word document, that when opened executed the malicious code
  - If macros were enabled, spread itself to first 50 contacts in Outlook

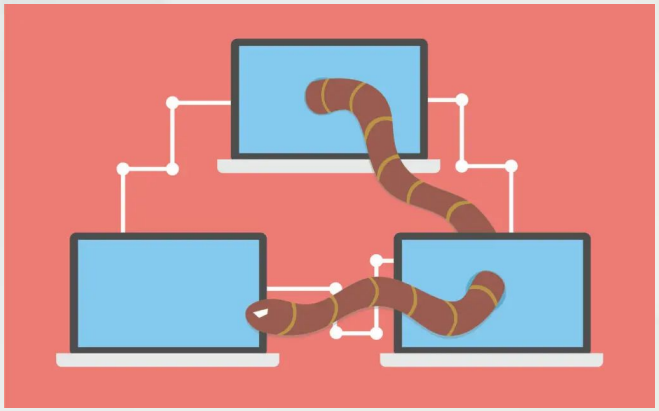


https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/

Worm

This is similar to a virus in the way that it spreads

- Standalone program
- Replicates itself in order to spread to other computers via the network
- The computers act as a “host”, actively attempting to “transmit” to other machines



https://cyberhoot.com/cybrary/worm/

Worm - Example

Morris Worm

- 1988, written by Robert Morris (student at Cornell) to highlight security flaws of the internet
  - Was **not** meant to be an actual attack
- Worm infects same computer multiple times which caused a fork bomb resulting in a denial of service attack
- Spread through the US and took down the entire internet
- 6000 computers were reportedly affected causing an estimated $10-$100 million dollars in repair bills

https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/

Before we continue...

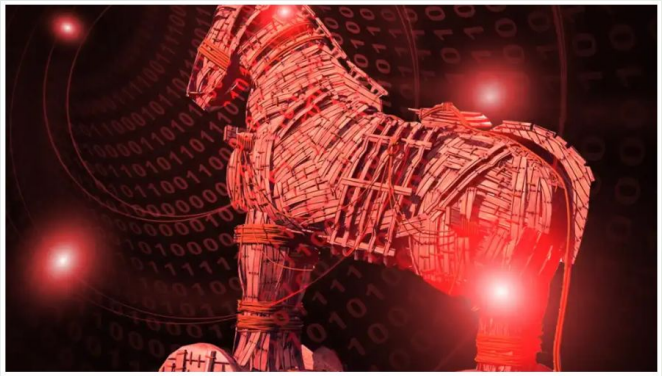
Fun trivia: “The Worm Before Christmas”

- https://www.networkworld.com/article/747474/security-the-worm-before-christmas-1988.html
  - Written by Dr. Cheng and some colleagues.

Trojan Horse

A Trojan horse typically pretends to be a standard program, but misleads users of its true intent of damaging the system

- Inspired by the Greek story of the fall of Troy
- Typically has an aspect of social engineering in these types of attacks



https://www.csoonline.com/article/567385/what-is-a-trojan-horse-how-this-tricky-malware-works.html

Trojan Horse

ILOVEYOU

- Technically a virus, but the way it was delivered was like a trojan horse
- 2000 that was an email attachment with the subject line “ILOVEYOU.”
- If opened, spread to every contact in a user’s Microsoft Outlook address book
- Also started overwriting certain files (e.g., JPEG and MP3 files) from the hard drive
- $80 million in damages
- David Smith was the creator, arrested and sentenced to 20 months in prison.

https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/

Bots

Usually created from a worm and is comprised of a compromised computer

Botnet: a network of compromised computers

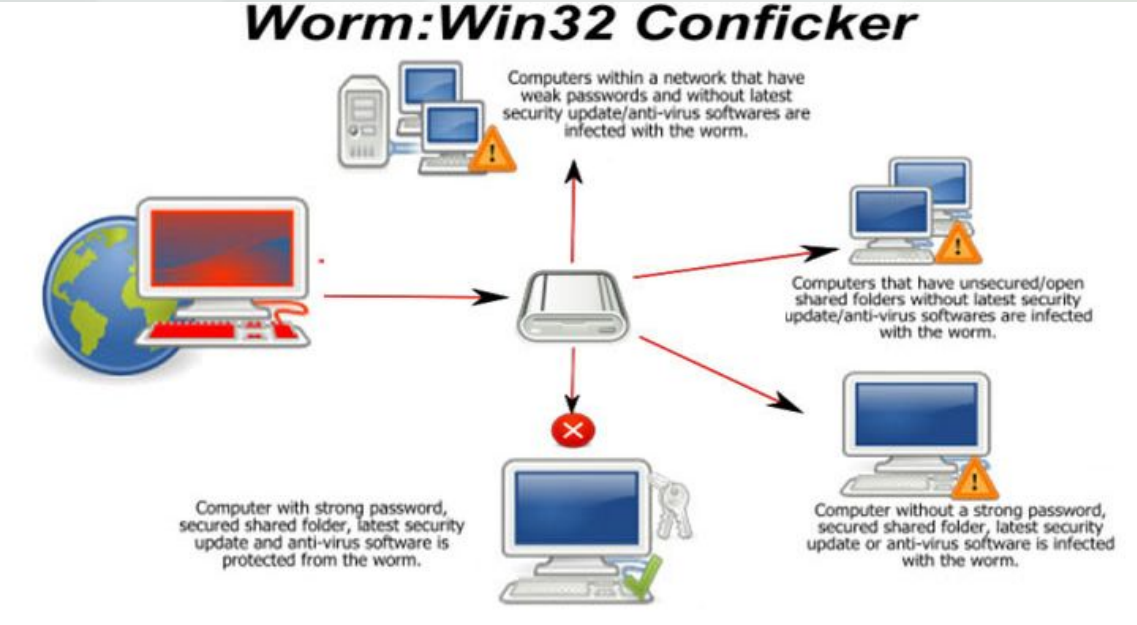
- Attackers can send commands to them

Slide taken from Kira Chan

Bots

Conflicker worm

- Infects a computer
- Computer then takes commands from some central location
- 10,500,000+ infected (source)



https://archive.f-secure.com/weblog/archives/00001584.html
https://www.cybereason.com/blog/what-is-the-conficker-worm

Slide taken from Kira Chan

Ransomware

The goal is to block access to the victim's personal data or files, unless a ransom is paid

- The attacker typically encrypts the files and demanding payment, this prevents users
- The ransom itself is typically for a decryption key

https://kinsta.com/knowledgebase/what-is-encryption/

Ransomware

WannaCry

- May 2017, 250,000 users of Microsoft Windows users across 150 countries.
- $4 billion in damages

McLaren Health Care

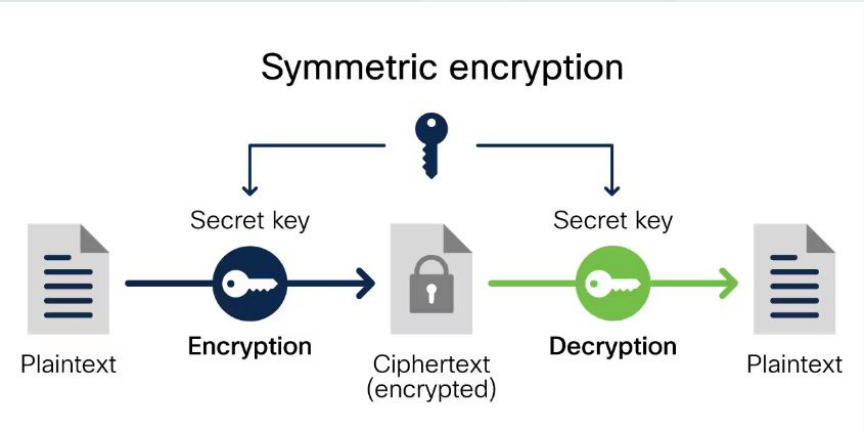
- October 2023
- 6 terabytes of data from 2.5 million patients

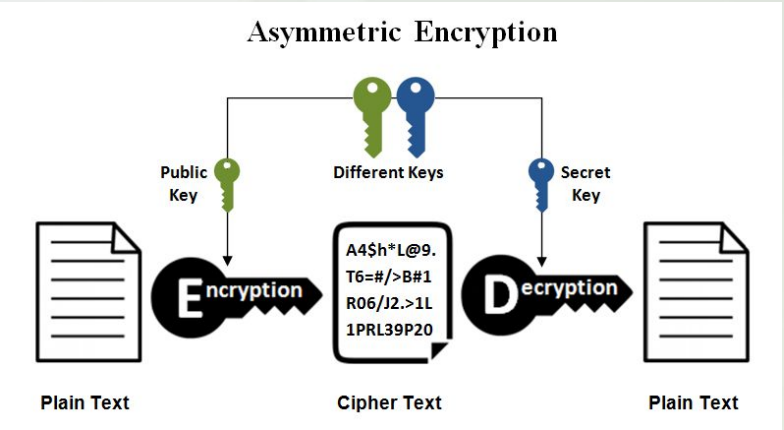
https://www.healthcareitnews.com/news/wannacry-timeline-how-it-happened-and-industry-response-ransomware-attack

Pause: Encryption

What is it?

- The goal of encryption is to make data unreadable, encoded, or “secret” to unauthorized data.
- Plaintext data is passed through a mathematical model, the output is your encrypted data, and you need a decryption key to put it back into plaintext
- Symmetric (1 key), Asymmetric (2 keys)
- **Why could this cause problems for your AV systems?**





https://www.cisco.com/c/en/us/products/security/encryption-explained.html
https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Pause: Malware and AV's

What could go wrong with malware and vehicles? Why?

Risk Assessment

Risk Assessment

Three questions to answer:

1. What am I trying to protect (asset)?
2. What do I need to protect against (threats)?
3. How much time, effort and money am I willing to expend to obtain adequate protection?

Three key steps:

1. Identify assets
2. Identify threats
3. Calculate risks

[Spafford]

Slide taken from Dr. Cheng

Risk Assessment

Tangibles

Computers, disk drives, proprietary data, backups and archives, manuals, printouts, commercial software distribution media, communications equipment & wiring, personnel records, audit records

Intangibles

Safety & health of personnel, privacy of users, personnel passwords, public image & reputation, customer/client goodwill, processing availability, configuration information

[Spafford]

Slide taken from Dr. Cheng

Risk Assessment

What are some risks?

- Illness /loss of key people
- Loss of phone/network services
  - Key to a productive workday
- Loss of utilities (phone water, electricity) for a short or prolonged time
- Natural disaster
  - Lightening or flood
- Theft of disks, tapes, key person's laptop or home computer
- Introduction of a virus
- Computer vendor bankruptcy
- Bugs in software
- Subverted employees or 3rd party personnel
- Labor unrest
- Political terrorism
- Random "hackers"

Risk Assessment

Estimate likelihood of each threat occurring

- If an event happens on a regular basis, you can estimate based on your records
  - Power company: official estimate of likelihood for power outage during coming year
  - Insurance company: actuarial data on probabilities of death of key personnel based on age & health

[Spafford]

Slide taken from Dr. Cheng

Risk Assessment

Creating a policy

- Defines what you consider to be valuable and what steps should be taken to safeguard those assets
  - States the responsibility for that protection.
  - Provides grounds upon which to interpret and resolve any later conflicts that might arise
- Policy should be general and change little over time
  - Should not list specific threats, machines or individuals by name

[Spafford]

Slide taken from Dr. Cheng

Key takeaways

1. Build security in from the start
2. Understand users
3. Design with care, and test
4. Find balance between features and security
5. Understand your threats
6. Use risk assessment tools

[Spafford]

Slide taken from Dr. Cheng

Key takeaways

4 Easy Steps to Security

1. Decide how important security is to your site
2. Involve and educate your user community
3. Devise a plan for making and storing backups of your system data
4. Stay inquisitive and suspicious

[Spafford]

Slide taken from Dr. Cheng

Thank You!

“The Worm Before Christmas”

By Clement C. Morris
(a.k.a. David Bradley, Betty Cheng, Hal Render, Greg Rogers, and Dan LaLiberte)

Twas the night before finals, and all through the lab
Not a student was sleeping, not even McNabb.
Their projects were finished, completed with care
In hopes that the grades would be easy (and fair).

The students were wired with caffeine in their veins
While visions of quals nearly drove them insane.
With piles of books and a brand new highlighter,
I had just settled down for another all nighter —

When out from our gateways arose such a clatter,
I sprang from my desk to see what was the matter;
Away to the console I flew like a flash,
And logged in as root to fend off a crash.

The windows displayed on my brand new Sun-3,
Gave oodles of info — some in 3-D.
When, what to my burning red eyes should appear
But dozens of “nobody” jobs. Oh dear!

With a blitzkrieg invasion, so virulent and firm,
I knew in a moment, it was Morris’s Worm!
More rapid than eagles his processes came,
And they forked and exec’ed and they copied by name:

“Now Dasher! Now Dancer! Now, Prancer and Vixen!
On Comet! On Cupid! On Donner and Blitzen!
To the sites in .rhosts and host.equiv
Now, dash away! dash away! dash away all!”

And then in a twinkling, I heard on the phone,
The complaints of the users. (Thought I was alone!)
“The load is too high!” “I can’t read my files!”
“I can’t send my mail over miles and miles!”

I unplugged the net, and was turning around,
When the worm-ridden system went down with a bound.
I fretted. I frittered. I sweated. I wept.
Then finally I core dumped the worm in /tmp.

It was smart and pervasive, a right jolly old stealth,
And I laughed, when I saw it, in spite of myself.
A look at the dump of that invasive thread
Soon gave me to know we had nothing to dread.

The next day was slow with no network connections,
For we wanted no more of those pesky infections.
But in spite of the news and the noise and the clatter,
Soon all became normal, as if naught were the matter.

Then later that month while all were away,
A virus came calling and then went away.
The system then told us, when we logged in one night:
“Happy Christmas to all! (You guys aren’t so bright.)”

Acknowledgements

- Gene Spafford
- Annie Anton
- Charles Pfleeger
- Marilyn Wulfekuhler