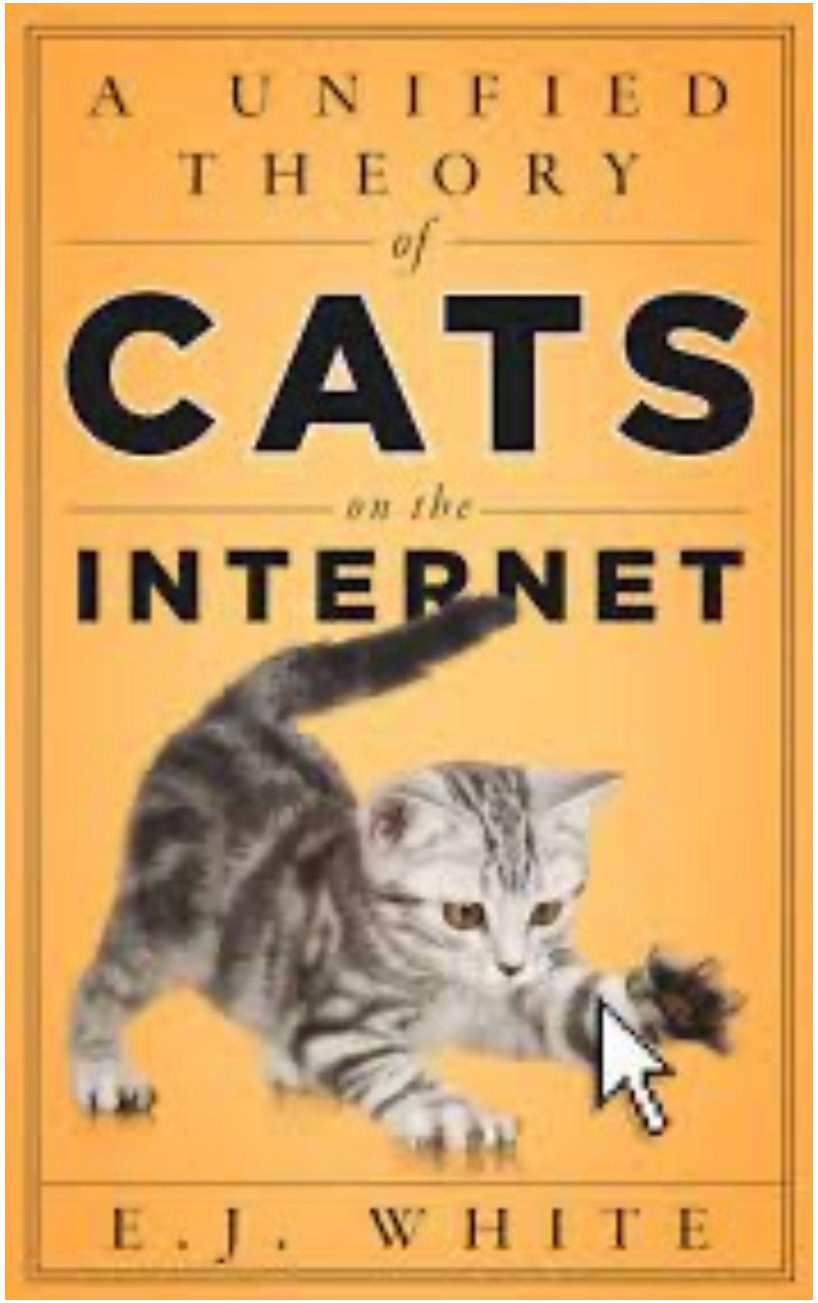
SEC_RITY IS NOT COMPLETE WITHOUT U!

Lecture 3: Is it possible to make software, hardware, and networks secure?

- White, E.J.. *A Unified Theory of Cats on the Internet*, Redwood City: Stanford University Press, 2020. https://doi.org/10.1515/9781503614031



UKRAINE UPDATE

- Tripwire for real war? Cyber's fuzzy rules of engagement (APnews) https://apnews.com/article/russia-ukraine-joe-biden-technology-business-hacking-5eadc06062f8c7acfc7b7302ec4c4478

- In November, Ukraine exposed an eight-year espionage operation by agents of Russia's FSB in Crimea involving more than 5,000 attempted hacks. The main goal: to gain control over critical infrastructure, including power plants, heating and water supply systems. Ukraine's state news https://www.ukrinform.net/rubric-crime/3344830-sbu-identifies-fsb-hackers-behind-over-5000-cyberattacks-on-ukraine-govt-agencies.html

WEEK 3:IS IT POSSIBLE TO MAKE SOFTWARE, HARDWARE, AND NETWORKS SECURE?

1. Tips and Hints for Secure Computing a) browser, b) Network, c) Computer, d) Email, e) Misinformation and Fake News [2-11]
2. The fallibility of humans? Errors, Vulnerabilities [13-22]

a) What does theory tell us? Undecidability, Termination [23-23]

3. Encryption [25-35]

a) Encryption: its uses and abuses.[36-54]

4. Appendix Protect YOURSELF AGAINST CYBERATTACKS [58-End]

1. GOVERNMENT WEBSITES FOR CYBERSECURITY

Cybersecurity
Infrastructure Security
Emergency Communications
National Risk Management

CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY

Includes a wealth of tips on how to keep your home safe
https://www.cisa.gov/tips/

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY WEBSITE CONTENTS

Threats

- Protecting Against Ransomware
- Protecting Against Malicious Code
- Handling Destructive Malware
- Dealing with Cyberbullies
- Understanding Denial-of-Service Attacks
- Avoiding Social Engineering and Phishing Attacks
- Preventing and Responding to Identity Theft

Email and Communication

- Staying Safe on Social Networking Sites
- Understanding Digital Signatures
- Using Caution with Email Attachments
- Reducing Spam

General Security Information

- Proper Disposal of Electronic Devices
- Defending Against Illicit Cryptocurrency Mining Activity
- Securing Network Infrastructure Devices
- Securing the Internet of Things
- Home Network Security
- Preparing for Tax Season
- Keeping Children Safe Online
- Understanding Firewalls for Home and Small Office Use
- Good Security Habits

Mobile Devices

- Privacy and Mobile Device Apps
- Holiday Traveling with Personal Internet-Enabled Devices
- Cybersecurity for Electronic Devices
- Using Caution with USB Drives
- Securing Wireless Networks

Privacy

- Supplementing Passwords
- Protecting Your Privacy
- Choosing and Protecting Passwords

Safe Browsing

- Shopping Safely Online
- Understanding Bluetooth Technology
- Understanding Website Certificates

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY WEBSITE CONTENTS

Software and Applications

- Understanding Patches and Software Updates
- Website Security
- Securing Enterprise Wireless Networks

Archive

- Before You Connect a New Computer to the Internet
- International Mobile Safety Tips
- Protecting Portable Devices: Physical Security
- Understanding Hidden Threats: Rootkits and Botnets
- Understanding ISPs
- Identifying Hoaxes and Urban Legends
- Understanding Hidden Threats: Corrupted Software Files
- Debunking Some Common Myths
- Understanding Voice over Internet Protocol (VoIP)
- Recognizing Fake Antiviruses
- Real-World Warnings Keep You Safe Online
- Effectively Erasing Files
- How Anonymous Are You?
- Risks of File-Sharing Technology
- Reviewing End-User License Agreements
- Avoiding Copyright Infringement
- Understanding Your Computer: Email Clients
- Understanding Your Computer: Web Browsers
- Understanding Your Computer: Operating Systems
- Protecting Portable Devices: Data Security
- Understanding Encryption
- Recognizing and
- Avoiding Spyware
- Using Instant Messaging and Chat Rooms Safely
- Benefits of BCC
- Understanding Anti-Virus Software
- Understanding Internationalized Domain Names
- Benefits and Risks of Free Email Services
- Recovering from Viruses, Worms, and Trojan Horses
- Evaluating Your Web Browser's Security Settings
- Browsing Safely: Understanding Active
- Content and Cookies
- Safeguarding Your Data
- Defending Cell Phones and PDAs Against Attack

1A) SECURING THE BROWSER

- https://www.cisa.gov/uscert/publications/securing-your-web-browser
- Microsoft Internet Explorer (IE) is a web browser integrated into the Microsoft Windows operating system. For up-to-date information on security and privacy settings for Internet Explorer, visit http://windows.microsoft.com/en-us/internet-explorer/ie-security-privacy-settings.
- Mozilla Firefox is a popular third-party browser for Windows, Mac, and Linux. To learn how to keep your information safe and secure with Firefox's private browsing, password features and other security settings, visit https://support.mozilla.org/en-US/products/firefox/privacy-and-security.
- Apple Safari is installed on its line of computers, tables, and phones. For information on the Safari's security settings on Apple devices, visit https://support.apple.com/en-us/HT201265. For information on Safari installed on computers, visit http://help.apple.com/safari/mac/8.0/ and select "Privacy and security" on the menu.
- In 2012, Google Chrome became the most widely used browser worldwide, according to Stat Counter and other sources. For more information on Chrome's security, safety and reporting features, visit https://support.google.com/chrome#topic=3421433 and select the options displayed under the topic.

THE BROWSER SECURITY SETTINGS

https://www.cisa.gov/uscert/ncas/tips/ST05-001

- ***Zones*** – Your browser may give you the option of putting web sites into different segments, or zones, and allow you to define different security restrictions for each zone: ***Internet, Local intranet, Trusted sites, Restricted sites. JavaScript – Java and ActiveX controls***
- ***Plug-ins*** – Sometimes browsers require the installation of additional software known as plug-ins to provide additional functionality. Plug-ins may be used in an attack, so before installing them, make sure that they are necessary and that the plugin download site is trustworthy.
- ***Manage cookies*** – You can disable, restrict, or allow cookies as appropriate. Generally, it is best to disable cookies and then enable them if you visit a site you trust that requires them (see Browsing Safely: Understanding Active Content and Cookies for more information).
- ***Block pop-up windows*** – Although turning this feature on could restrict the functionality of certain web sites, it will also minimize the number of pop-up ads you receive, some of which may be malicious (see Recognizing and Avoiding Spyware for more information).

1B) BEFORE YOU CONNECT A NEW COMPUTER TO THE INTERNET

https://www.cisa.gov/uscert/ncas/tips/ST15-003

Secure your router. (See Securing Your Home Network for more information.

Enable and configure your firewall. Refer to your router's user guide for instructions on how to enable your firewall and configure the security settings. Set a strong password to protect your firewall against unwanted changes.

Install and use antivirus software. Be sure to install the software from a reputable source, such as the vendor's website.

Remove unnecessary software. Intruders can attack your computer by exploiting software vulnerabilities, so the fewer software programs you have installed, the fewer avenues there are for potential attack. Remove any software you feel isn't necessary after confirming it's safe to remove. Back up important files and data before removing unnecessary software to prevent accidentally removing programs that turn out to be essential to your OS.

1B) BEFORE YOU CONNECT A NEW COMPUTER TO THE INTERNET PART 2

Modify unnecessary default features. Like removing unnecessary software, modifying or deleting unnecessary default features reduces attackers' opportunities. Review the features that are enabled by default on your computer, and disable or customize those you don't need or don't plan on using.

Operate under the principle of least privilege. In most instances of malware infection, the malware can operate only using the privileges of the logged-in user. To minimize the impact of a malware infection, consider using a standard or restricted user account (i.e., a non-administrator account) for day-to-day activities. Only log in with an administrator account—which has full operating privileges on the system—when you need to install or remove software or change your computer's system settings.

Apply software updates and enable automatic updates. Only download software updates directly from a vendor's website, from a reputable source, or through automatic updates.

1C) EMAIL ATTACHMENTS

Trust your instincts. If an email or email attachment seems suspicious, don't open it, even if your antivirus software indicates that the message is clean.

Save and scan any attachments before opening them. If you have to open an attachment before you can verify the source, take the following steps:

- Be sure the signatures in your antivirus software are up to date.
- Save the file to your computer or a disk.
- Manually scan the file using your antivirus software.
- If the file is clean and doesn't seem suspicious, go ahead and open it.

Turn off the option to automatically download attachments. To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and make sure to disable it.

Consider creating separate accounts on your computer. Most operating systems give you the option of creating multiple user accounts with different privileges. Consider reading your email on an account with restricted privileges. Some viruses need "administrator" privileges to infect a computer.

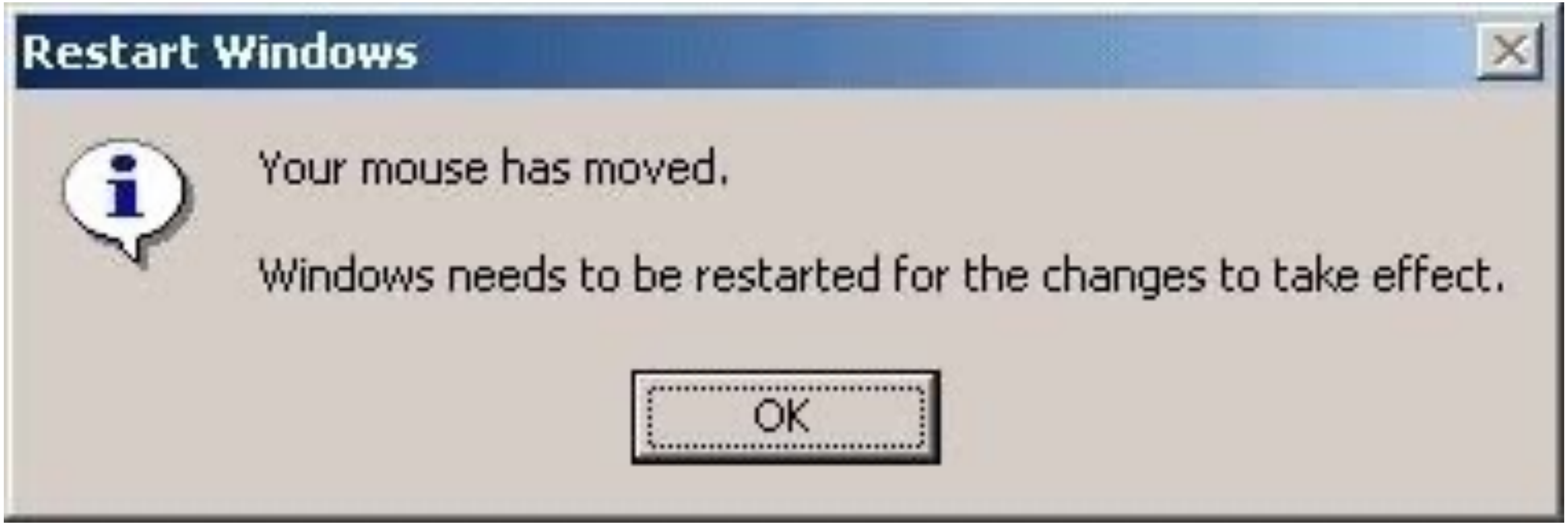
https://www.cisa.gov/uscert/ncas/tips/ST04-010

1D) COUNTERING ONLINE MISINFORMATION

- UNICEF RESOURCE PACK (p6-9) https://www.unicef.org/eca/media/13636/file
- EU Final report of the independent High Level Group on fake news and online disinformation https://www.ecsite.eu/sites/default/files/amulti-dimensionalapproachtodisinformation-reportoftheindependenthighlevelgrouponfakenewsandonlinedisinformation.pdf

- Phishing Prevention tips (Not a government site)
- https://usa.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips

JOKE



Restart Windows

Your mouse has moved.

Windows needs to be restarted for the changes to take effect.

2A) WHY DO WE TOLERATE HUMAN OVER MACHINE ERROR? Melanie Thomson

Research suggests that regardless of the activity or task:

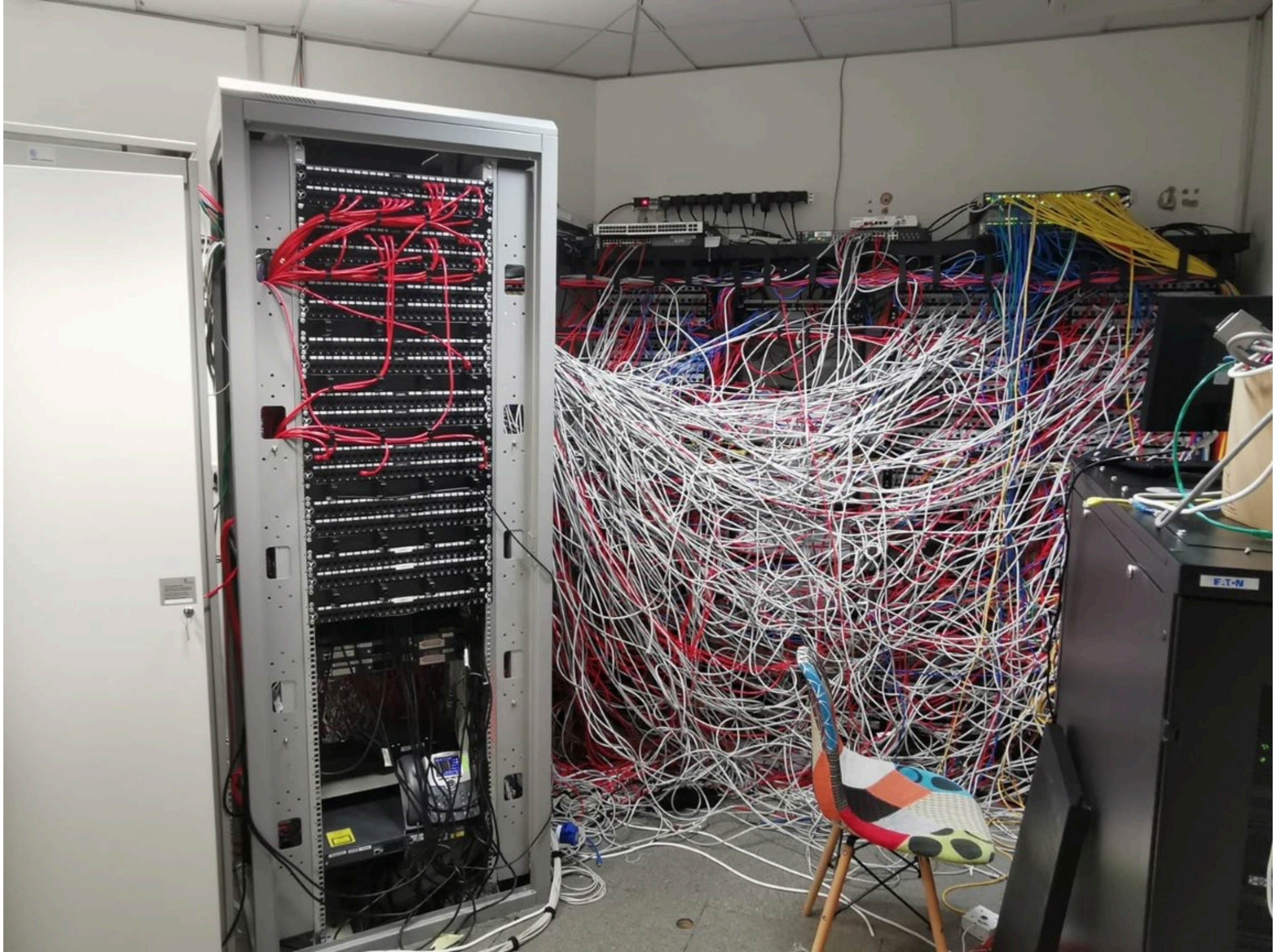
- Humans make ***3 to 6 errors per hour*** and on average:
- 50 errors per day (or at least, 'per work shift’). Graham Edkins[1]

We are more likely to forgive human error over machine – why?

- Making errors is an integral part of the way we humans live.
- Many believe that you cannot learn without making an error or two along the way.

It is okay for humans to make a mistake!!!.

[1] https://www.linkedin.com/pulse/human-factors-error-role-bad-luck-incident-graham-edkins/



EATON

VULNERABILITY OF LINES OF CODE

Major programming projects (likely written by expert programmers) found rates of major exploitable vulnerabilities at a rate of 0.003 to 0.08 per 1000 lines of code. (Or 1 per 12 500 - 300 000 lines of code).

CVE = Count of Exploitable Vulnerabilities. LoC = Lines of Code.

- ***Web Browsers:***

  Google Chrome 380 CVE with 6 239 930 LoC or ***0.06 vulnerabilities per 1000 lines of code***.

  Firefox 395 CVE in 8 000 969 LoC or ***0.05 vulnerabilities per 1000 lines of code.***

- ***Open source programming languages:***

  Python with 3 exploitable CVSS>=7) in 862 830 LoC or 0.003 ***vulnerabilities per 1000 lines of code.***

  Ruby 13 CVSS >= 7 in 171,122 LoC or 0.08 ***vulnerabilities per 1000 lines of code.***

  PHP with 122 exploitable CVSS>=7 in 3,761,587 LoC or 0.03 ***vulnerabilities per 1000 lines of code.***

- ***Web Frameworks:***

  django with 1 exploitable CVSS >= 7 in 149,292 LoC or 0.007 ***vulnerabilities per 1000 lines of code.***

  Ruby on Rails 7 exploitable CVSS >= 7 in 156,317 LoC or 0.05 ***vulnerabilities per 1000 lines of code.***

VULNERABILITIES PER OPERATING SYSTEM(1999-2022)

- https://www.cvedetails.com/top-50-products.php

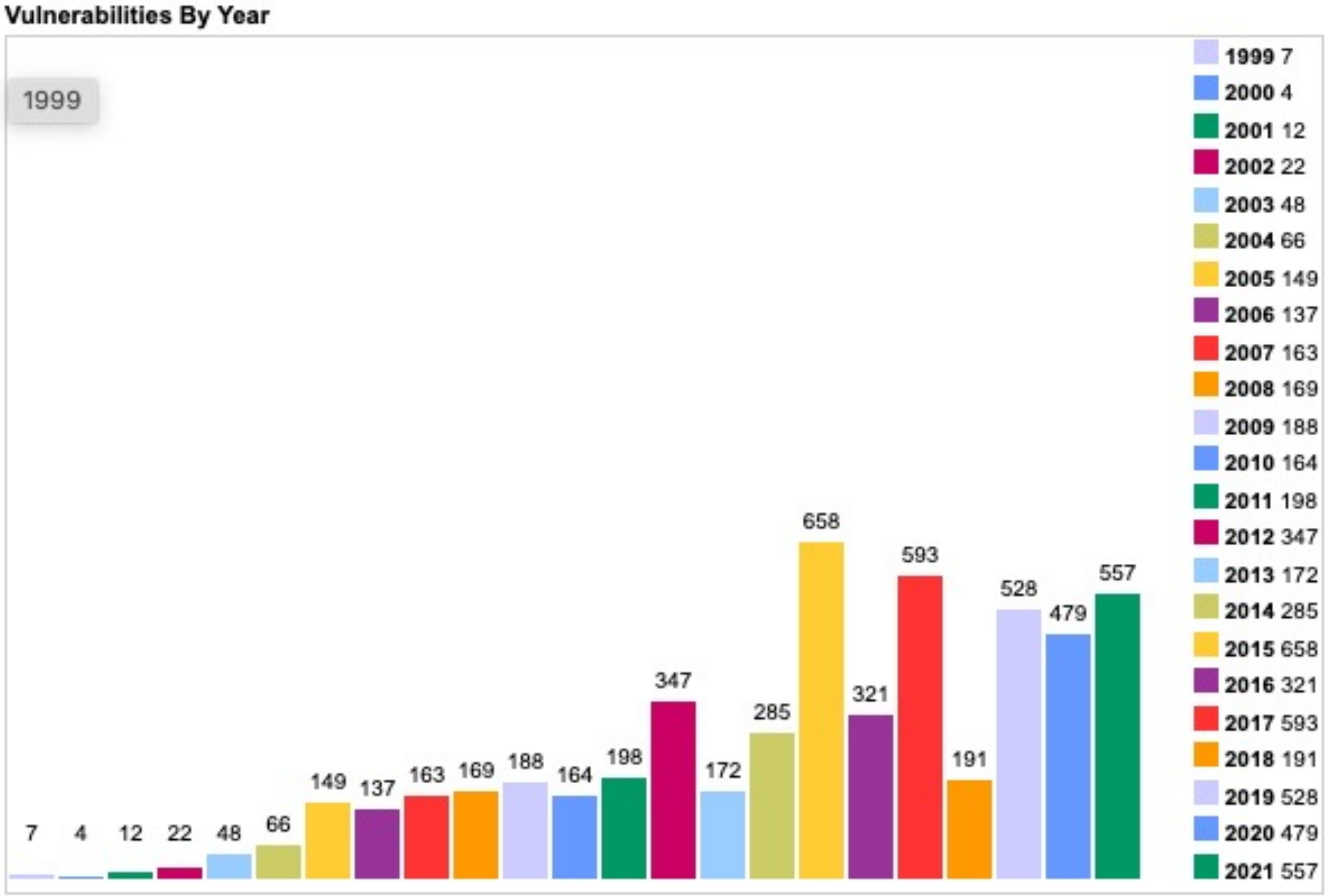
Operating System	*# Vulnerabilities*
Android	4043
Linux Kernel	2746
Mac Os X	2958
Windows 10	2569
Office	694

Top 50 by Vulnerabilities https://www.cvedetails.com/top-50-product-cvssscore-distribution.php

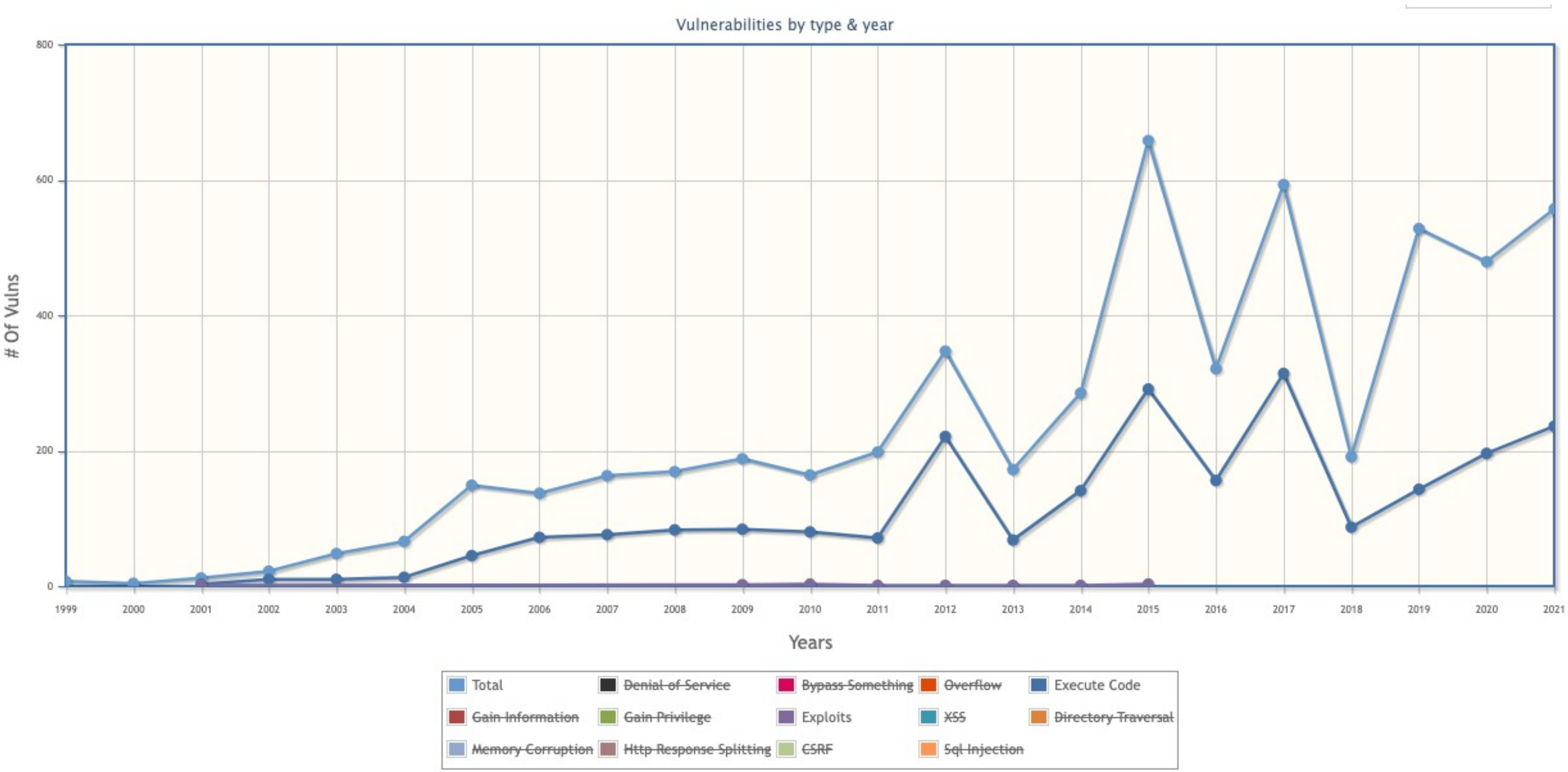
Apple Vulnerability Statistics over the Years

Year	*# Vulnerabilities*	*DoS*	*Code Execution*	*Overflow*	*Memory Corruption*	*Gain Privildges*		
1999	7	1						
2000	4	1		1				
2001	32	3	3	3		2		
2002	22	7	10	5		2		
2003	48	7	10	9		4		
2004	66	8	12	10		5		
2005	149	29	45	38	1	12		
2006	137	41	72	53	5	6		
2007	163	55	76	46	15	17		
2008	169	52	83	48	15	7		
2021	557	2052	2400	1740	1546	225		

APPLE VULNERABILITIES



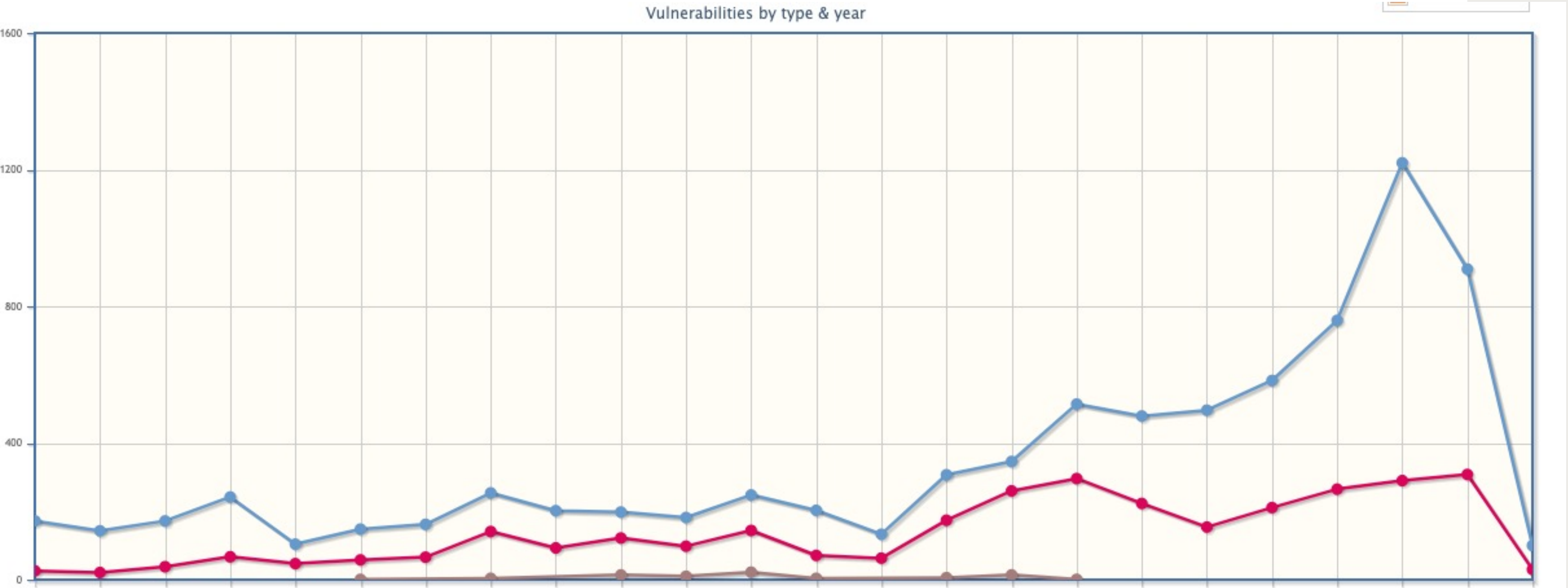
VULNERABILITIES PER YEAR APPLE EXECUTE CODE VULNERABILITIES



Microsoft Vulnerability Statistics over the Years

Year	*# Vulnerabilities*	*DoS*	*Code Execution*	*Overflow*	*Memory Corruption*	*Gain Privildges*		
1999	172	42	26	18				
2000	143	42		1				
2001	172	67	3	3		2		
2002	242	57	10	5		2		
2003	104	28	10	9		4		
2004	148	36	12	10		5		
2005	162	46	45	38	1	12		
2006	254	75	72	53	5	6		
2007	202	54	76	46	15	17		
2008	198	40	83	48	15	7		
2021	8276	1574	3266	1521	1303	663		

VULNERABILITIES PER YEAR MICROSOFT EXECUTE CODE VULNERABILITIES



DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

WHAT DOES THEORY TELL US?

- List of undecidable problems (Wikipedia). https://en.wikipedia.org/wiki/Undecidable_problem

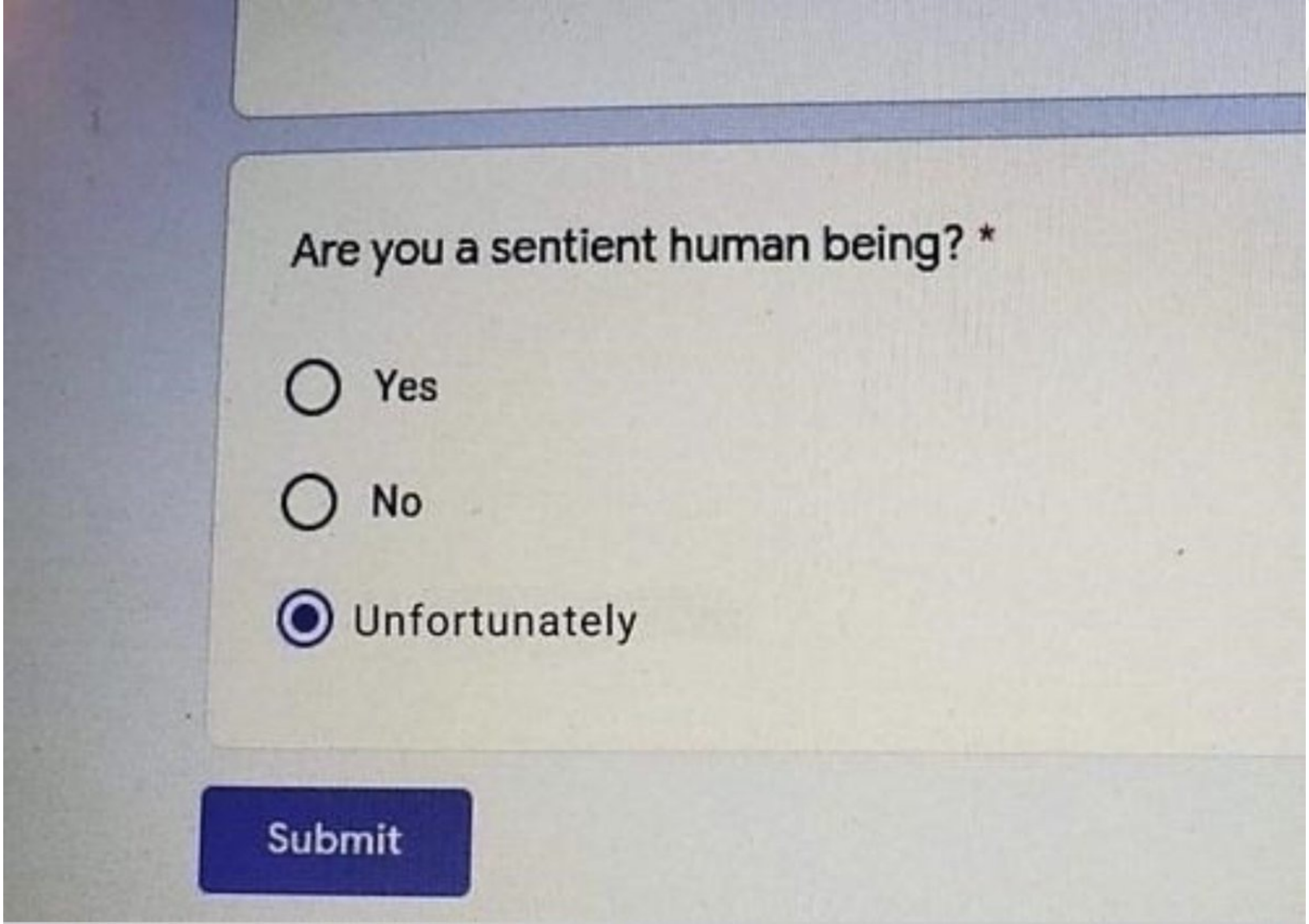
  The halting problem (determining whether a Turing machine halts on a given input)

  The mortality problem (determining whether it halts for every starting configuration).

  Rice's theorem states that all non-trivial semantic properties of programs are undecidable.

These problems are implied by Gödel's incompleteness theorems

- Incompleteness theorem 1) states that no consistent system of axioms whose theorems can be listed by an effective procedure (i.e., an algorithm) is capable of proving all truths about the arithmetic of natural numbers. For any such consistent formal system, there will always be statements about natural numbers that are true, but that are unprovable within the system.
- Incompleteness theorem 2), an extension of the first, shows that the system cannot demonstrate its own consistency.



Are you a sentient human being? *

○ Yes

○ No

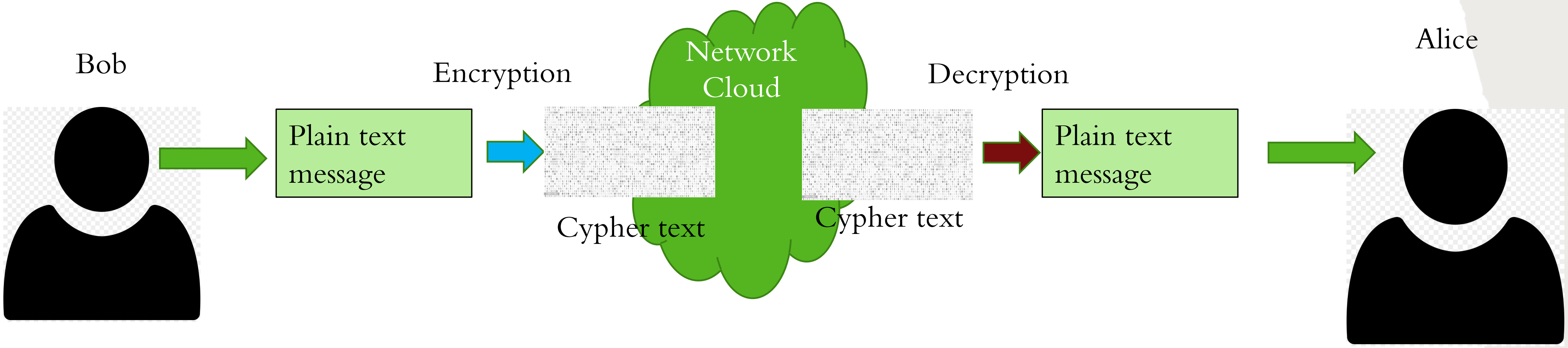
● Unfortunately

2. ENCRYPTION

Auguste Kerckhoffs Principles (1883) *Journal of Military Science, Military Cryptography)*

- The system should be, if not theoretically unbreakable, unbreakable in practice.
- ***The design of a system should not require secrecy, and compromise of the system should not inconvenience the correspondents*** (Kerckhoffs's principle).
- The key should be memorable without notes and should be easily changeable.
- The cryptograms should be transmittable by telegraph.
- The apparatus or documents should be portable and operable by a single person.
- The system should be easy, neither requiring knowledge of a long list of rules nor involving mental strain.

ENCRYPTION BASICS



Bob

Plain text message

Encryption

Cypher text

Network Cloud

Cypher text

Decryption

Plain text message

Alice

$\text{Decryption}_{\text{key1}}\ (\text{Encryption}_{\text{key2}}\ (\text{ plain text }))\ = \text{plain text}$

Sometimes key1 = key 2 symmetric encryption
Sometimes key1 <> key 2 asymmetric encryption

"I'm applying for the Information Security position.
Here is a copy of my resumé, encoded, encrypted and shredded."

TRIVIAL EXAMPLE

Cleartext:	*A*	*P*	*P*	*L*	*E*	*Key*	*4*	*4*	*4*	*4*	*4*
Ciphertext:	E	T	T	P	I						

Encrypt (APPLE) $_{\text{Shift Right 4 4 4 4}}$ = ETTPI and Decrypt (ETTPI) $_{\text{Shift Left 4 4 4 4}}$ = APPLE asymmetric

Encrypt (APPLE) $_{\text{invert}}$ = ∀ЬЬΓE Decrypt (∀ЬЬΓE) $_{\text{invert}}$ = APPLE symmetric

GOOD ENCRYPTION (SHANNON) USES:

1) Confusion

Confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two.

The property of confusion hides the relationship between the ciphertext and the key.

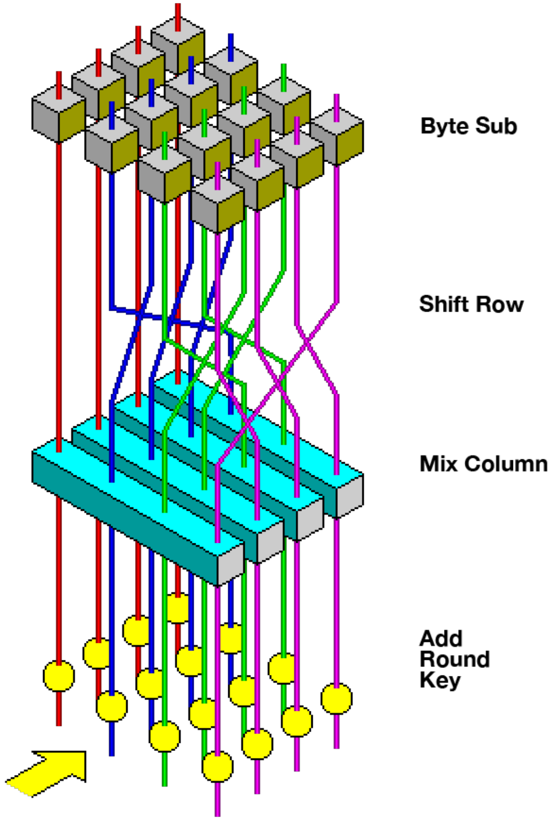
2) Diffusion

Diffusion means that if we change a single bit of the plaintext, then about half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then about half of the plaintext bits should change.

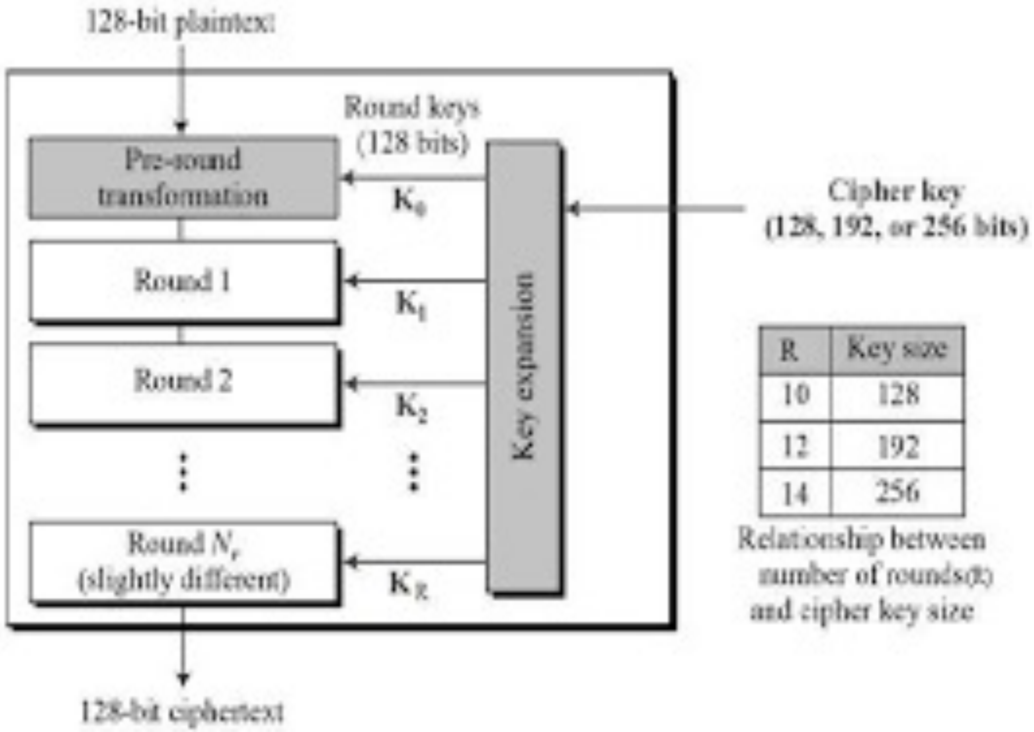
"Putting your text in Pig Latin isn't the same as encrypting."

SYMMETRIC ENCRYPTION(*ADVANCED ENCRYPTION STANDARD, NIST 2001*)

(supersedes the Data Encryption Standard (DES))



substitution–permutation network



R	Key size
10	128
12	192
14	256

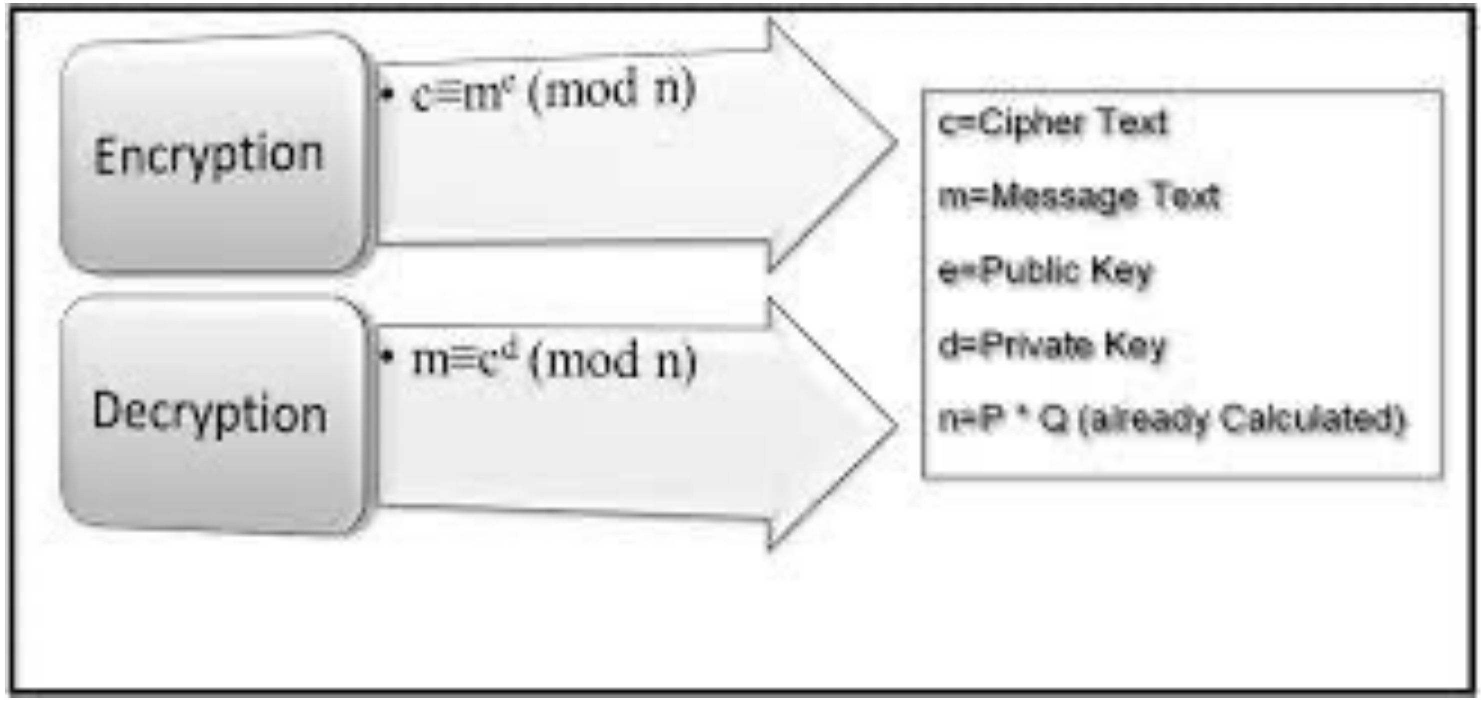
Relationship between number of rounds(R) and cipher key size

ATTACKS ON AES

(AES has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.)

- In 2009, a new related-key attack was discovered that exploits the simplicity of AES's key schedule and has a complexity of 2^{119}.
- Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir, published an attack against AES-256 that uses only two related keys and 2^{70} time to recover the complete 256-bit key of a 11-round version. (Not really effective against 12 or 14 rounds.)
- The first key-recovery attacks on full AES were biclique attack by Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger, and were published in 2011. The attack faster than brute force by a factor of about four and requires $2^{126.2}$ operations to recover an AES-128 key.
- According to the Snowden documents, the NSA is doing research on whether a cryptographic attack based on tau statistic may help to break AES

RCA ASYMMETRIC ENCRYPTION



- $c \equiv m^e \pmod{n}$
- $m \equiv c^d \pmod{n}$

c=Cipher Text

m=Message Text

e=Public Key

d=Private Key

n=P * Q (already Calculated)

ATTACKS ON RSA ENCRYPTION

- The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem” and mistakes in implementing the protocol
- Mistakes have been found in the implementations of the protocol
- For smaller primes and certain choices of primes, factoring is possible

ELLIPTIC CURVE CRYPTOGRAPHY – SYMMETRIC AND ASYMMETRIC

- The U.S. National Institute of Standards and Technology (NIST) has endorsed elliptic curve cryptography in its Suite B set of recommended algorithms, specifically elliptic-curve Diffie–Hellman (ECDH) for key exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signature.
- The typical ECC key size of 256 bits is equivalent to a 3072-bit RSA key and 10,000 times stronger than a 2048-bit RSA key!
- Some of the newer encryption protocols have made them safer from quantum computing should it ever become popular.

Key Differences	*Symmetric Encryption*	*Asymmetric Encryption*
Size of cipher text	Smaller cipher text compares to original plain text file.	Larger cipher text compares to original plain text file.
Data size	Used to transmit big data.	Used to transmit small data.
Resource Utilization	Symmetric key encryption works on low usage of resources.	Asymmetric encryption requires high consumption of resources.
Key Lengths	128 or 256-bit key size.	RSA 2048-bit or higher key size.
Security	Less secured due to use a single key for encryption.	Much safer as two keys are involved in encryption and decryption.
Number of keys	Symmetric Encryption uses a single key for encryption and decryption.	Asymmetric Encryption uses two keys for encryption and decryption
Techniques	It is an old technique.	It is a modern encryption technique.
Confidentiality	A single key for encryption and decryption has chances of key compromised.	Two keys separately made for encryption and decryption that removes the need to share a key.
Speed	Symmetric encryption is fast technique	Asymmetric encryption is slower in terms of speed.
Algorithms	RC4, AES, DES, 3DES, and QUAD.	RSA, Diffie-Hellman, ECC algorithms.

Where do cyber security technicians go when they die?

Encrypts

yellowjokes.com

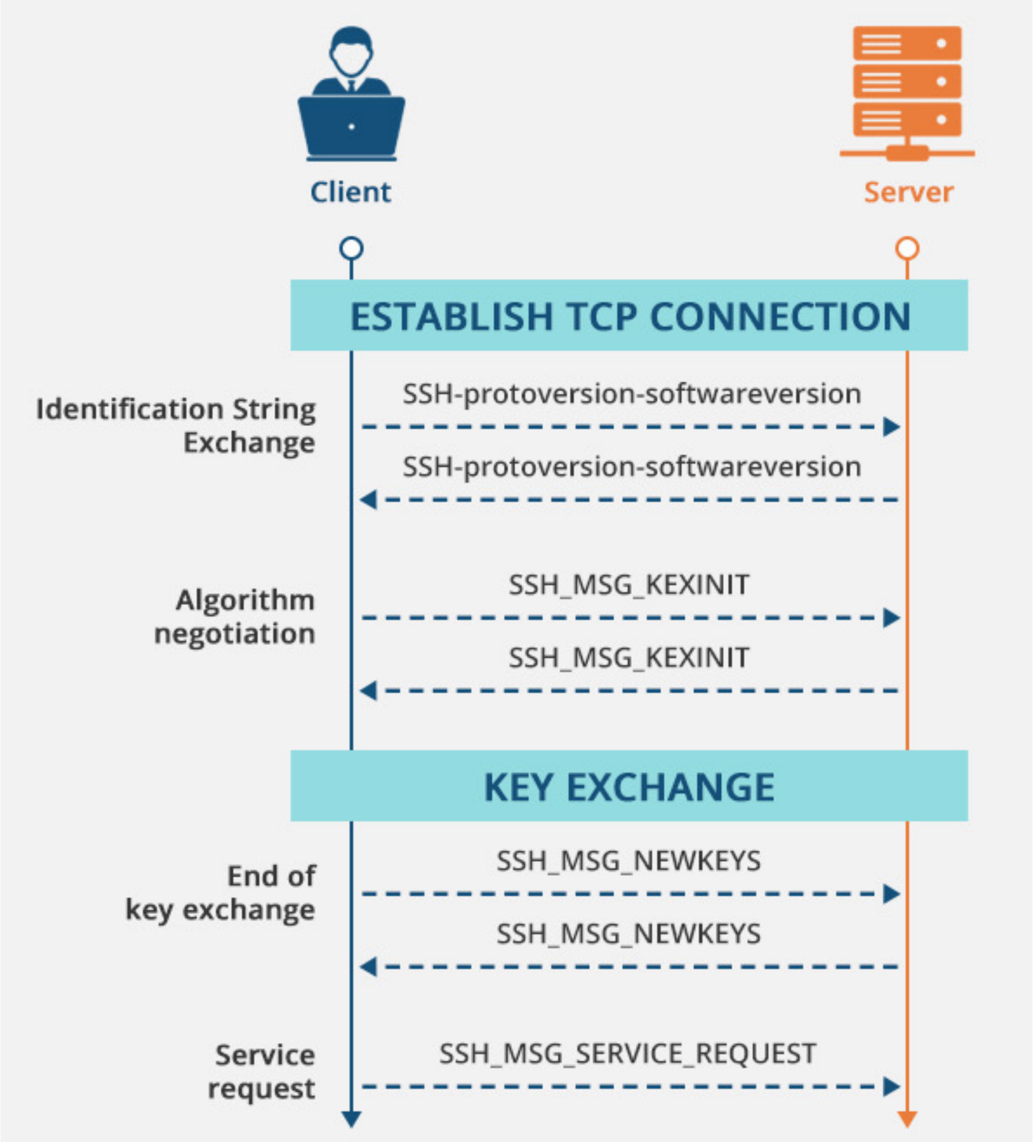
3A) TYPICAL USES OF ENCRYPTION

- Hide contents of a message
- Make the contents of a file confidential and provide privacy
- Make a password confidential:

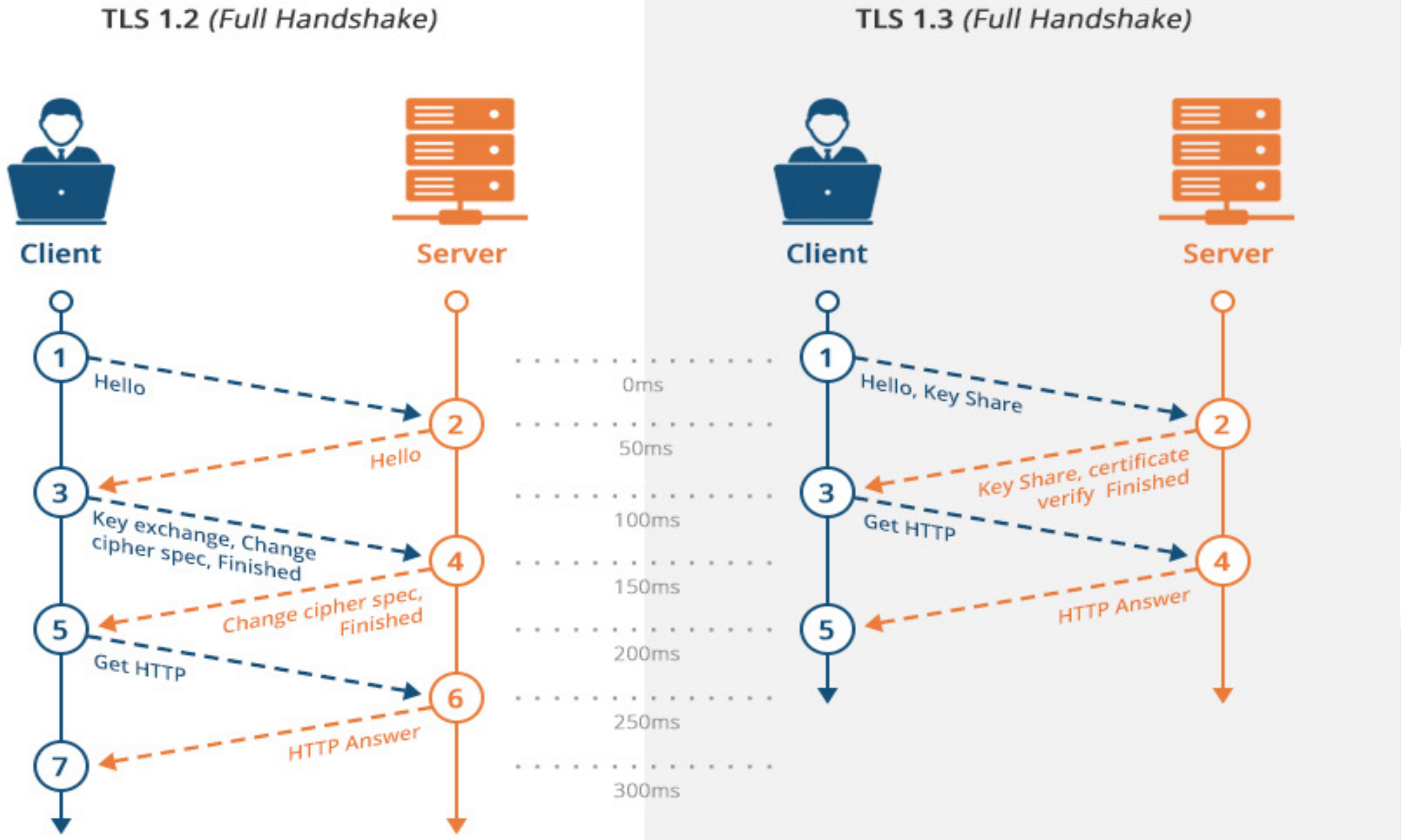
  Encrypt and hash a password to a large number (one way hash). Compare two hashes for validity.

  Encrypt a password and decrypt it to check its valid
- Identify a remote user to a server using a certificate
- Make an unforgeable document. The encryption/decryption key guarantees the document and its integrity.
- Show provenance of a document by encrypting the document with a sequence number, the date, time and user credential.
- A “Nonce” may be added to hide the identity and prevent reuse of the document. A nonce is a random number used only once.

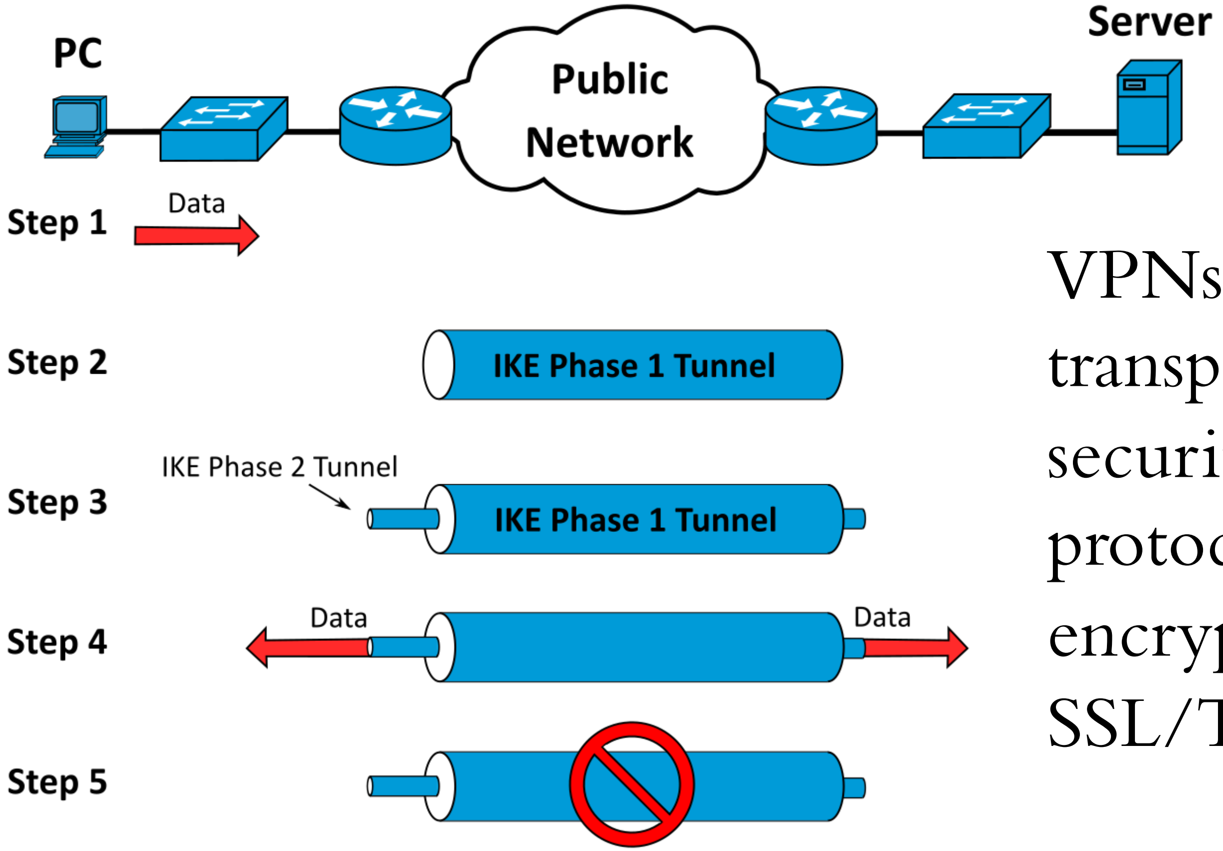
SECURE SHELL PROTOCOL SSH COMMUNICATION



Transport Layer Security



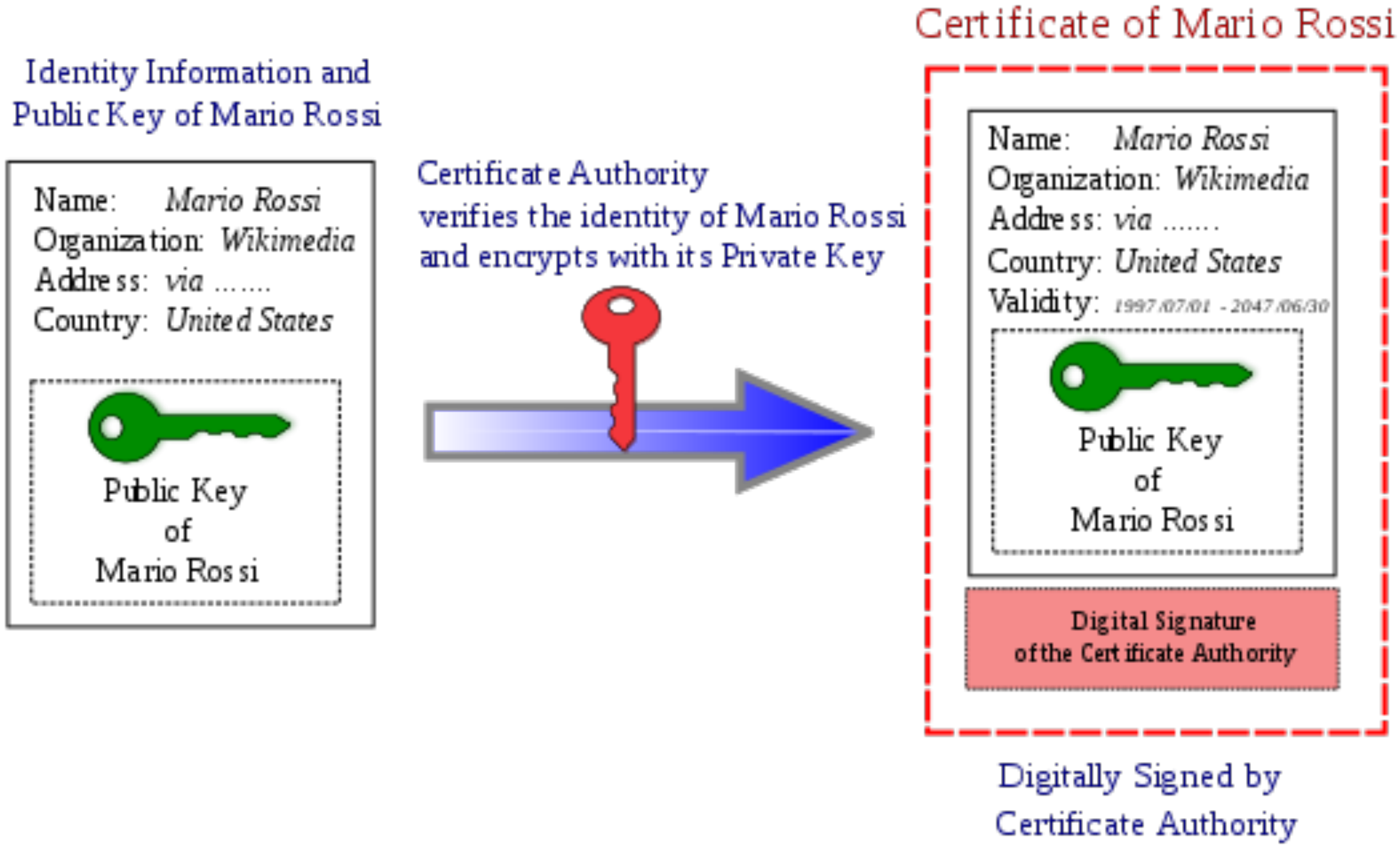
VIRTUAL PRIVATE NETWORK



VPNs use a transport layer security protocol for encryption, e.g. SSL/TLS…

Michel Bakni

CERTIFICATES



Identity Information and Public Key of Mario Rossi

Name: *Mario Rossi*
Organization: *Wikimedia*
Address: *via ....*
Country: *United States*

Public Key of Mario Rossi

Certificate Authority verifies the identity of Mario Rossi and encrypts with its Private Key

Certificate of Mario Rossi

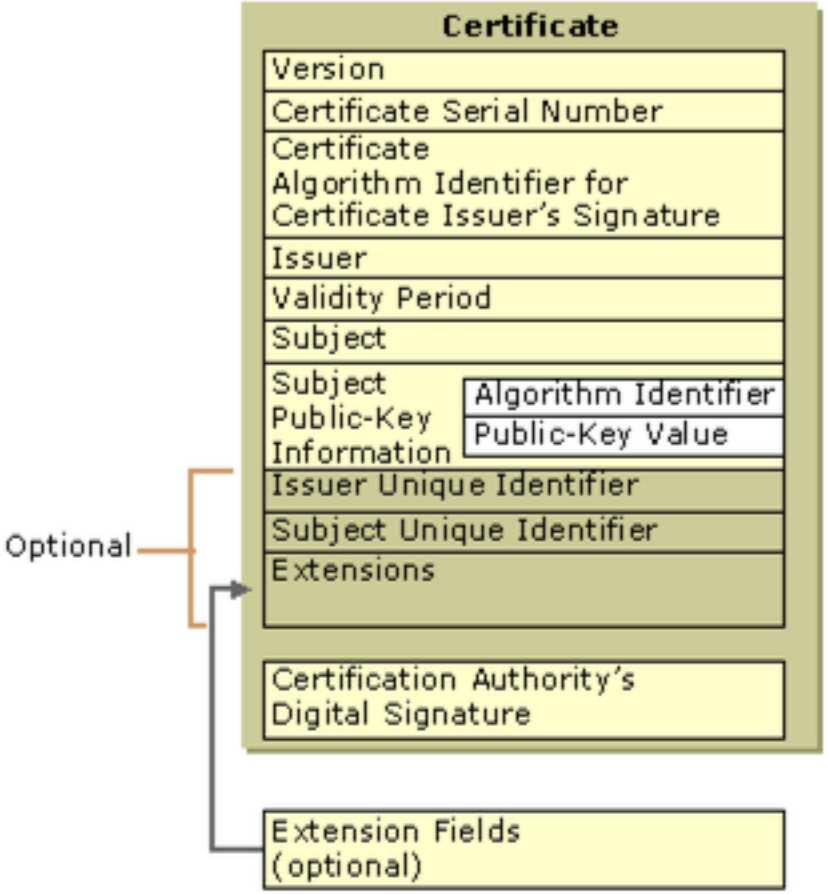
Name: *Mario Rossi*
Organization: *Wikimedia*
Address: *via ....*
Country: *United States*
Validity: *1997/07/01 - 2047/06/30*

Public Key of Mario Rossi

Digital Signature of the Certificate Authority

Digitally Signed by Certificate Authority

Standard X.509 certificate format



Certificate

Version

Certificate Serial Number

Certificate
Algorithm Identifier for
Certificate Issuer's Signature

Issuer

Validity Period

Subject

Subject
Public-Key
Information

Algorithm Identifier

Public-Key Value

Issuer Unique Identifier

Subject Unique Identifier

Extensions

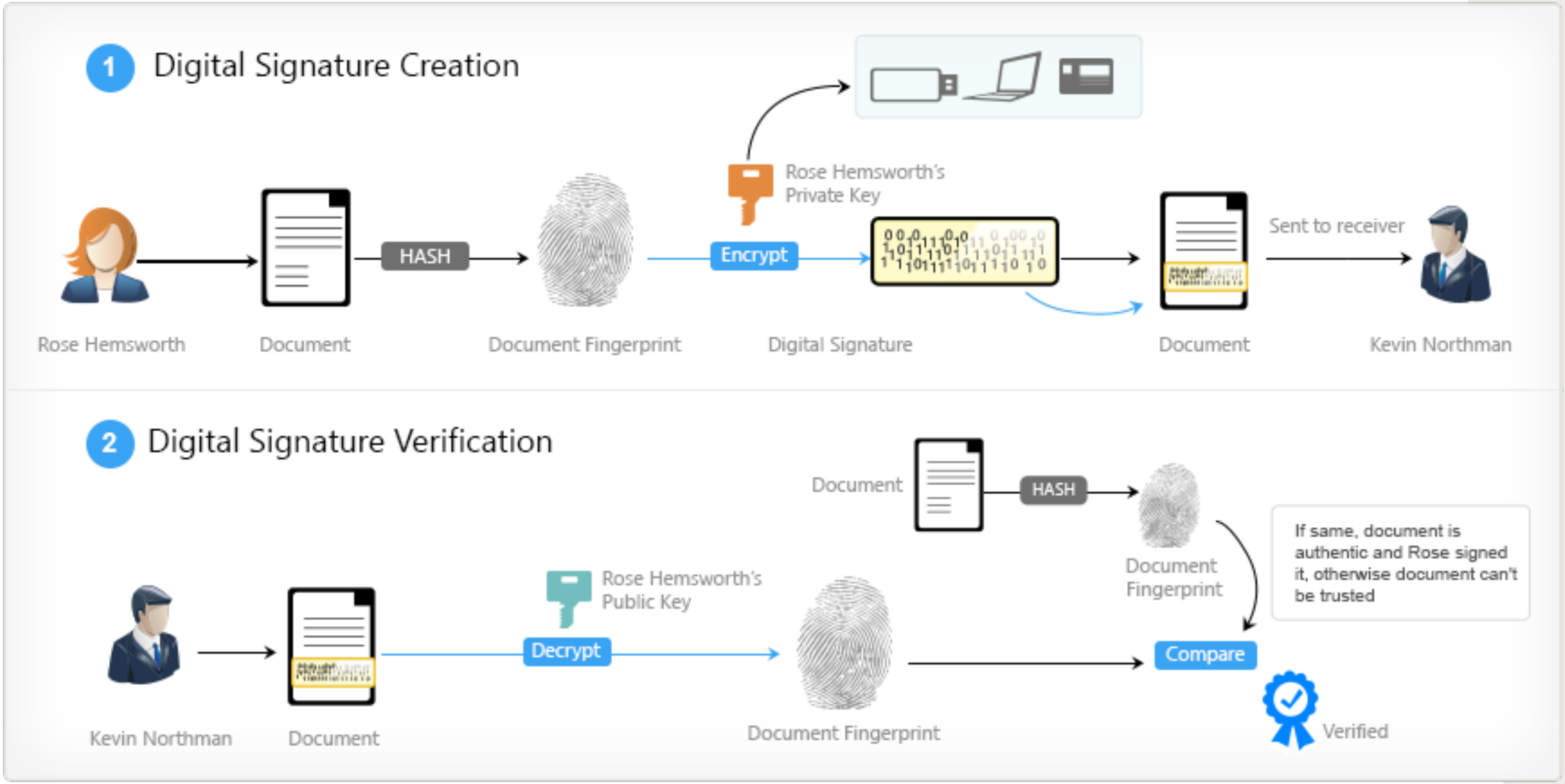
Optional

Certification Authority's
Digital Signature

Extension Fields
(optional)

c{4}^c

code4copy.com



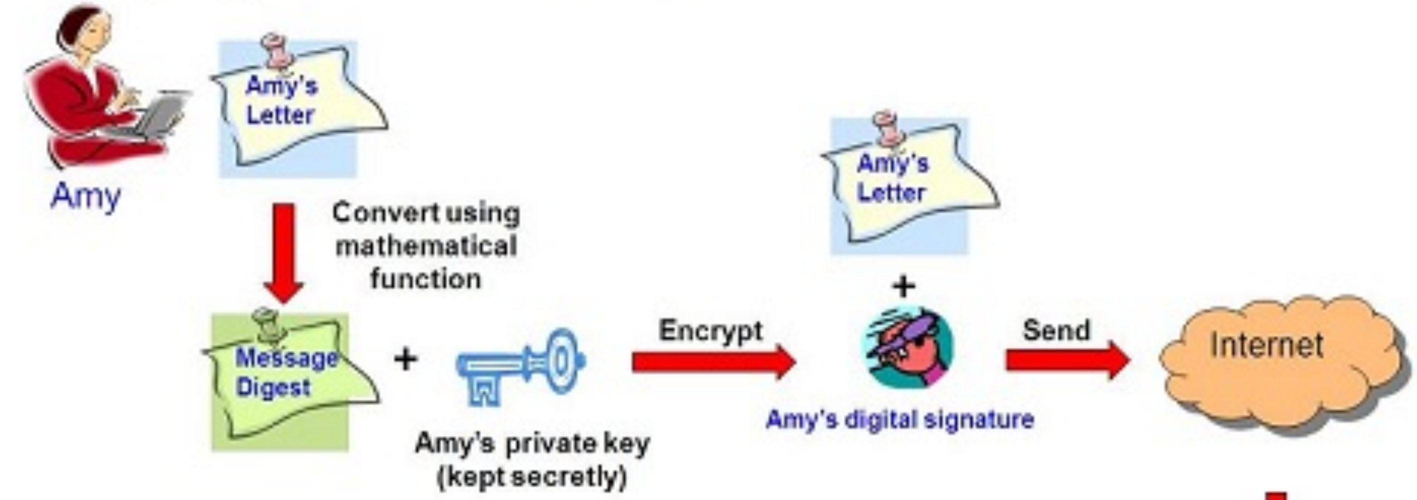
1 Digital Signature Creation

2 Digital Signature Verification

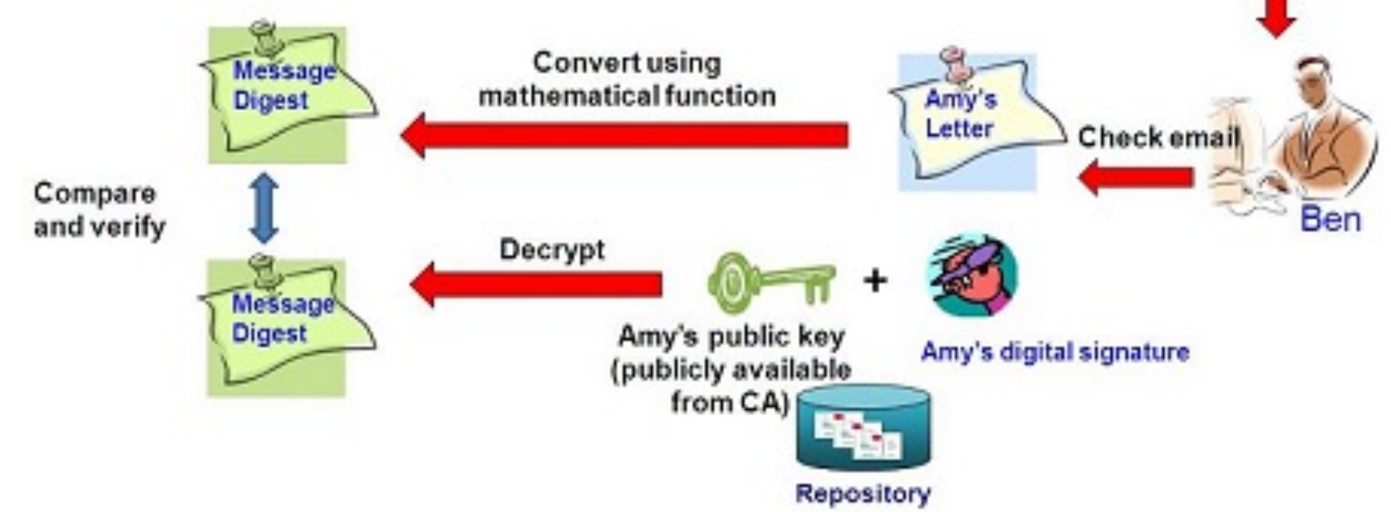
If same, document is authentic and Rose signed it, otherwise document can't be trusted

Digital Signature

1. Amy converts her letter into a message digest by using a mathematical function. She then creates her digital signature by encrypting the message digest using her private key. Her letter, together with her digital signature are sent to Ben via email.



2. Ben, upon receiving the email, verifies Amy's digital signature using Amy's public key to decrypt the message digest by comparing the other one converted from the letter using the same mathematical function.



2A) SIMPLE ATTACKS AGAINST ENCRYPTED COMMUNICATIONS.

- Brute-Force Attack: Guess key by trying all permutations
- Attack against protocol vulnerability.
- Man-in-the-Middle Attack. https://en.wikipedia.org/wiki/Man-in-the-middle_attack
- Replay Attack: Basically repeats protocol.
- Side-Channel Attacks: Electromagnetic, Acoustic. Power, Optical, Timing, Memory cache, Hardware vulnerability

CYBERATTACKS AND ENCRYPTION

- Steal the keys
- Encrypted traffic allows monitoring blind spots. Encrypted malware, spear-phishing. difficult to detect
- Tor – Encrypted internet -like network that allows private browsing, defense against surveillance, anonymity among users, multilayered encryption. The goal of onion routing was to have a way to use the internet with as much privacy as possible, and the idea was to route traffic through multiple servers and encrypt it each step of the way. This is still a simple explanation for how Tor works today.
- Encrypted malware makes it difficult to remove or to know what it is doing if it is executed

2B) MAN IN THE MIDDLE ATTACKS

There are many approaches to man in the middle attacks. Here are some:

- ARP Cache Poisoning
- DNS Cache Poisoning
- HTTPS Spoofing. ...
- Wi-Fi Eavesdropping. ...
- Session Hijacking.

ARP CACHE POISONING.

ARP Cache Poisoning. Address Resolution Protocol (ARP) is a low-level process that translates the machine address (MAC) to the IP address on the local network. ...

- The attacker must have access to the network. They scan the network to determine the IP addresses of at least two devices—let's say these are a workstation and a router.
- The attacker uses a spoofing tool, such as Arpspoof or Driftnet, to send out forged ARP responses.
- The forged responses advertise that the correct MAC address for both IP addresses, belonging to the router and workstation, is the attacker's MAC address. This fools both router and workstation to connect to the attacker's machine, instead of to each other.
- The two devices update their ARP cache entries and from that point onwards, communicate with the attacker instead of directly with each other.
- The attacker is now secretly in the middle of all communications.

DNS CACHE POISONING

DNS (Domain Name Server) cache poisoning is ***the act of entering false information into a DNS cache***, so that DNS queries return an incorrect response and users are directed to the wrong websites. DNS cache poisoning is also known as 'DNS spoofing.

E.g. when wanting to connect to Illinois.edu, the network protocols look for edu and Illinois in the closest (network wise) domain name server. That domain name server will return the Internet protocol address (eg 192.17.172.3) of the gateway to the Illinois network.

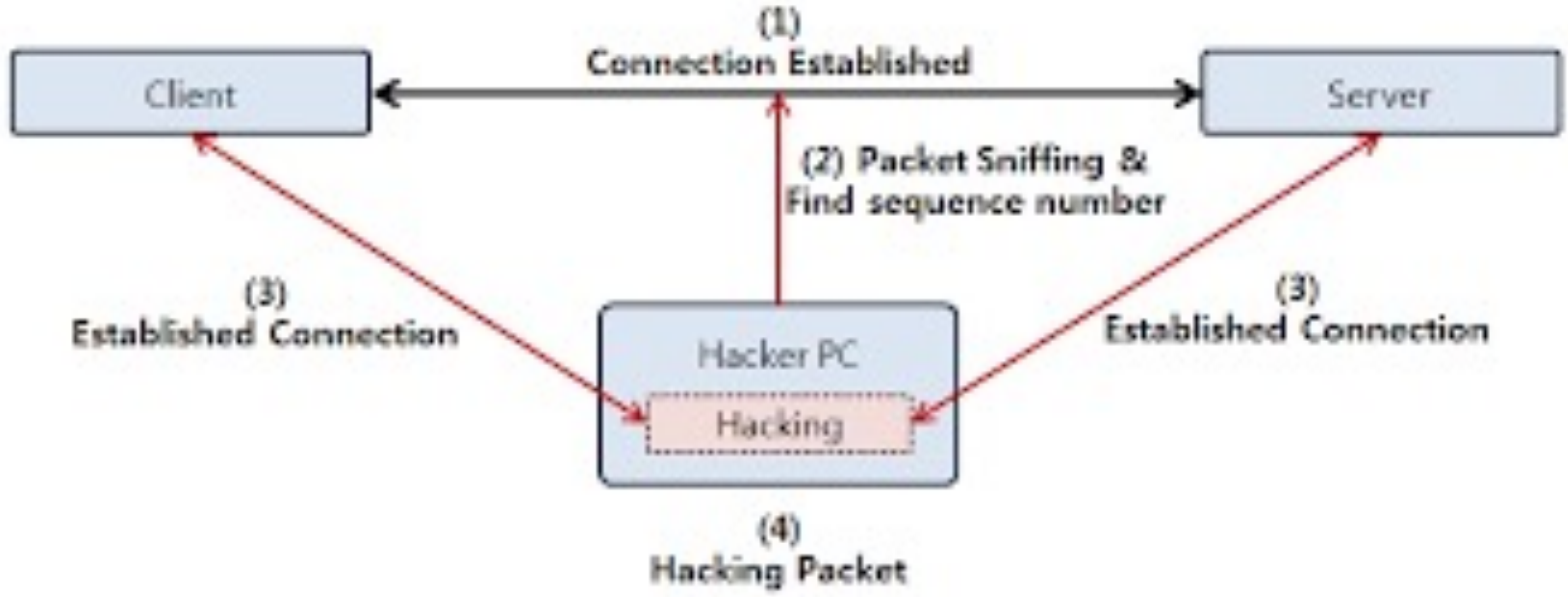
HTTPS SPOOFING

To stage homographic attacks, hackers register a domain name that is similar to the target website, and also registers its SSL certificate to make it look legitimate and secure. Then they send a link to their intended victim. Since most browsers support the display of punycode hostnames in their address bar, when the user browses to the address, they won't notice that it is a bogus version of the site they expect to visit. Their browser even shows that the website's certificate is legitimate and secure, further making it difficult to detect the attack.

WI-FI EAVESDROPPING

Eavesdropping is as an electronic attack where digital communications are intercepted by an individual whom they are not intended. This is done in two main ways: ***Directly listening to digital or analog voice communication or the interception or sniffing of data relating to any form of communication***.

SESSION HIJACKING



Tech update:
Mac now supports Windows.

"We forgot to back up our files, so we're asking everyone to remember everything they've typed during the past 10 days."

REFERENCES

- https://www.cisa.gov/tips/
- https://www.cisa.gov/uscert/publications/securing-your-web-browser
- UNICEF RESOURCE PACK (p6-9) https://www.unicef.org/eca/media/13636/file
- EU Final report of the independent High Level Group on fake news and online disinformation https://www.ecsite.eu/sites/default/files/amulti-dimensionalapproachtodisinformation-reportoftheindependenthighlevelgrouponfakenewsandonlinedisinformation.pdf
- Product Vulnerabilities https://www.cvedetails.com/top-50-products.php
- Kerckhoffs's principle
- https://en.wikipedia.org/wiki/Man-in-the-middle_attack
- https://en.wikipedia.org/wiki/Multi-factor_authentication

4. APPENDIX PROTECT YOURSELF AGAINST CYBERATTACKS

The US Government recommends the following actions:

4A) 13 steps to PREVENT CYBERATTACKS
4B) 8 steps DURING a CYBERATTACK
4C) 7 steps AFTER a CYBERATTACK

https://www.ready.gov/cybersecurity

13 STEPS TO PREVENT CYBERATTACKS

1. Limit the personal information you share online. Change privacy settings and do not use location features.
2. Keep software applications and operating systems up-to-date.
3. Create strong passwords by using upper and lower case letters, numbers and special characters. Use a password manager and two methods of verification. CHANGE DEFAULTS.
4. Watch for suspicious activity that asks you to do something right away, offers something that sounds too good to be true or needs your personal information. Think before you click. When in doubt, do NOT click.
5. Protect your home and/or business using a secure Internet connection and Wi-Fi network, and change passwords regularly.

https://www.ready.gov/cybersecurity

PROTECT YOURSELF AGAINST CYBERATTACKS

6. Don’t share PINs or passwords. Use devices that use biometric scans when possible (e.g. fingerprint scanner or facial recognition).
7. Check your account statements and credit reports regularly.
8. Be cautious about sharing personal financial information, such as your bank account number, social security number, or credit card number. Only share personal information on secure sites that begin with https://. Do not use sites with invalid certificates. Use a Virtual Private Network (VPN) that creates a more secure connection.
9. Use antivirus solutions, malware and firewalls to block threats.

https://www.ready.gov/cybersecurity

PROTECT YOURSELF AGAINST CYBERATTACKS

10. Back up your files regularly in an encrypted file or encrypted file storage device.
11. Do not click on links in texts or emails from people you don't know. Scammers can create fake links to websites.
12. Remember that the government will not call, text or contact you via social media about owing money or receiving economic impact payments.
13. Keep in mind that scammers may try to take advantage of financial fears by calling with work-from-home-opportunities, debt consolidation offers and student loan repayment plans.

https://www.ready.gov/cybersecurity

8 STEPS DURING AN ATTACK

1. Check your credit statement for unrecognizable charges.
2. Check your credit reports for any new accounts or loans you didn't open.
3. Be alert for soliciting emails and social media users asking for private information.
4. If you notice strange activity, limit the damage by immediately changing all of your internet account passwords.
5. Consider turning off the device. Take it to a professional to scan for potential viruses and remove any that they find. Remember: A company will not call you and ask for control of your computer to fix it. This is a common scam.
6. Let work, school or other system owners know.
7. Run a security scan on your device to make sure your system is not infected or acting more slowly or inefficiently.
8. If you find a problem, disconnect your device from the Internet and perform a full system restore.

https://www.ready.gov/cybersecurity

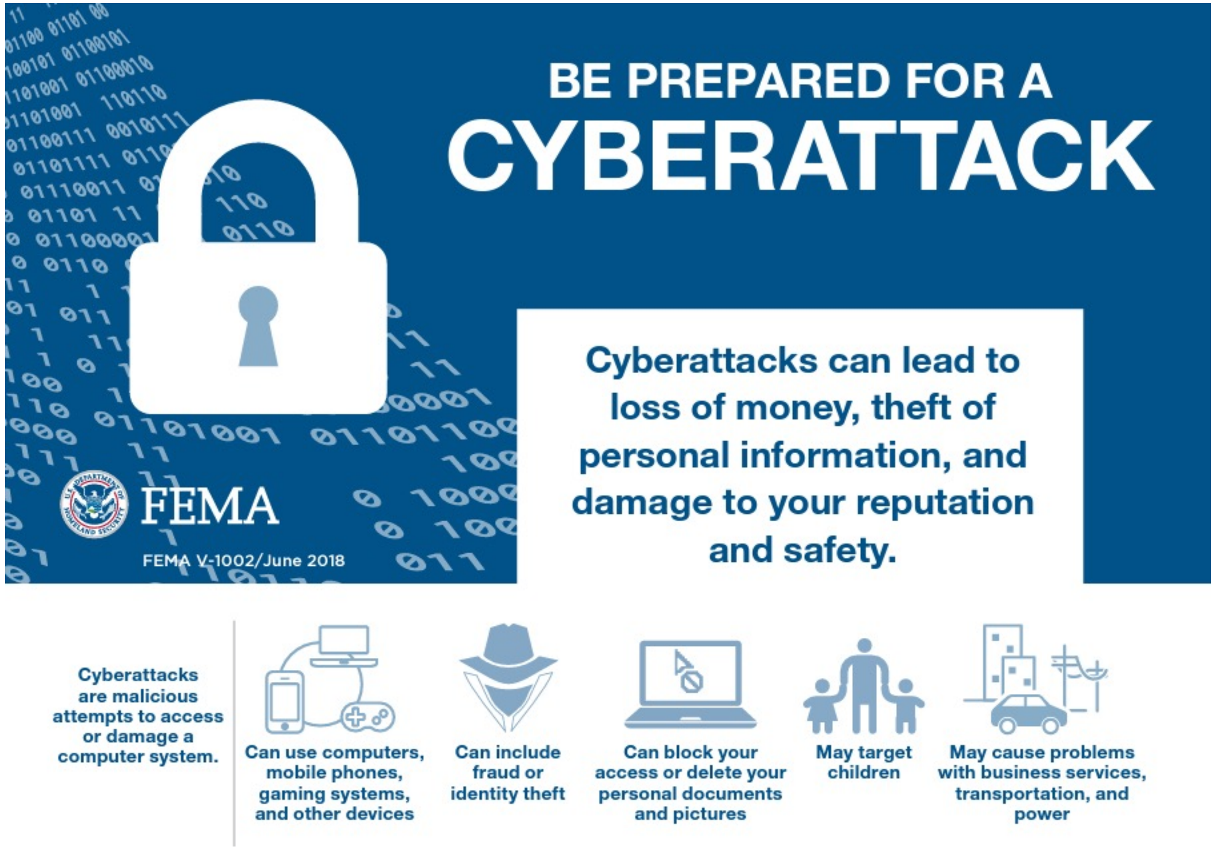
7 STEPS AFTER A CYBERATTACK

1. Contact banks, credit card companies and other financial services companies where you hold accounts. You may need to place holds on accounts that have been attacked. Close any unauthorized credit or charge accounts. Report that someone may be using your identity.
2. File a report with the Office of the Inspector General (OIG) if you think someone is illegally using your Social Security number.
3. File a complaint with the FBI Internet Crime Complaint Center (IC3). They will review the complaint and refer it to the appropriate agency.
4. File a report with the local police so there is an official record of the incident.
5. Report identity theft to the Federal Trade Commission.
6. Contact the Federal Trade Commission (FTC) at ftc.gov/complaint if you receive messages from anyone claiming to be a government agent.
7. Contact additional agencies depending on what information was stolen. Examples include contacting:
   1. The Social Security Administration (800-269- 0271) if your social security number was compromised, or
   2. The Department of Motor Vehicles if your driver's license or car registration has been stolen.

Report online crime or fraud to your local United States Secret Service (USSS) Electronic Crimes Task Force or the Internet Crime Complaint Center.

https://www.ready.gov/cybersecurity

READY CYBERATTACK INFORMATION SHEET



BE PREPARED FOR A

CYBERATTACK

Cyberattacks can lead to loss of money, theft of personal information, and damage to your reputation and safety.

FEMA

FEMA V-1002/June 2018

Cyberattacks are malicious attempts to access or damage a computer system.

Can use computers, mobile phones, gaming systems, and other devices

Can include fraud or identity theft

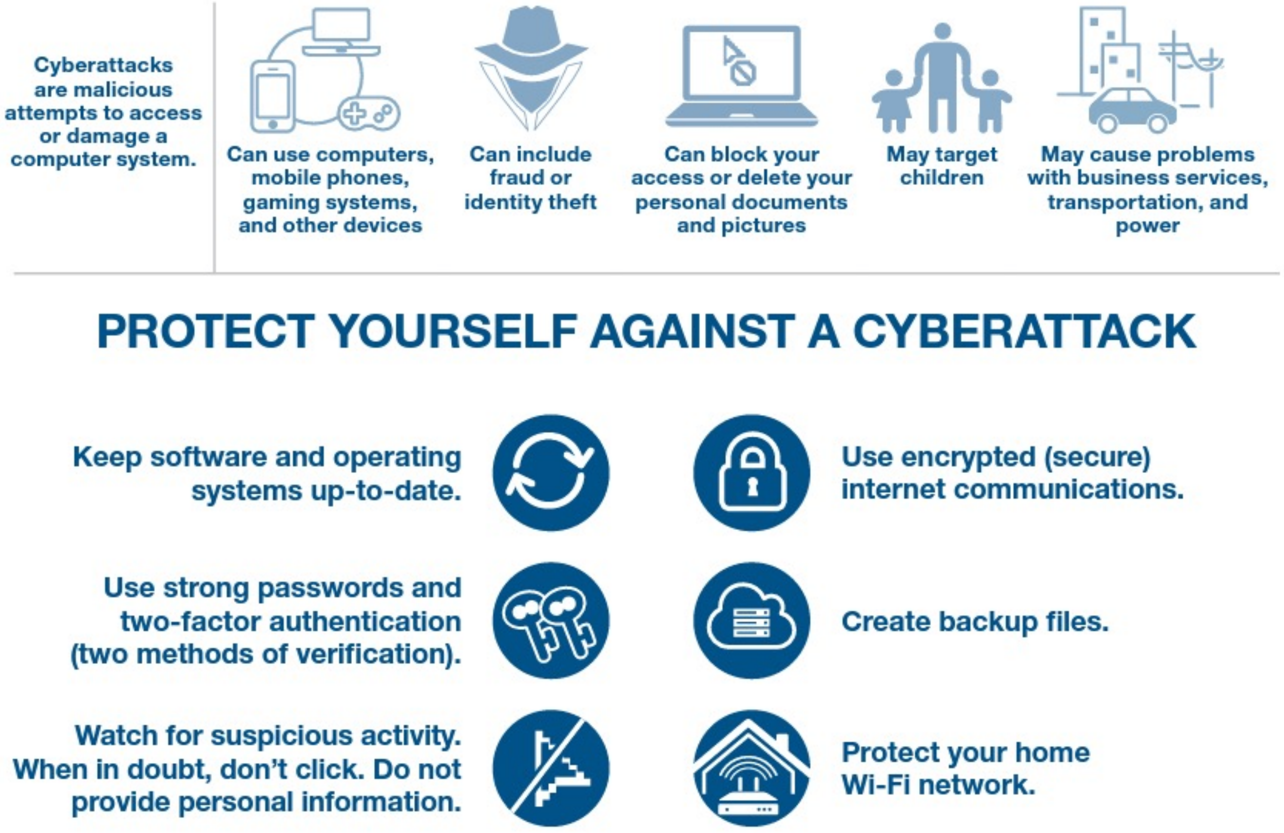
Can block your access or delete your personal documents and pictures

May target children

May cause problems with business services, transportation, and power

https://www.ready.gov/sites/default/files/2020-11/ready_cyberattack_information-sheet.pdf

READY CYBERATTACK INFORMATION SHEET



Cyberattacks are malicious attempts to access or damage a computer system.

Can use computers, mobile phones, gaming systems, and other devices

Can include fraud or identity theft

Can block your access or delete your personal documents and pictures

May target children

May cause problems with business services, transportation, and power

PROTECT YOURSELF AGAINST A CYBERATTACK

Keep software and operating systems up-to-date.

Use encrypted (secure) internet communications.

Use strong passwords and two-factor authentication (two methods of verification).

Create backup files.

Watch for suspicious activity. When in doubt, don't click. Do not provide personal information.

Protect your home Wi-Fi network.

https://www. ready_cyberattack_information-sheet

INFORMATION SHEET-PREVENT

1. Keep your anti-virus software updated.
2. Use strong passwords that are 12 characters or longer. Use upper and lowercase letters, numbers, and special characters. Change passwords monthly. Use a password manager.
3. Use a stronger authentication such as a PIN or password that only you would know. Consider using a separate device that can receive a code or uses a biometric scan (e.g., fingerprint scanner).
4. Watch for suspicious activity that asks you to do something right away, offers something that sounds too good to be true, or needs your personal information. Think before you click.
5. Check your account statements and credit reports regularly.
6. Use secure internet communications. Use sites that use "HTTPS" if you will access or provide any personal information. Don't use sites with invalid certificates. Use a Virtual Private Network (VPN) that creates a secure connection.
7. Use antivirus solutions, malware, and firewalls to block threats.
8. Regularly back up your files in an encrypted file or encrypted file storage device.
9. Limit the personal information you share online. Change privacy settings and do not use location features.
10. Protect your home network by changing the administrative and Wi-Fi passwords regularly. When configuring your router, choose the Wi-Fi Protected Access 2 (WPA2) Advanced Encryption Standard (AES) setting, which is the strongest encryption option.

INFORMATION SHEET-LIMIT DAMAGE

1. Limit the damage. Look for unexplained charges, strange accounts on your credit report, unexpected denial of your credit card, posts you did not make showing up on your social networks, and people receiving emails you never sent.
2. Immediately change passwords for all of your online accounts.
3. Scan and clean your device. Consider turning off the device. Take it to a professional to scan and fix.
4. Let work, school, or other system owners know. Information Technology (IT) departments may need to warn others and upgrade systems.
5. Contact banks, credit card companies, and other financial accounts. You may need to place holds on accounts that have been attacked. Close any unauthorized credit or charge accounts. Report that someone may be using your identity.

INFORMATION SHEET-REPORT

1. File a report with the Office of the Inspector General (OIG) if you think someone is illegally using your Social Security number. OIG reviews cases of waste, fraud, and abuse. To file a report, visit www.idtheft.gov.

2. You can also call the Social Security Administration hotline at 1-800-2690271. For additional resources and more information, visit http://oig.ssa. gov/report.

3. File a complaint with the FBI Internet Crime Complaint Center (IC3) at www.IC3.gov. They will review the complaint and refer it to the appropriate agency.

4. Learn tips, tools, and more at www. dhs.gov/stopthinkconnect.

MAC SPECIFIC NOTES

- Use FILEVAULT to secure data on your disk by encrypting its contents automatically. (Don't forget your password!!!) PC windows owners can use bitlocker or VERACRYPT which is free.
- Firewall On
- Use Backup to record backups to Time Machine. Set automatic. Use external disk drive or Cloud. [windows machines use backup and restore]
- Set Software Update to automatic
- Use Touch Id for two or multi factor factor authentication
- Limit IP address tracking by hiding your IP address from known trackers in Mail and Safari.
- Ensure DNS is to your service provider's DNS
- Limit Bluetooth downloads to specific folder in sharing
- Enable Location Services for Networking & Wireless – needed for visiting other countries

WINDOWS SPECIFIC NOTES

1. Disable Windows 10 automatic login.
2. Set a password with your screensaver.
3. Turn on your firewall.
4. Disable remote access.
5. Enable or install antivirus protection tools.
6. Enable auto-updates for your operating system.
7. Set up file backups.
8. Turn on encryption.
9. Set up your user accounts.
10. Set up a password manager.

VPN

- ***Why should you use a VPN connection?***
- Your ISP usually sets up your connection when you connect to the internet. It tracks you via an IP address. Your network traffic is routed through your ISP's servers, which can log and display everything you do online.
- Your ISP may seem trustworthy, but it may share your browsing history with advertisers, the police or government, and/or other third parties. ISPs can also fall victim to attacks by cyber criminals: If they are hacked, your personal and private data can be compromised.
- This is especially important if you regularly connect to public Wi-Fi networks. You never know who might be monitoring your internet traffic and what they might steal from you, including passwords, personal data, payment information, or even your entire identity.
- ***What should a good VPN do?***
- You should rely on your VPN to perform one or more tasks. The VPN itself should also be protected against compromise. These are the features you should expect from a comprehensive VPN solution:
- ***Encryption of your IP address:*** The primary job of a VPN is to hide your IP address from your ISP and other third parties. This allows you to send and receive information online without the risk of anyone but you and the VPN provider seeing it.
- ***Encryption of protocols:*** A VPN should also prevent you from leaving traces, for example, in the form of your internet history, search history and cookies. The encryption of cookies is especially important because it prevents third parties from gaining access to confidential information such as personal data, financial information and other content on websites.
- ***Kill switch:*** If your VPN connection is suddenly interrupted, your secure connection will also be interrupted. A good VPN can detect this sudden downtime and terminate preselected programs, reducing the likelihood that data is compromised.
- ***Two-factor authentication:*** By using a variety of authentication methods, a strong VPN checks everyone who tries to log in. For example, you might be prompted to enter a password, after which a code is sent to your mobile device. This makes it difficult for uninvited third parties to access your secure connection.

HERE'S HOW TO SURF SECURELY WITH A VPN

- A VPN encrypts your surfing behavior, which can only be decoded with the help of a key. Only your computer and the VPN know this key, so your ISP cannot recognize where you are surfing. Different VPNs use different encryption processes, but generally function in three steps:
- Once you are online, start your VPN. The VPN acts as a secure tunnel between you and the internet. Your ISP and other third parties cannot detect this tunnel.
- Your device is now on the local network of the VPN, and your IP address can be changed to an IP address provided by the VPN server.
- You can now surf the internet at will, as the VPN protects all your personal data.
-

VPN SPECIFIC NOTES

VPNs allow you to make encrypted connections to other sites. So if you are at an airport or coffee house and want to use a free internet securely, these are good.

Monthly plan

- ExpressVPN
- SurfsharkNordVPN
- The university uses CISCO

Free

- ProtonVPN
- Privado VPN
- Hide.me
- Windscribe

ROUTER SECURITY SPECIFIC NOTES

- First install the latest firmware updates for your router.
- Then update the software on your other devices,
- Set to ***WPA3 Personal*** for better security
  Set to ***WPA2/WPA3 Transitional*** for compatibility with older devices
- ***WPA3 Personal*** is the newest, most secure protocol currently available for Wi-Fi devices. It works with all devices that support Wi-Fi 6 (802.11ax), and some older devices.
- ***WPA2/WPA3 Transitional*** is a mixed mode that uses WPA3 Personal with devices that support that protocol, while allowing older devices to use WPA2 Personal (AES) instead.
- ***WPA2 Personal (AES)*** is appropriate when you can't use one of the more secure modes. In that case, also choose AES as the encryption or cipher type, if available.
- Avoid WPA/WPA2 mixed modes, WPA Personal, WEP, including WEP Open, WEP Shared, WEP Transitional Security Network, or Dynamic WEP (WEP with 802.1X), TKIP, including any security setting with TKIP in the name

WIRELESS NETWORK SPECIFIC NOTES

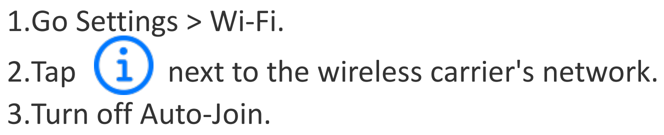
- name (SSID). Set to a ***single, unique name*** (case-sensitive) Use a name that's unique to your network, and make sure that all routers on your network use the same name for every band they support.
- Don't use common names or default names such as *linksys*, *netgear*, *dlink*, *wireless*, or *2wire*, and don't give your 2.4GHz and 5GHz bands different names.
- Set "Hidden network" to disabled.
- Set MAC address filtering, authentication, access control to disabled. It can easily be faked so its not worth it.
- Automatic firmware updates. Set enabled.
- Radio mode. Set to All.
- Bands. Enable all bands.

WIRELESS NETWORKS

- Channel. Set to Auto.
- Channel Width. Set to ***20MHz*** for the 2.4GHz band. Set to ***Auto*** or all widths (***20MHz, 40MHz, 80MHz***) for the 5GHz band
- DHCP Set to ***Enabled***, if your router is the only DHCP server on the network.
- DHCP lease time. ***8 hours*** for home or office networks; ***1 hour*** for hotspots or guest networks
- NAT. Set to ***Enabled***, if your router is the only device providing NAT on the network
- WMM. Set to ***Enabled***

AUTO-JOIN WHEN USED WITH WIRELESS CARRIER WI-FI NETWORK

- If you see ”Privacy Warning” under the name of your carrier's network in Wi-Fi settings, your cellular identity could be exposed if your device were to join a malicious hotspot impersonating your carrier's Wi-Fi network. To avoid this possibility, you can prevent your iPhone or iPad from automatically rejoining your carrier’s Wi-Fi network:



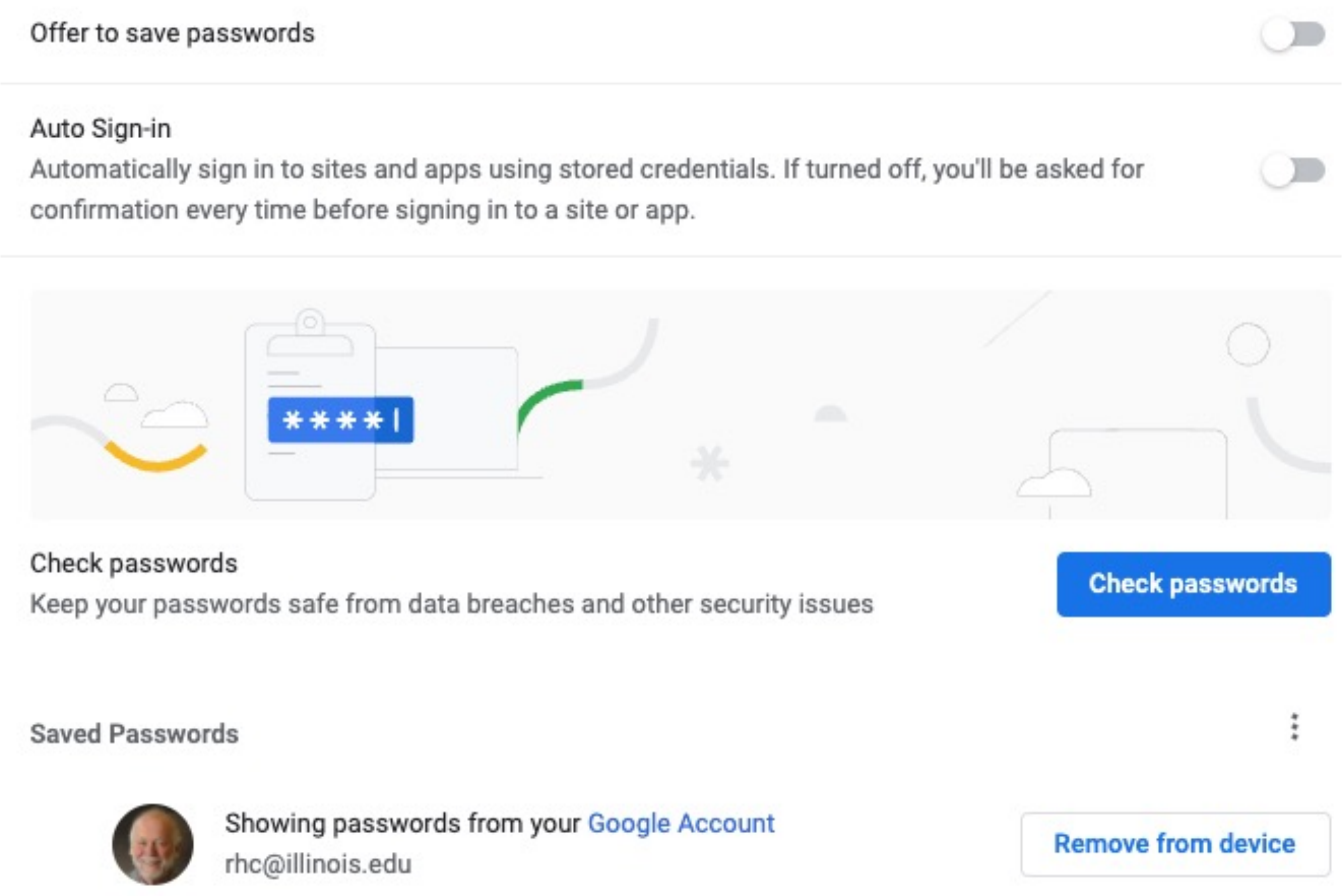
1.Go Settings > Wi-Fi.
2.Tap ⓘ next to the wireless carrier's network.
3.Turn off Auto-Join.

https://support.apple.com/en-us/HT202068

BROWSER SETTINGS CHROME NOTES

- ***CHROME***
  Enable Phishing and Malware Protection –Activate it under the ***“Privacy”*** section of the settings menu.
- ***Disable Instant Search*** – Sure, it’s incredible convenient to be able to search just by entering your query in the address bar, but it’s not the most secure. Using this method, anything you type is immediately sent to Google. You can disable this in the settings menu.
- ***Don’t Sync Your Email Account*** – Once again, what seems like an extremely convenient feature actually makes you less secure. By syncing your account with the Chrome browser, you’re allowing Google to store sensitive information like passwords and an autofill data on its servers. If you still want to sync accounts, at least turn on the “encrypt all synced data” option in the settings menu.
- ***Turn Off Autofill and Never Save Passwords*** –Yes, it’s nice not having to type in passwords and finish entering data into certain fields, but by leaving these settings on you’re allowing Google to save that information on its servers, thus making it easier to steal.
- ***Other Suggestions Cookies*** – Choose the option that lets you keep local data until you quit your browser and make sure to block third-party cookies.
- ***Javascript*** – Select the option that prevents sites from running Javascript.
- ***Pop-ups*** – This one is pretty obvious, make sure you choose to block pop-ups.
- ***Location*** – Turn off the feature that allows sites to track your location.

BROWSER SETTINGS CHROME NOTES



Offer to save passwords

Auto Sign-in

Automatically sign in to sites and apps using stored credentials. If turned off, you'll be asked for confirmation every time before signing in to a site or app.

Check passwords

Keep your passwords safe from data breaches and other security issues

Saved Passwords

Showing passwords from your Google Account

rhc@illinois.edu

BROWSER SETTINGS FIREFOX NOTES

- ***FIREFOX***

  Configure Privacy Settings – Again, it should be obvious why you would want to make sure to get your ***privacy settings set up correctly***. You can find them under the "Privacy" tab. You're going to set up Firefox so it stores only enough information as is needed for it to function properly:

  Choose "Use custom settings for history."

  Unselect "Remember my browsing and download history."

  Unselect "Remember search and form history."

  Unselect "Accept third-party cookies."

  Choose the cookie storage option to "Keep until I close Firefox."

  Choose "Clear history when Firefox closes."

BROWSER SETTINGS FIREFOX NOTES

- ***Configure Security Settings*** – In order to avoid risky websites and prevent Firefox from storing your passwords, you'll need configure your security settings in the "Security" tab.

  Select "Warn me when sites try to install add-ons."

  Select "Block reported attack sites."

  Select "Block reported web forgeries."

  Unselect "Remember passwords for sites."

- ***Disable Javascript*** – Under the "Content" tab, unselect "Enable Javascript." Javascript can cause a lot of problems, so it's better to just avoid it all together.
- Enable Pop-up Blocking – Also under the "Content" tab, you can select to prevent pop-ups, which is definitely recommended.
- ***Don't Sync*** – This isn't a setting so much as a suggestion: don't sync. Doing so allows Firefox to store sensitive information about you.

BROWSER SETTINGS IE10 NOTES

- To access *security settings* in IE10, go through the "Internet Options" menu.
- ***Configure Security Settings*** – Again, make sure IE10 has the correct security settings selected before browsing on it. To do this, select the "Security" tab.

  Set Security Zones – This feature allows you to select individual security levels for different "zones" like internet, local internet, trusted sites, etc… Spend some time here and select your desired levels.

  Set internet zone security to "Medium High" or above, as this will block certain kinds of cookies, enable ActiveX filtering and enable several other forms of default security.

  Disable JavaScript – Under "Custom Level," find "Active Scripting" and select "Disable." Again, Javascript creates a lot of vulnerabilities—best just to avoid it.

  Automatically Clear History – Choose "Delete browsing history on exit." You can find it under the "General" tab.

  Configure Privacy Settings – Do this under the "Privacy" tab.

  - Set internet zone privacy to "Medium High" or above.
  - Never allow websites to request your location.
  - Activate "Pop-Up Blocker."

    Configure Advanced Security Settings – In the "Security" section under "Advanced," you can activate some additional security settings

    - Click "Restore advanced settings" to ensure all default settings are active.
    - Choose "Do not save encrypted pages to disk."
    - Choose "Empty Temporary Internet Files folder when browser is closed."
    - Turn off "AutoComplete."

    Tracking Protection – In IE10's "Safety" menu is the Tracking Protection feature. You will need to provide a list of names of all the sites you don't want your information being sent to, or you can download a list.

PASSWORD MANAGERS NOTES

- NORDPASS
- KEEPER
- Roboform
- DASHLANE
- 1Password
- LastPass
- Enpass
- RememBear
- Zoho Vault
- passbolt

PASSWORD MANAGERS VERSUS BROWSER PASSWORD ASSISTANT

Password Manager	***Browser***
Cross-platform and work with *any* browser. Can share passwords between mobile apps, desktop applications and browsers	Can use only when using specific browser e.g. chrome
Better form filling. Store credit card numbers and other personal data to autofill web forms. Encrypted. Robust auto-fill options	
Can provide notifications about passwords, password lengths, password usage, dark web use	
Easily and securely share passwords with other people. Eg. Emergency password for son/daughter. Share a (encrypted) password with friend.	
VPN capabilities for accessing open Wi-Fi hotspots	
Password auditing and updating features let you identify and eliminate weak or duplicate passwords	Free
Multi-factor authentication options for protecting your vault, including app-based authenticators like Symantec VIP and Google Authenticator, hardware tokens like YubiKey, and fingerprint readers.	

PHISHING PREVENTION TIPS

- ***Phishing email*** appears in your email inbox — usually with a request to follow a link, send a payment, reply with private info, or open an attachment. The sender's email might be tailored to closely resemble a valid one and may contain info that feels personal to you.
- ***Domain spoofing*** is a popular way an email phisher might mimic valid email addresses. These scams take a real company's domain (ex: @america.com) and modify it. You might engage with an address like "@arneria.com" and fall victim to the scheme.
- ***Voice phishing (vishing)*** scammers call you and impersonate a valid person or company to deceive you. They might redirect you from an automated message and mask their phone number. Vishers will try to keep you on the phone and urge you to take action.
- ***SMS phishing (smishing)*** similarly to vishing, this scheme will imitate a valid organization, using urgency in a short text message to fool you. In the message, you'll usually find a link or a phone number they want you to use**.** Mobile messaging services are also at risk of this.
- ***Social media phishing*** involves criminals using posts or direct messages to persuade you into a trap. Some are blatant like free giveaways or sketchy "official" organization pages with an urgent request. Others might impersonate your friends or build a relationship with you long-term before 'attacking' to seal the deal.
- ***Clone phishing*** duplicates a real message that was sent previously, with legitimate attachments and links replaced with malicious ones. This appears in email but may also show up in other means like fake social media accounts and text messages.

LEGITIMATE WEBSITES MIGHT BE MANIPULATED

- ***Watering hole phishing*** targets popular sites that many people visit. An attack like this might try to exploit weaknesses in a site for any number of other phishing attacks. Delivering malware, link redirection, and other means are common in these schemes.
- ***Pharming(DNS cache poisoning)*** uses malware or an onsite vulnerability to reroute traffic from safe websites to phishing sites. Manually typing a URL will still lead visitors to the malicious site if it is a victim of pharming.
- ***Typosquatting (URL hijacking)*** tries to catch people who type an incorrect website URL. For example, a website might be created that is one letter off from a valid one. Typing "wallmart" instead of "walmart" could potentially lead you to a malicious site.
- ***Clickjacking*** uses a website's vulnerabilities to insert hidden capture boxes. These will grab user login credentials and anything else you might enter on the otherwise safe site.
- ***Tabnabbing*** happens when an unattended fraudulent page reloads into an imitation of a valid site login. When you return to it, you might believe it to be real and unknowingly hand over access to your account.
- ***HTTPS phishing*** gives a malicious website the illusion of security with the classic "padlock next to the URL bar" indicator. While this encryption sign used to be exclusive to sites that were verified as safe, now any site can get this. So, your connection and info you send may be blocked to outsiders, but you're already connected to a criminal.

- ***Evil twin*** attacks mimic official public Wi-Fi at locations like coffee shops and airports. This is done in efforts to get you to connect and eavesdrop on all your online activity.
- ***Search engine results phishing*** uses methods to get a fraudulent webpage to appear in search results before a legitimate one. It is also known as SEO phishing or SEM phishing. If you don't look carefully, you may click the malicious page instead of the real one.
- ***Angler phishing*** impersonates a customer service representative for a real company to trick you out of information. On social media, a fake help account spots your "@mentions" to company's social handle to respond with a fake support message.
- ***BEC (business email compromise)*** involves various means of breaching a company's communications circle to get high-value info. This can include CEO impersonation or pretending a vendor with a fake invoice to initiate activities like wire transfers.
- ***Cryptocurrency phishing*** targets those with cryptocurrency wallets. Instead of using long-term means to mine cryptocurrency themselves, these criminals try to steal from those that already have these funds.

POPULAR PHISHING ATTACKS

- ***Iran Cyberattack phishing scams*** use an illegitimate Microsoft email, prompting a login to restore your data in attempts to steal your Microsoft credentials. Scammers use your fear of being locked out of Windows and the relevance of a current news story to make it believable.
- ***Office 365 deletion alerts*** are yet another Microsoft-related scam used to get your credentials. This email scam claims that a high volume of files have been deleted from your account. They give a link for you to login, of course resulting in your account being compromised.
- ***Notice from bank.*** This scam tricks you with a fake account notification. These emails normally give you a convenient link which leads to a web form, asking for your bank details "for verification purposes." Do not give them your details. Instead, give your bank a call as they may want to take action on the malicious email.
- ***Email from a 'friend'.*** This scam takes the form of a known friend who is in a foreign country and needs your help. This 'help' normally involves sending money to them. So, before you send your 'friend' money, give them a call first to verify whether it's true or not.
- ***Contest winner/Inheritance email.*** If you've won something unexpectedly or received an inheritance from a relative you've never heard of — don't get too excited. Because, most of the time these emails are scams that require you click on a link to enter your info for prize shipment or inheritance 'verification'.
- ***The tax refund/rebate.*** This is a popular phishing scam as many people have annual taxes which they pay or have to submit payment to. These phishing messages normally say that you are either eligible to receive a tax refund, or you have been selected to be audited.

CHECK AND REPORT

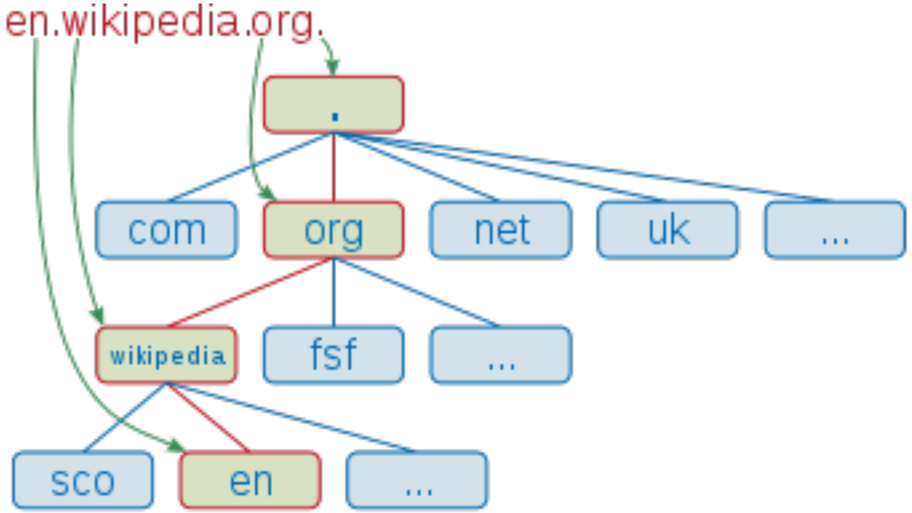
- Verify the sender by checking their email address
- Check the link, before you click — make sure the links start with https:// and not http://
- Be careful when providing personal information — never provide your credentials to third parties.
- Do not rush or panic react — scammers use this in order to pressure you into clicking links or opening attachments.
- If you gave sensitive information, don’t panic — reset your credentials on sites you've used them. Change your passwords and contact your bank immediately.
- Report all scams

THINGS TO CHECK WHEN BROWSING

- *Hover over links.*
- *Are the URLs legitimate?*
- *Message body is an image?*
- *Request for personal information? Urgency.*
- *Suspicious attachments*
- *Is my email address listed as the 'from' address?*
- *IP Reputation (Advanced)*

HOW TO CHECK AN EMAIL OR WEBSITE

- Check the domain: zzz@yyy.zzz The yyy.zzz is the domain.
- Visit https://whois.com and use whois search.



- Use Google search on the whole email address
- Use Google search on the url, make sure it is https and the name is spelt correctly

Thank you!!