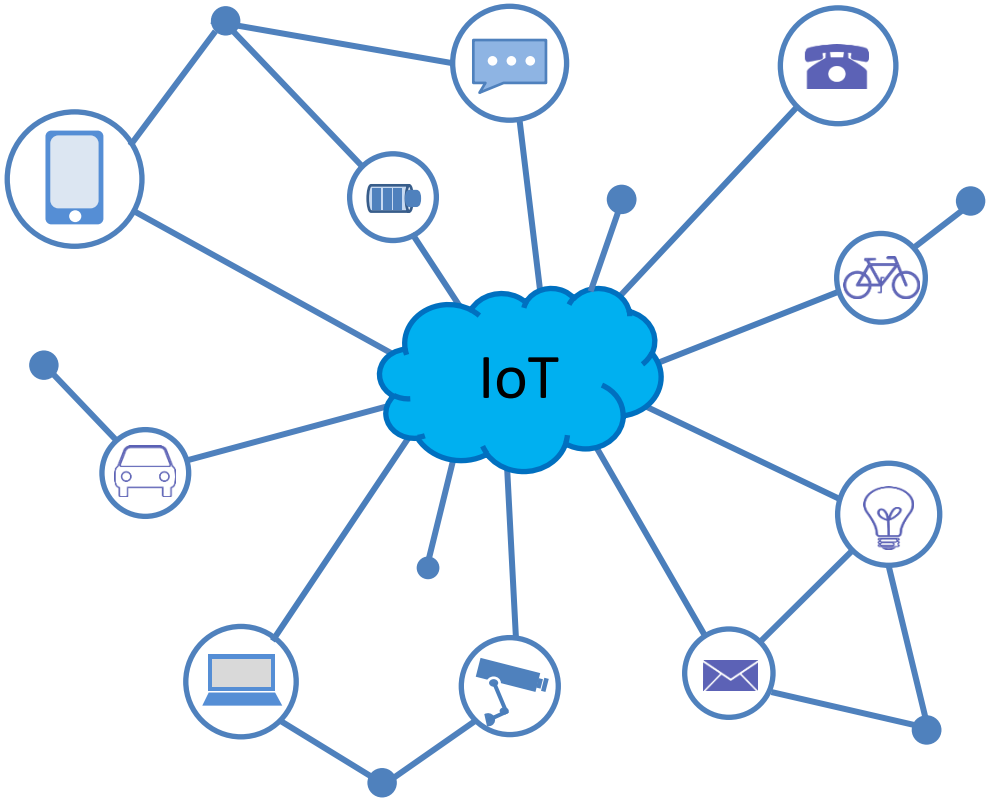
Security+ Bootcamp Session 1

with **Michael J. Shannon - CISSP, CCNP-SEC, Palo Alto PCNSE7, GSEC, Security+, ITIL 4 Managing Professional, and OpenFAIR**

The Threat Landscape

- There is no shortage of news about individuals, public and private organizations, and government agencies falling victim to an array of malware attacks
- The Internet of Things (IoT) means risk will not subside
- Organized criminal groups have vast resources to launch Advanced Persistent Threats (APTs)



Threat Agents

- Threat agents are the persons, methods, operations, techniques, systems, or entities that act – or have the potential to act – in order to initiate, transport, carry out, or in any way support a particular threat or exploit
- Also called a "threat actor"
- Individual or group

Attributes of Agents

- Internal/external
- Structured/unstructured
- Level of sophistication
- Resources/funding
- Intent/motivation

Structured vs. Unstructured Threats

- Structured threats
  - Planned
  - Organized
  - Persistent
  - Multi-phased
  - Can be internal or external
  - Exploit kits, zero-days, modules, ransomware
- Unstructured threats
  - Accidental
  - Non-malicious
  - Drive-by web surfing
  - No AUP
  - Poor awareness
  - E-mail and webmail
  - USBs and personal electronics

Script Kiddies

- Originates from the combination of inexperienced crackers using script viruses and prepackaged malicious code
- The most common script viruses are spread via e-mail attachments using scripts and modules from exploit kits
- Techniques are often learned on YouTube and other social media sites

Hacktivists

- Hacktivism unofficially began in the late 1980s when viruses and worms spread messages of protest, for example "Worms Against Nuclear Killers (WANK)"
- The term "hacktivism" was coined by the Cult of the Dead Cow (cDc), which also gave birth to "Hacktivismo," a group of international crackers protesting human rights abuses
- Responsible for DoS, DDoS, hijacking and defacing web sites, and other cyber attacks

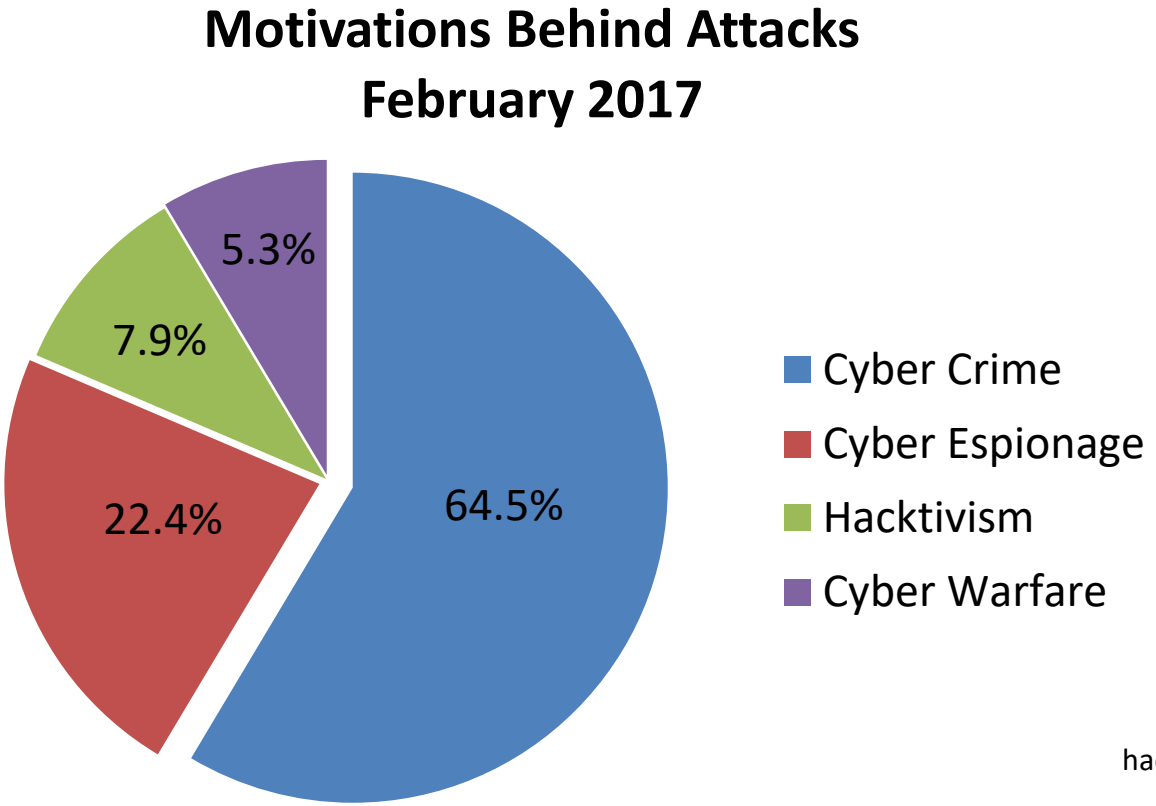
Organized Crime

- Attackers are not limited to just rogue individual script kiddies and small teams of hackers
- Organized crime is often implicated in attacks
- These attackers are remarkably shrewd and tricky and have huge supporting funds and human resources
- No industry or business sector is exempt from this threat

Nation States

- World War C involves many of the same activities as criminal syndicates
- Cyber warfare, espionage, and blackmail (blackstortion)
- Zero-day code is sitting on systems in every country placed by different countries
- DDoS attacks are of great concern today for government agencies and industries

Organized Crime and Nation States



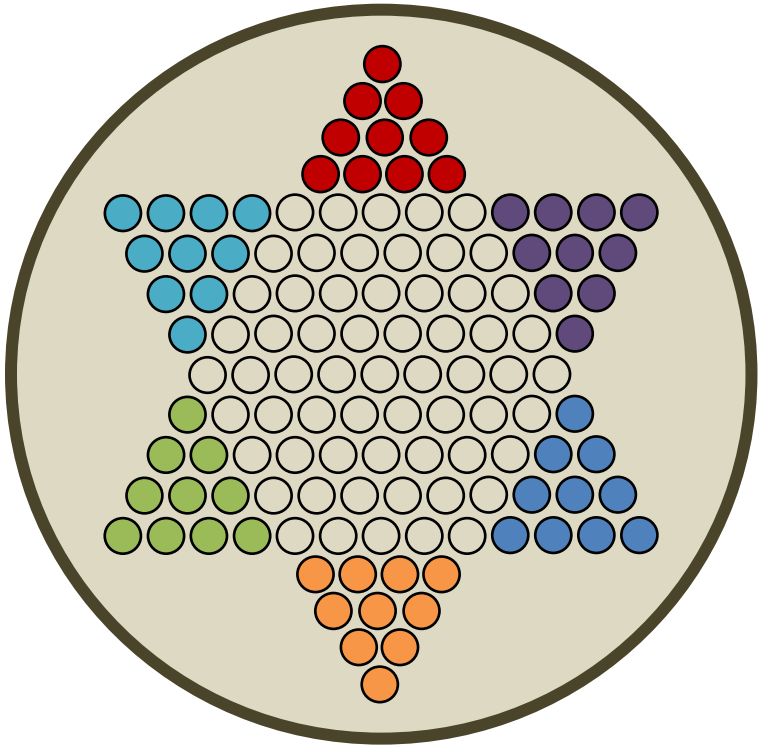
hackmageddon.com

Insiders

- APTs can involve getting someone hired in an organization with a clean background/fake identity that is part of the hacker team
- Disgruntled or desperate employees
- Individuals being blackmailed or coerced
- Normal people can commit fraud and embezzlement
- Background checks even on temp and contract workers

Competitors

- Corporate espionage to steal intellectual property (IP) – trade secrets, formulas, customer lists, processes, etc.
- Gain a competitive advantage by stealing marketing campaigns and secrets
- Hack web sites to ruin reputations and goodwill
- Sabotage to destroy stock value



Indicators of Compromise (IOCs)

- Indicators of Compromise (IOCs) are forensic artifacts of an incursion or disturbance
- Network-based and/or host-based
- Also called a "cyber-observable" – a measurable event or stateful property in the cyber domain
- The term “indicators of action” (IOA) is also used by professionals

Advanced Persistent Threats (APTs)

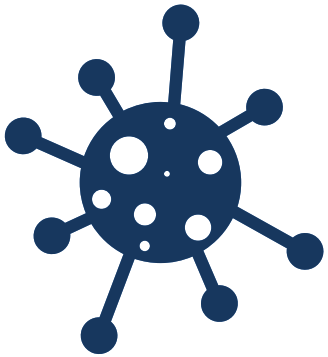
- Advanced Persistent Threats (APTs) involve
  - Bleeding edge, stealth malware, and zero-days
  - Cost/benefit analysis
  - Large amount of resource support
  - Long-term strategies
  - Unrelenting and focused

Advanced Persistent Threats (APTs)

- APT steps:
  1. Initial compromise
  2. Escalation of privileges
  3. Internal reconnaissance
  4. Lateral propagation, compromising other systems on track towards goal
  5. Mission completion

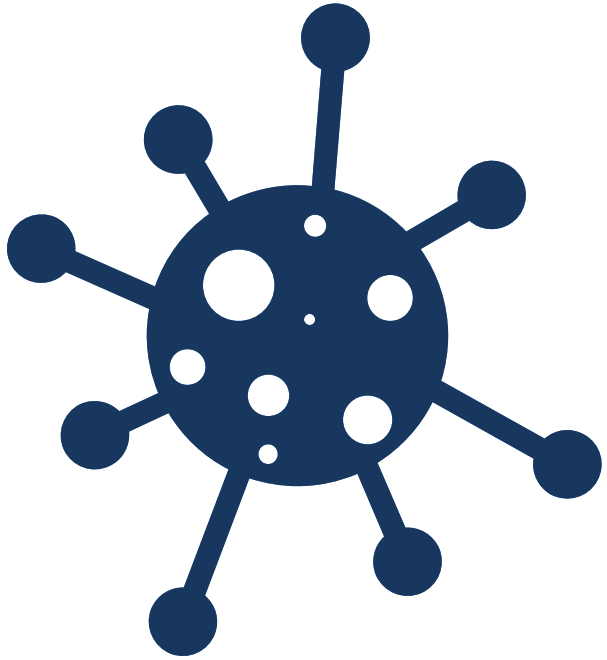
Viruses

- A virus is an unwanted and unsolicited malicious program or piece of code that can damage an electronic system
- By strict definition, viruses are not transferred without the help of human or system intervention
- They are commonly transferred from one system to another in many ways:
  - Sharing data
  - Adding/removing storage devices
  - Downloading files from the Internet
  - Opening phishing email messages



Virus Types

- File infector
- Boot sector/system infector
- Multipartite
- Polymorphic
- Script
- Encrypted
- Macro
- Companion



Ransomware and Cryptomalware

1. INSTALLATION

After a victim's computer is infected, the crypto-ransomware installs itself, and sets keys in the Windows Registry to start automatically every time your computer boots up.

2. CONTACTING HEADQUATERS

Before crypto-ransomware can attack you, it contacts a server operated by the criminal gang that owns it.

3. HANDSHAKE AND KEYS

The ransomware client and server identify each other through a carefully arranged "handshake" and the server generates two cryptographic keys. One key is kept on your computer, the second key is stored securely on the criminal's server.

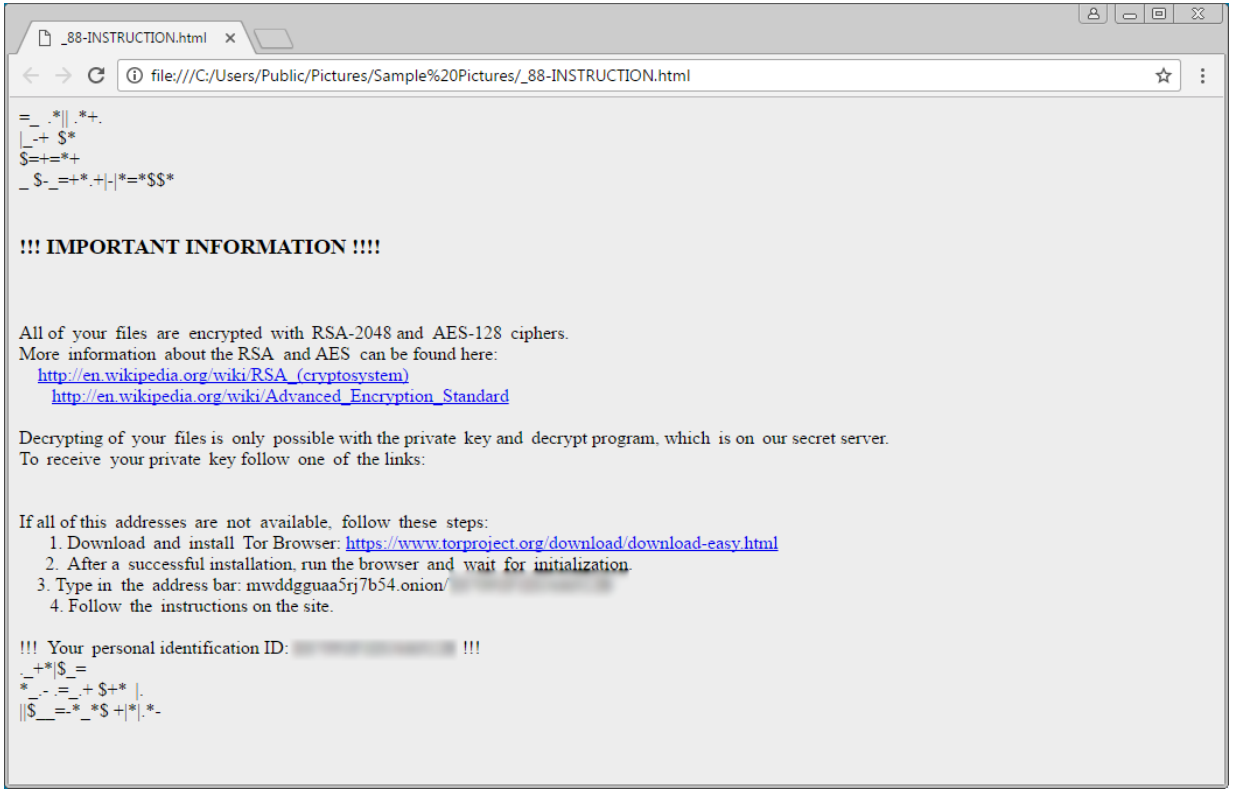
4. ENCRYPTION

With the cryptographic keys established, the ransomware on your computer starts encrypting every file it finds with any of dozens of common file extensions, from Microsoft Office documents to JPG images and more.

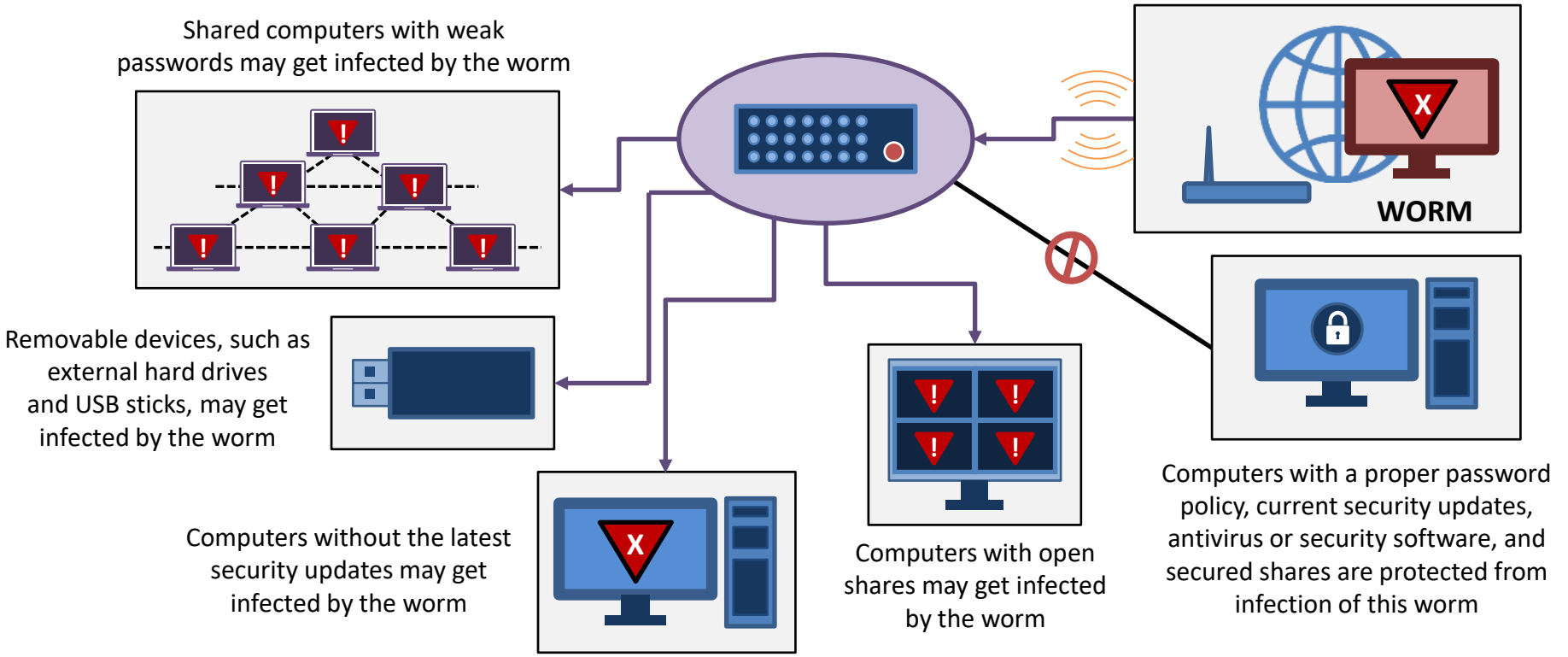
5. EXTORTION

The ransomware displays a screen giving you a time limit to pay up before the criminals destroy the key to decrypt your files. The typical price, $300 to $500, must be paid in untraceable bitcoins or other electronic payments.

Ransomware


_88-INSTRUCTION.html
file:///C:/Users/Public/Pictures/Sample%20Pictures/_88-INSTRUCTION.html
=_ .*|| .*+.
|_-+ $*
$=+=*+
_ $-_=+*.+|-|*=*$$*
!!! IMPORTANT INFORMATION !!!!
All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: mwddgguaa5rj7b54.onion/
4. Follow the instructions on the site.
!!! Your personal identification ID: !!!
._+*|$_=
_.- .=_.+ $+ |.
||$__=-*_*$ +|*|.*-

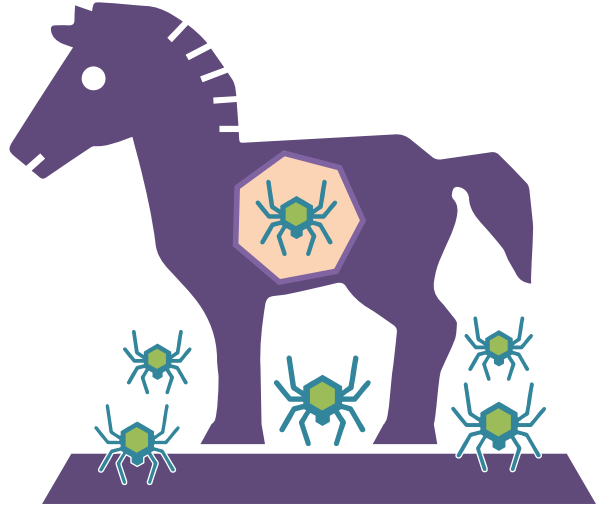
Worms



Classic examples are Sasser, ILOVEYOU, Conficker, Stuxnet

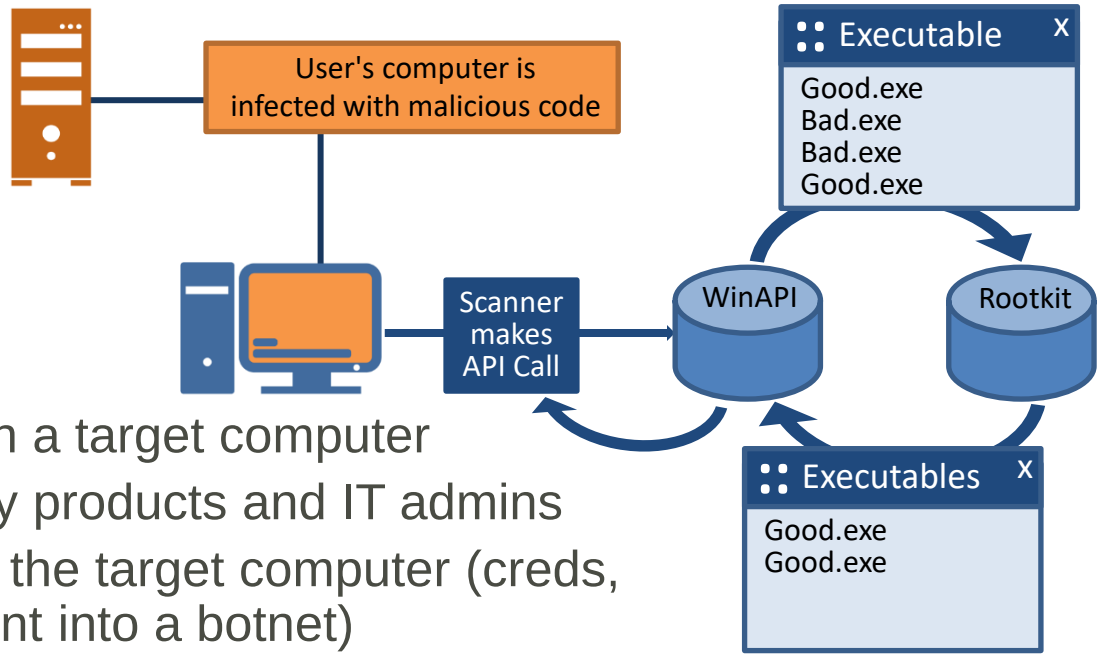
Trojans

- Malware that masquerades as a legitimate program:
  - Games and other apps
  - Device drivers
  - Utilities and tools
  - Freeware and shareware
  - System updates and upgrades
  - Patches
- Often installs backdoors, C&C, keyloggers, logic bombs, bots, ransomware, and more



Rootkits

- Rootkits are malicious modules that are placed in unauthorized areas to
  - Access data
  - Monitor actions
  - Escalate privileges
  - Modify programs
  - Conduct further exploits
- Three main goals:
  - To run without restrictions on a target computer
  - To go undetected by security products and IT admins
  - To exfiltrate something from the target computer (creds, remote access, or recruitment into a botnet)



Keyloggers

- Keystroke logging is typically done by malicious code that records keystrokes and sends data back to a C&C server
- Software is also used to track employees or family members to adhere to acceptable use
- It can also be used to study human-computer collaboration
- Keylogger detectors are special mitigation tools
- Spyware uses keyloggers to capture passwords, credit card information, or other PII
- **Examples: PAL KeyLog Pro, KeyGhost**

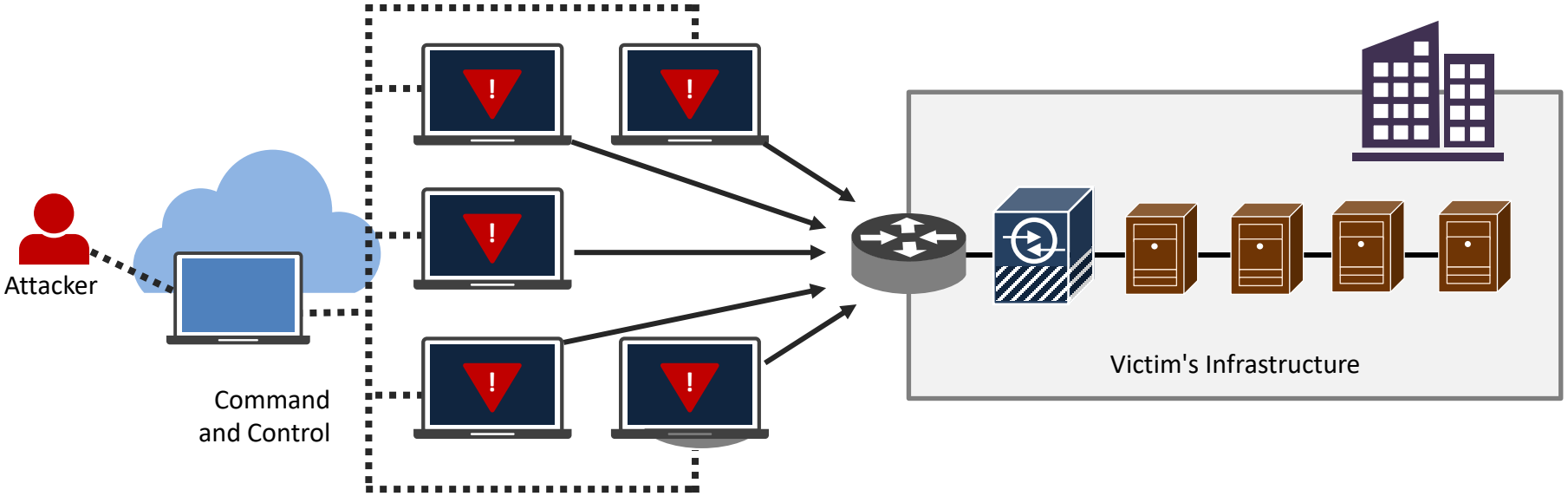
Spyware/Adware

- Spyware is software that gathers information about a computer user without the user's permission
- Spyware can show advertisements, track information, and make modifications to endpoints without user knowledge
- Malware, adware, and spyware are often found among P2P networks, download sites, and bit torrents
- Alexa, ECHO and similar “smart” appliances can be used as spyware

Bots and Botnets

- Bots are the most common form of Distributed Denial-of-Service (DDoS) attack today
- The robot network (botnet) consists of a zombie computer and a master command and control (C&C) server to remotely control victims, and many victims are unaware
- The communication often occurs over Internet Relay Chat (IRC), encrypted channels, bot-centric peer-to-peer networks, and even social media like Twitter
- Bots can exfil data, log keystrokes, scan memory, even force system to participate in mining cyber currency, and more

Bots and Botnets

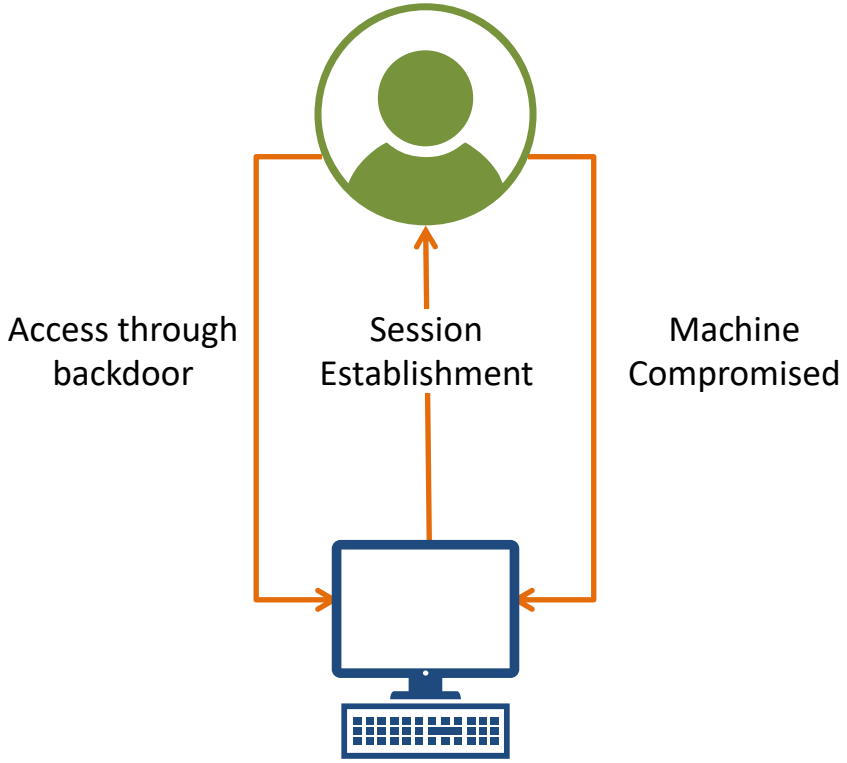


Remote Access Trojans (RATs)

- RATs are specific forms of Trojan horse malware – often part of multi-staged exploits
- Well-known for creating back doors to give malicious users access to the system
- Often seen in targeted attack campaigns to establish C&C communications
- New RATs allow for remote access to mobile devices
- **Well-known RATs include Gh0st, PoisonIvy, and Sakula**
- PlugX and variants are common choice for nation states

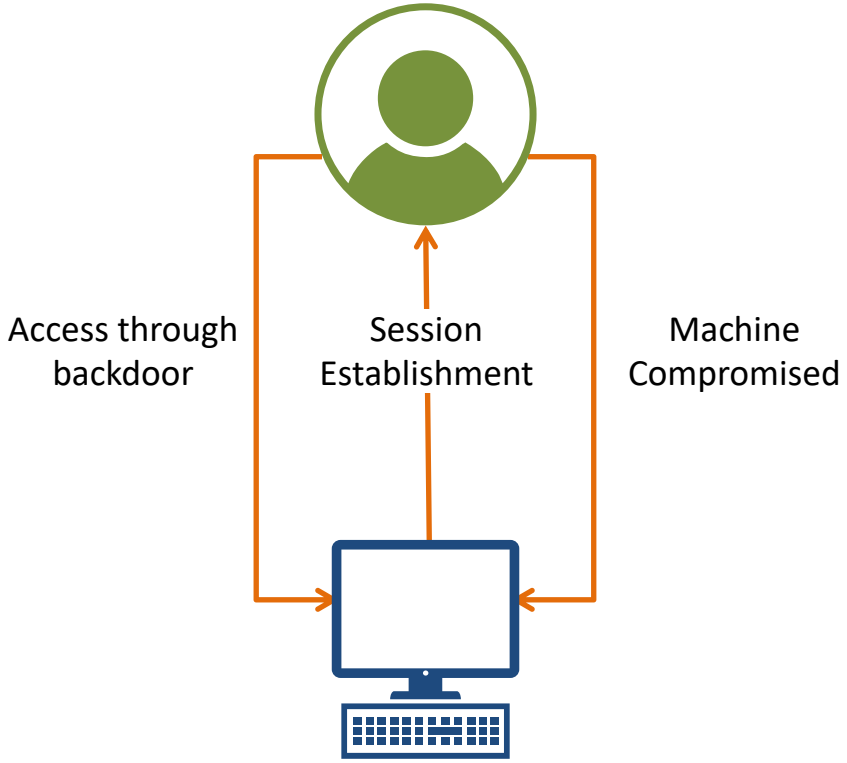
Backdoors

- Backdoors are Trojan programs that are closely related to the results of a botnet or DDoS attack
- This malware is used to generate a covert channel so that the remote attacker can access and control the system
- These are becoming more common on phones and other mobile devices

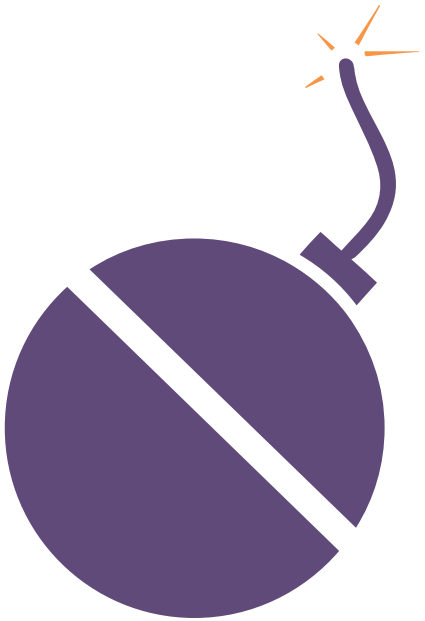


Backdoor Exploits

- Perform DoS attacks on other systems (DDoS)
- Run and terminate tasks and processes
- Download additional files for multi-phased attack
- Upload files and other content
- Audit the system status
- Open remote command line shells
- Modify computer settings
- Shut down or restart the system



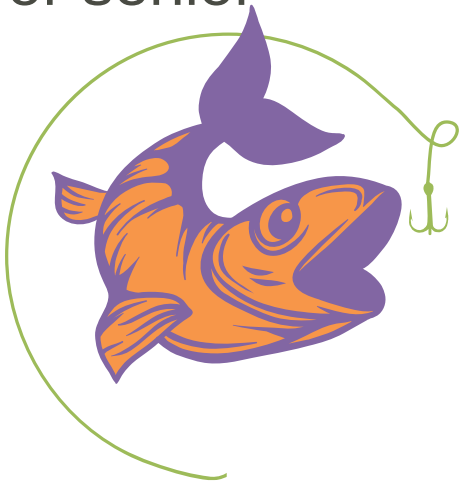
Logic Bombs



- Logic bombs trigger the exploit when a certain event occurs:
  - Mouse movements
  - File access
  - Date and/or time
  - Program execution
  - Number of times code is run
  - During a major event
  - On a holiday

Phishing, Spear Phishing, and Whaling

- Email phishing attacks or hoaxes are one of the most common exploit vectors available to crackers
- Spear phishing is targeting certain employees
- Whaling is targeting high-level employees or senior management and directors



Phishing, Spear Phishing, and Whaling

- There are key indicators in email and webmail to identify:
  - Vague salutations – "Dear valued customer"
  - Suspicious looking display names or domains – company name is farther into the URL path
  - Wrong information when you hover mouse over links
  - Awkward grammar and misspelled words
  - Subject line has urgent or intimidating phrases
  - Lack of legitimate contact information
  - Spoofed headers and logos

Vishing and Smishing

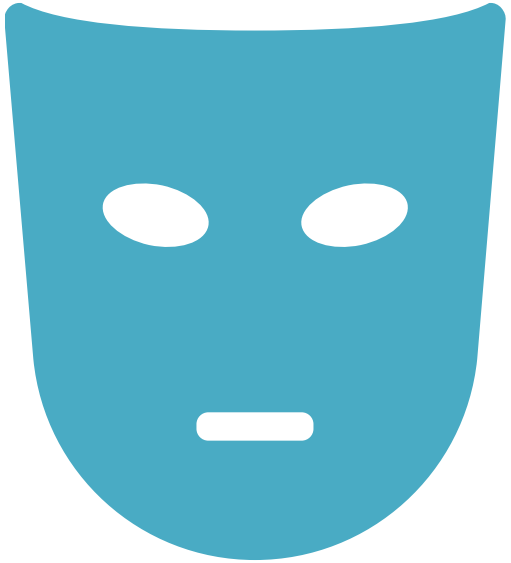
- Vishing uses the same process as phishing, except that it targets cell phones, telephones, and VoIP systems as its vector instead of email
- For instance, a cracker (visher) may call spoofing a collection agency and claiming that the potential victim is delinquent in a loan payment – they will attempt to get PII such as the social security numbers or credit card information
- Smishing uses SMS texting as the vector instead of email

Tailgating and Piggybacking

- Tailgating occurs when access tokens or badges are being used in a single-factor or multi-factor authentication scheme for physical access to buildings, rooms, or certain high-security areas such as datacenters

Impersonation and Hoaxing

- Janitors and cleaning services
- Pest control
- Fire/building inspectors
- Temporary or contract workers
- Security professionals
- Auditors
- Penetration testers
- Newly hired employees
- Relatives of management



Dumpster Diving

- Dumpster diving is an attack where the goal is to reclaim important information by inspecting the contents of trash containers and dumpsters

- Credit card information
- Invoices and receipts
- IP addressing
- Organization charts
- Names of key employees
- Manuals and charts
- Memos and sticky notes

Shoulder Surfing

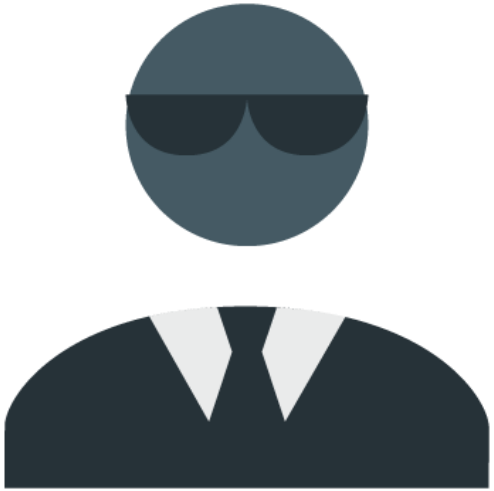
- An attack where the goal is to look over the shoulder of an individual as he or she enters password information or a PIN
- This is much easier to do today with camera-equipped mobile devices
- Binoculars and telescopes from nearby buildings can see screens and keyboards

Watering Hole Attacks (Social Networks)

- Watering hole attacks leverage a compromised web server in order to target particular groups or associations
- Only members of the association are attacked, while other traffic is untouched
- Watering holes are difficult to identify using traffic analysis since most traffic from the infected site is benign

Reasons for Phishing Effectiveness

- There is a reason why email and web-based attacks are so successful:
  - Authority
  - Intimidation
  - Consensus
  - Scarcity
  - Familiarity and trust
  - Urgency



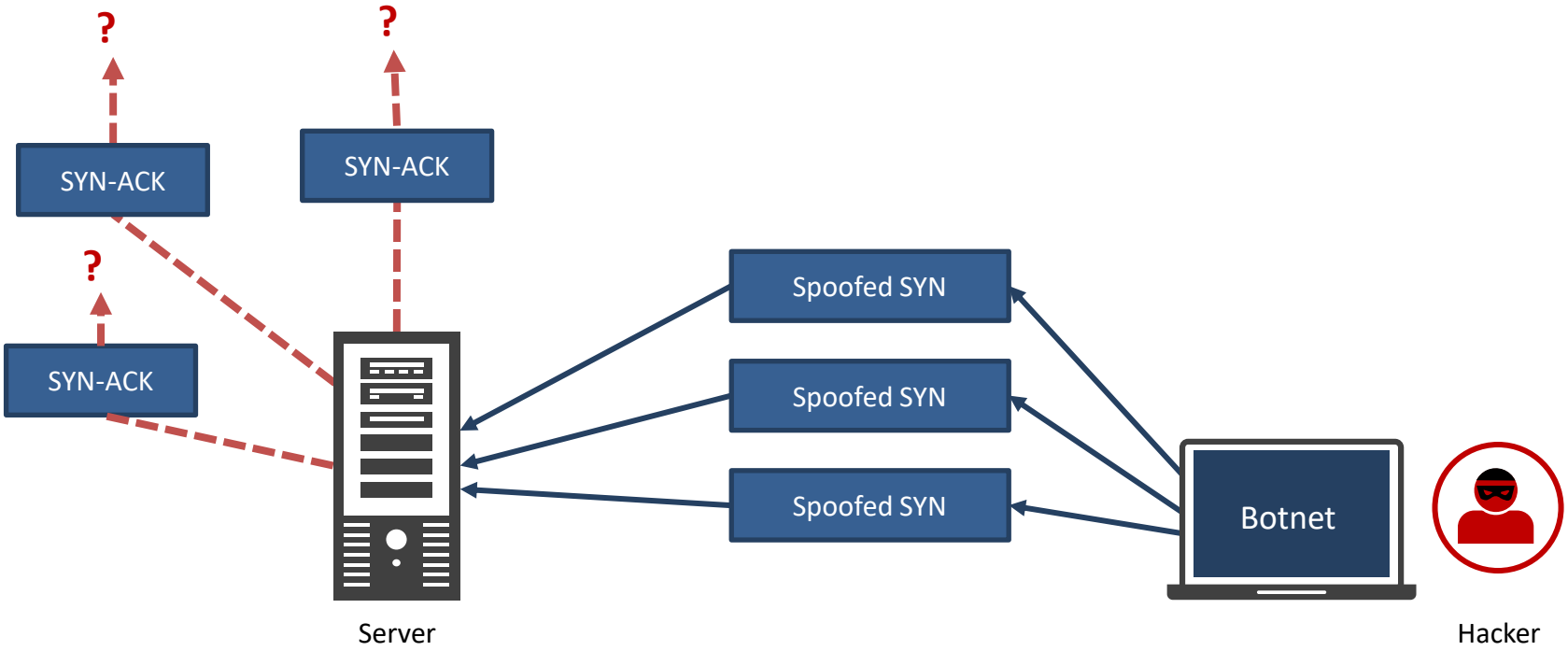
Use of Open-source Intelligence (OSINT) in Threats

- OSINT is retrieving anything in the public domain (broadcasts, courthouse documents, web searches, FOIA documents, social media, content on the dark web
- Can be used as a countermeasure or as an exploit in the reconnaissance phase of an APT
- **Common tools are Shodan, Google Dorks, and Maltego**

DoS and DDoS Attacks

- Denial of Service attacks are some of the oldest exploits that leverage inherent weaknesses in the TCP/IP stack
- DoS attacks try to consume a systems (or networks) critical resources such as disk space, CPU cycles, memory (switch CAM tables), bandwidth, input queues, DHCP leases, etc.
- DoS attacks are still common and a major risk, because they can effectively interrupt business operations
- They are fairly simple to conduct with script kiddie tools

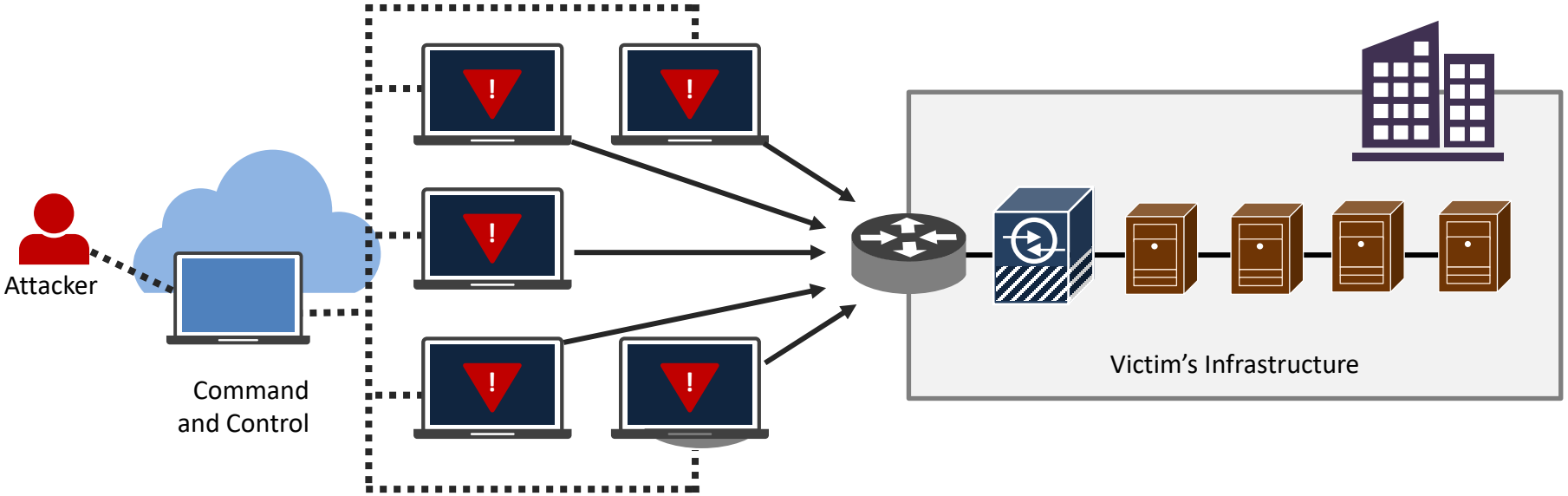
Classic TCP SYN flood DoS Attacks



DDoS Attacks

- Malicious “zombiefied” hosts can also combine to flood a victim with many attack packets simultaneously from potentially thousands of sources
- This is a Distributed DoS (DDoS) attack which are often sourced from networks of compromised systems called botnets
- A botnet consists of a group of systems loaded with computer robot code (or bots)
- A command and control (C&C) server control mechanism directs the zombie computers remotely, often by using Internet Relay Chat (IRC), peer-to-peer, or even Twitter

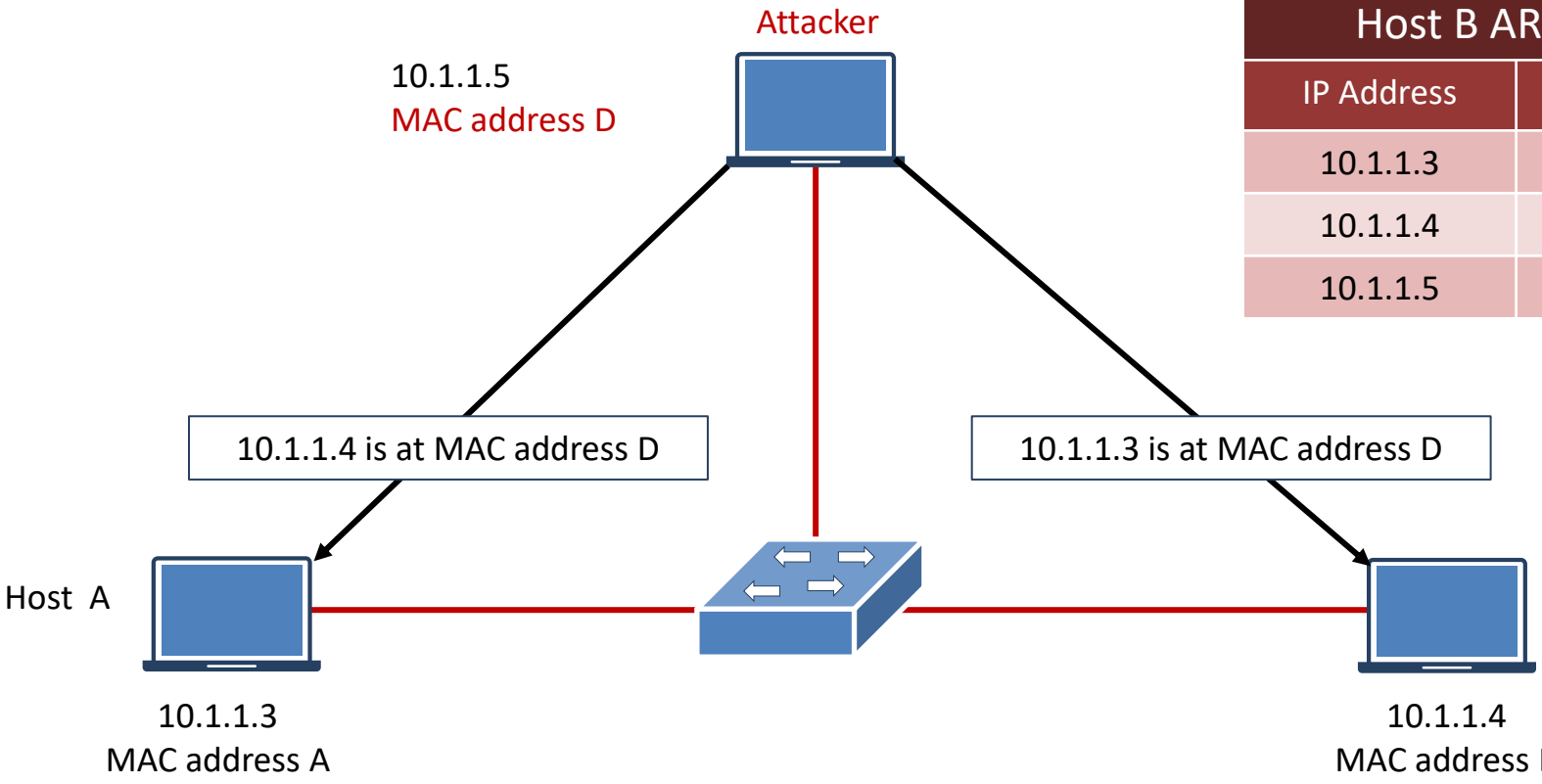
DDoS Attacks



Man-in-the-middle Attacks

- A Man-in-the-middle can be good (Proxy, ALG, translators) or it can be dangerous (Proxy ARP, DHCP Spoofing)
- A system with the ability to view the communication between two (or more) hosts (frames, packets) injects itself in the path between the hosts systems
- They are complex attacks that can be simplex or duplex at different layers of the OSI model

Man-in-the-middle Attacks



Host B ARP Table	
IP Address	MAC Address
10.1.1.3	D
10.1.1.4	R
10.1.1.5	D

Buffer Overflow Attacks

- A buffer overflow exploits flaws in application and operating system design and deployment
- If a service expects an input to be within a certain window size but does not verify, it may be vulnerable to a buffer overflow attack
- The attacker sends larger than expected input, for example the web server accepts and writes to memory
- Associated buffers are filled, and adjacent memory is overwritten as a result. This overwrite may contain instructions or code that crash the server resulting in a DoS

Injection Attacks

- This attack is often the result of MITM or RAT attack
- Can inject false MAC or IP addresses
- SQL Injection attacks are very common against Web servers
- Exploit tools like Loki can inject bad information to routers that do not authenticate their peers or neighbors
- STP attacks can inject spoofed BPDUs

Cross-site scripting (XSS)

- Flaws in pages rendered by web servers and not the web server code itself (i.e. Apache, IIS)
- Involves injection of malicious scripts or code into trusted or innocent web sites pages
- Attacker typically sends browser-side scripts to end user
- Can occur anytime a web program uses user input within the output it generates without validating or encoding
- Malicious script can steal cookies, session tokens, or other sensitive data stored by the browser and used with the site

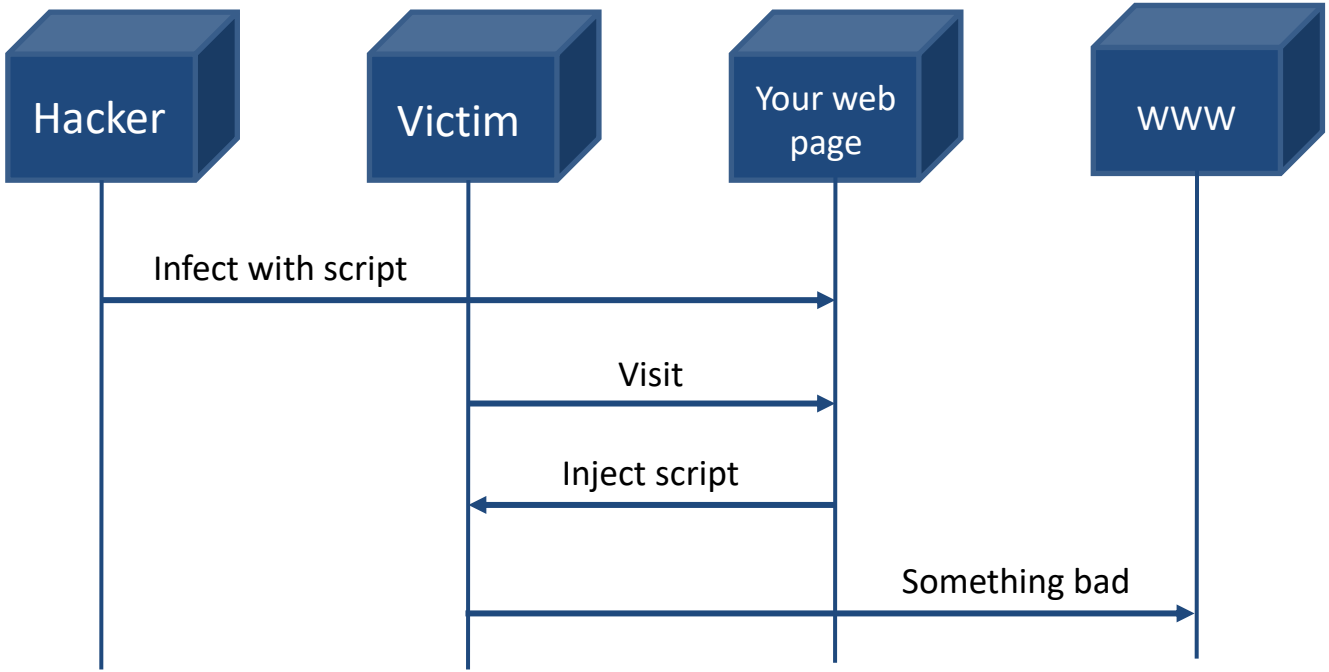
DOM-based XSS

- Also called Local XSS or Type 0
- Does not involve vulnerable web servers
- Insecurely written HTML page on end user’s system or local gadgets and widgets
- Allows the attacker to manipulate the DOM through untrusted input
- They can render input that might lead to other XSS vulnerabilities

Reflected XSS

- Also called Nonpersistent XSS or Type 1
- A classic input trust vulnerability where the application is expecting some input (i.e. a query string) and the attacker sends something developer did not expect
- Example: attacker provides a JavaScript code fragment as the querystring and the victim clicks on the link
- Prevalent since it’s not feasible to turn off all scripting in browsers

Cross-site Scripting (XSS)



Server XSS or client XSS

Stored XSS

- Also called Persistent XSS or Type 2
- A variant of type 1 where, rather than reflecting the input, the web server persists the input
- The user is served up later to unsuspecting victims
- Difference is an intermediate phase where the untrusted input is stored in a file or a database before unloading on the victim
- Often found in blogs and review/feedback web applications

Cross-site Request Forgery (CSRF)

- Attack forces an end user to perform undesirable actions in a web application in which they are authenticated
- An effective CSRF attack can force users to perform state-changing requests such as
  - Transferring funds
  - Changing their e-mail address
  - Changing their password
- If the victim is an administrative account, the CSRF attack can compromise the entire web application

Privilege Escalation

- Advanced Persistent Threats (APTs) often attempt an escalation of access privileges soon after the initial compromise
- The goal is to become a root or administrative user, level 15 user on a switch or router, exec user, Domain Admin group member, etc.
- The higher the level, the broader the access, the more potential there is to damage or exfiltrate critical data
- Least privilege principles are key

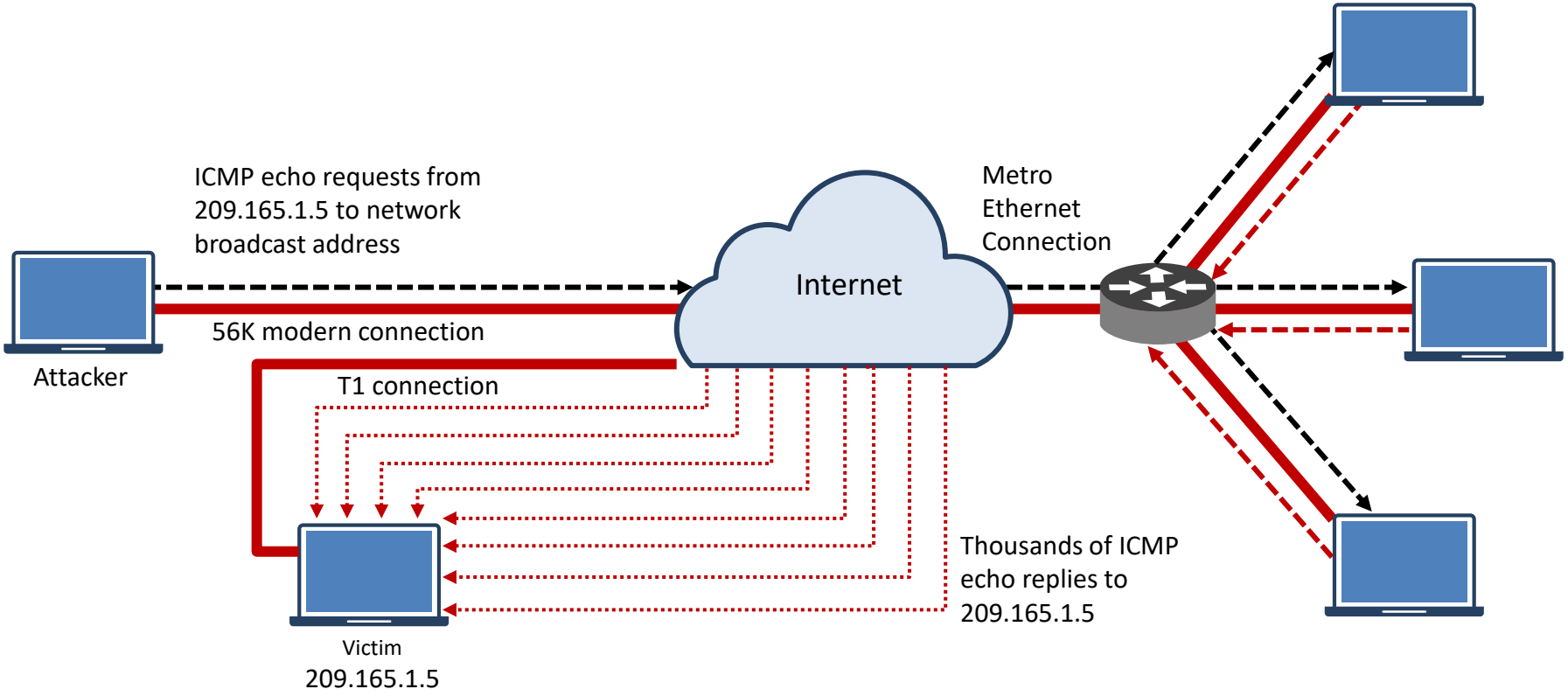
ARP poisoning

- A form of Man-in-the-middle attack that exploits ARP
- Malicious hosts injects false frames in order to corrupt (poison) the ARP cache buffers on endpoints, switches, servers, firewalls, and routers
- Only works in IPv4 networks – not IPv6
- Exploit kits have several scripts, module and tools to compromise the ARP protocol.
- It can be mitigated with port security, snooping binding databases on switches and MACsec implementation 802.1AE

Reflection and Amplification

- An attacker spoofs the source IP address of the packets so that it is actually the IP address of the anticipated target
- Hosts that receives these packets become reflectors when they reply by sending response packets to the spoofed address
- If the request packets (for example, DNS) solicit a larger response, the attack also becomes an amplification attack
- Reflection and amplification are two separate elements of an attack
- Attackers can use amplification with a single reflector or multiple reflectors (like IPv6 amplification)

Reflection and Amplification



Spoofing

- Spoofing is posing as something it is not
- It is not necessarily a type of attack but rather a technique
- Often the early phases of a reconnaissance attack or structured DoS attack
- The spoofed source address is often the ultimate target as devices perform return amplification
- Can be an external system masquerading as an internal system or vice-versa

Spoofing

- Attackers can spoof:
  - MAC addresses
  - IPv4 and IPv6 IP address
  - DHCP, ARP, and other services
  - Routers
  - Domains and URLs
  - Web sites and email addresses

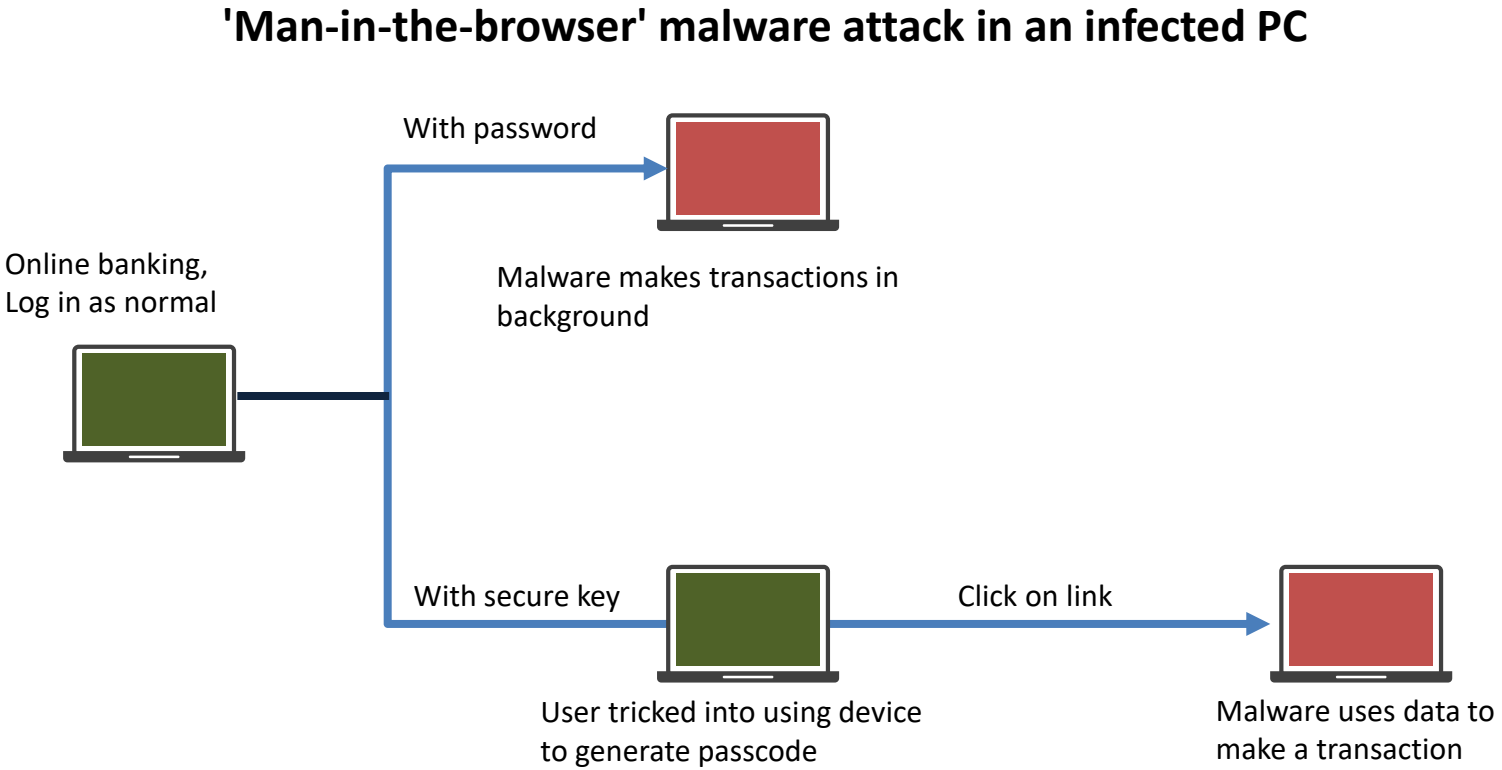
DNS Poisoning

- DNS poisoning is when an attacker changes the name resolution information that should be in a DNS server's cache, so that client systems are redirected to incorrect websites
- This is accomplished by name server misconfiguration, improper software design, and malicious exploits designed for the DNS system
- When a DNS cache is poisoned, it is often changed in order to redirect requests for a domain to a different address and website
- This other site could be performing phishing, pharming or some other malicious activity

Domain Hijacking/Clickjacking

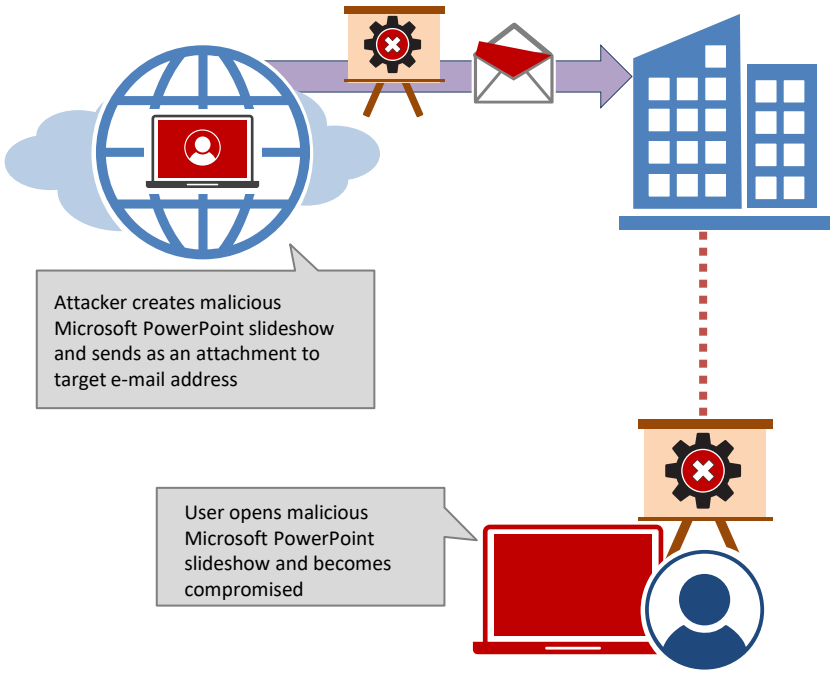
- Also called User Interface redress attack, UI redress attack, and UI redressing
- Hacker uses several transparent layers to trick users into clicking on a button (or link) on another web page when they were actually trying to click on the top-level web page
- Attacker hijacks clicks meant for their page and routes them to another page, often controlled by another domain or application
- Keystrokes can also be hijacked with skillfully constructed iframes, CSS, and text boxes

Man-in-the-Browser



Zero Day Attacks

- Zero-day exploits (also zero-day or zeroday) are unpublished exploits that security software vendors, IPS sensors, firewalls, cloud security services and more are presently unaware of
- There is an entire black market creating and selling this code
- Many state-based and organized crime groups use these

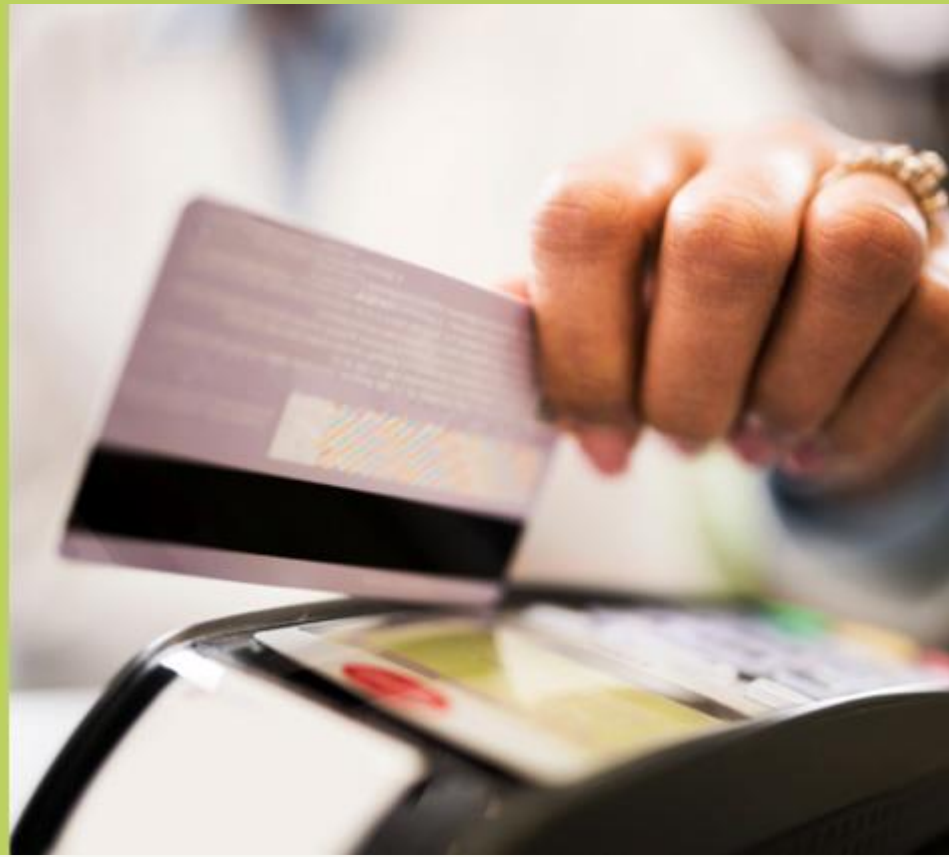


Pass the Hash Attacks

- Sometimes the authentication process relies on the password's cryptographic hash and there are various tools to extract these hashes (Cain) from compromised Windows machines (lately Windows 10) and use them to access other services
- This technique is known as pass-the-hash and is one of attacks that Windows Virtual Secure Module (VSM) was intended to protect against
- Example: On Windows networks, hackers do not need the plaintext passwords to access certain services

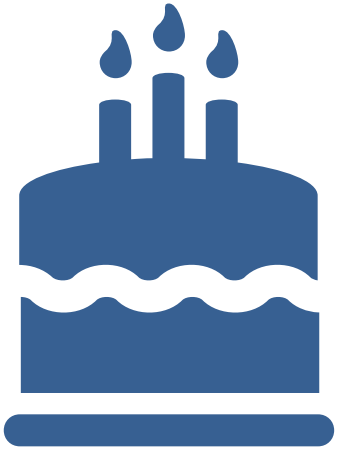
Driver Manipulation

- **Shimming** is the process of stealing information and money from Point-of-Sale systems, credit card readers, and ATM machines
- **Refactoring** involves changing an application's source code without modifying the characteristics
  - Often used to introduce legacy applications into new computer systems and devices
  - Can also re-engineer classic attack code to create variants and hybrid viruses and worms



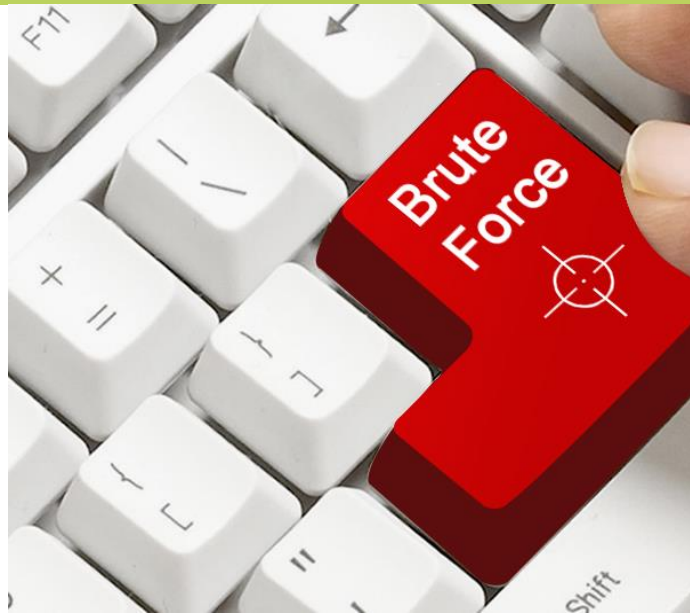
Birthday Attacks

- A birthday attack exploits the math behind the birthday paradox in probability theory
- In probability theory, in a room with 23 people or more, the odds are greater than 50% that two will share the same birthday
- These are commonly used to create collisions in hashing protocols where to different inputs generate the same output
- This has been done with MD5



Known Plaintext and Ciphertext-Only Attacks

- Known plaintext attack – the attacker has access to the ciphertext of several messages, but also knows something about the plaintext that underlies that ciphertext (also called meet-in-the-middle)
- Ciphertext-only attack – the attacker has the ciphertext of several messages, all of which have been encrypted using the same encryption algorithm, but the attacker has no knowledge of the underlying plaintext



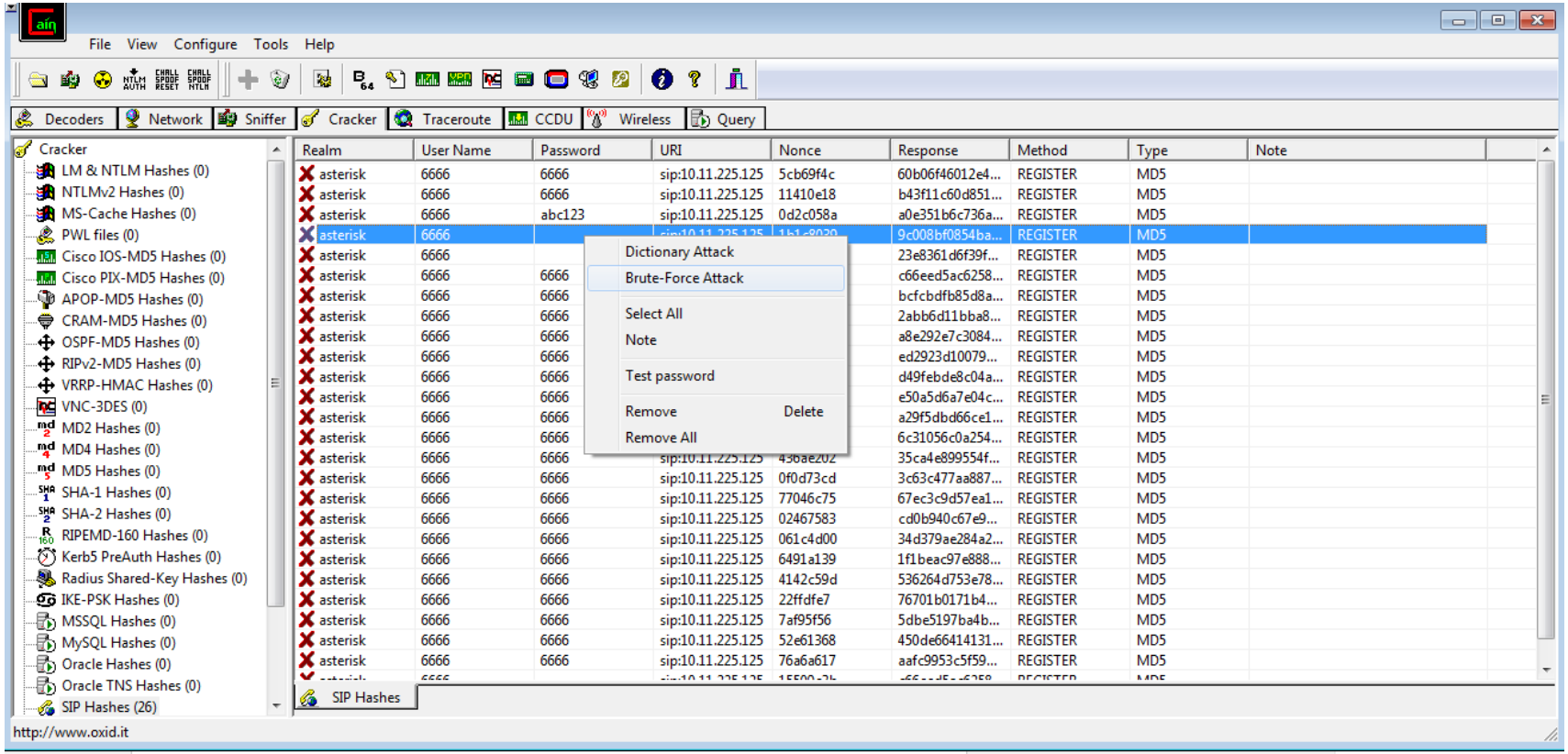
Rainbow Table Attacks

- The attacker attempts to use a rainbow hash table to crack the passwords stored in a database system
- A rainbow table is a hash function used in cryptography for storing important data such as passwords in a backend database for a web service
- Sensitive data is often hashed multiple times with the same or different keys in order to avoid rainbow table attacks

Brute-Force and Dictionary Attacks

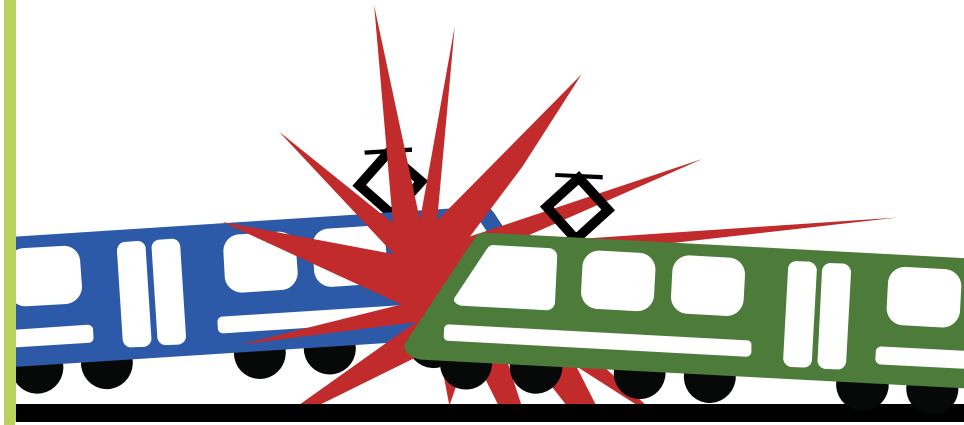
- Repeated attempts to identify a user account, password, or both
- Also runs against stored hashes on systems (or offline)
- Hackers use many tools and techniques to crack passwords:
  - Online and offline brute force
  - Dictionaries, word lists
  - Rainbow tables
  - Cracked password lists
  - Hybrid cracking

Brute-Force and Dictionary Attacks



Collisions

- Hash algorithms produce a fixed-length output and there are a finite number of possible outputs
- It is possible for two different inputs to produce an identical output – this is a hash collision
- MD5 should be avoided since it can generate collisions – two files with the same fingerprint – one is benign, and one is malware



Downgrade Attacks

- An attack that takes advantage of an application's and/or service's ability to give up a newer and more secure method of communication (encrypted) and "fall back" to an older, less-optimal mode (clear-text) for backward compatibility
- SSL/TLS is particularly vulnerable (OpenSSL)
- The POODLE attack is a man-in-the-middle exploit that leverages Internet and security software clients' willingness to fall back to SSL 3.0

Introduction to Cryptology

- Cryptography
  - Study and practice of securing communications
  - Encryption and hashing
- Cryptanalysis
  - Study and practice of exploiting weaknesses in communications

Cryptography Services

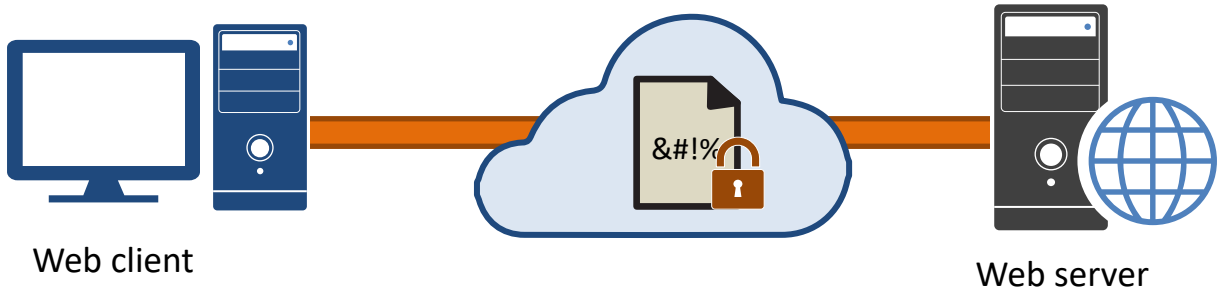
- Confidentiality
  - Hiding the real information from unwanted eyes
  - Often involves a system that converts plaintext data into ciphertext
  - Data at rest, in transit, in use
- Integrity
  - Ensures the data has not been altered
  - Often attaches a digest or fingerprint to the data through cryptographic hashing
  - At rest, in transit, in use

Cryptography Services

- Availability
  - Protecting systems from flooding and denial-of-service techniques
  - Controls that provide redundancy, failover, and backups
- Non-repudiation
  - Ensures original sender can't deny sending data or transaction
  - Commonly used digital signatures

Encryption

- Implemented at different OSI layers
  - Application
    - PGP
  - Session
    - SSL/TLS
  - Network
    - IPsec
  - Datalink
    - MACsec



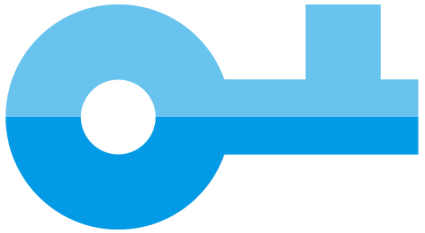
Cryptographic Keys

- Sets of alpha-numeric characters used for converting plaintext to cipher text
  - Encryption
  - Digital signatures
  - Hash functions
  - Message authentication codes

- The ciphers, algorithms, and protocols are open source
- Keys can be generated manually, using Random Number Generators (RNG), and Pseudorandom Number Generators (PRNG)
- Key must be large to prevent a successful brute force attack

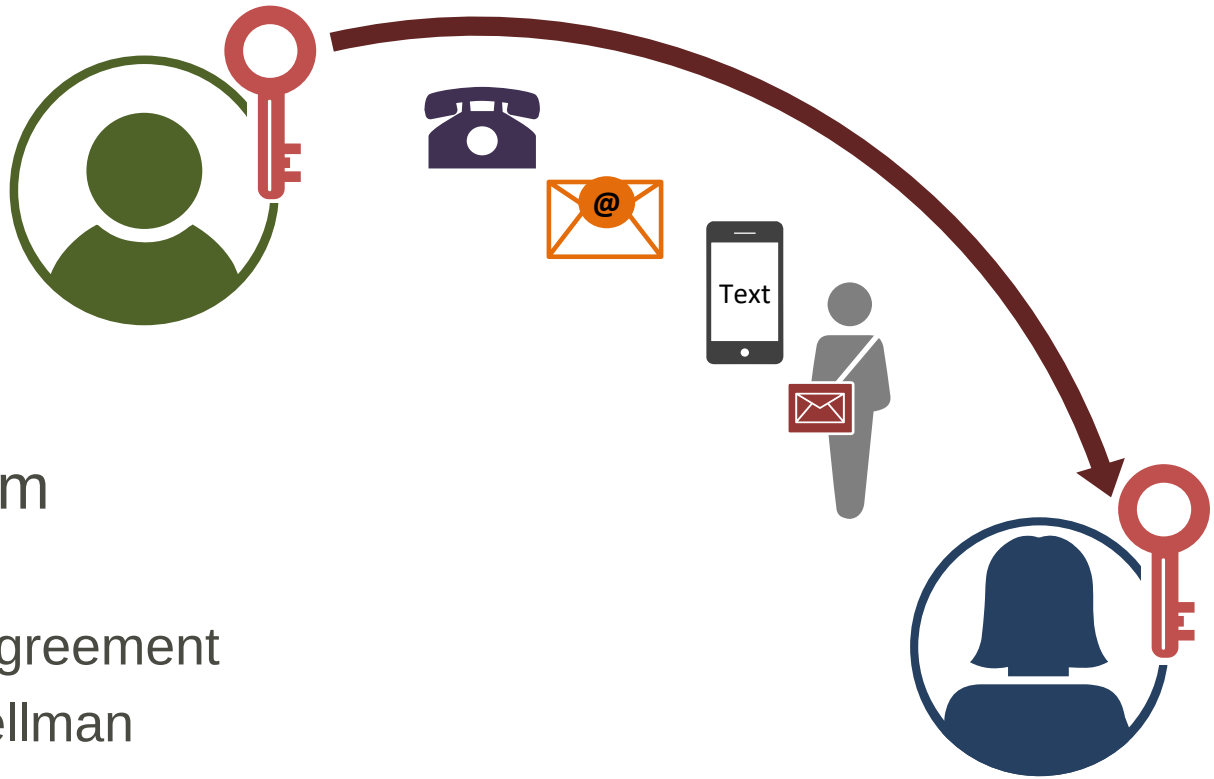
Keys

- Static key
  - Used for a long period of time
    - Used multiple times for different key establishment processes
- Session key
  - A single-use symmetric key used for an entire session
    - Encrypts and decrypts all messages for the specific session
    - Limits amount of information encrypted with key
      - Makes many cryptanalytic attacks more difficult
- Ephemeral key
  - Used for a very short period of time
    - Used for only one single key establishment processes



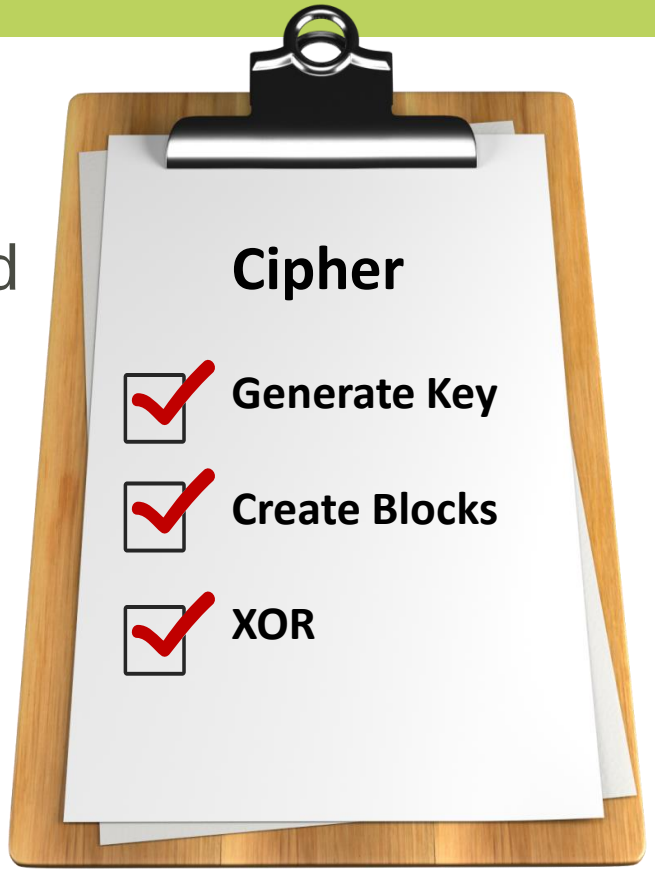
Key Exchange

- Phone
- Email
- Text
- Couriers
- Diplomatic bags
- Asymmetric algorithm
  - RSA – key exchange
  - Diffie-Hellman – key agreement
  - Elliptic Curve Diffie-Hellman



Ciphers

- An algorithm used for encryption and decryption
- Outlines the procedures that are followed
  - Well-defined series of steps
- There are many different types – from simple to complex
- Often involves transposition, diffusion, and confusion techniques

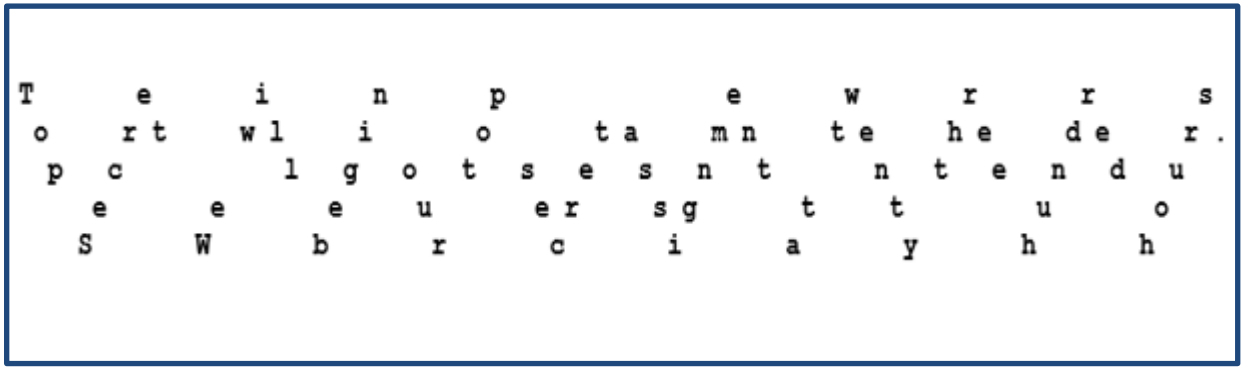


Ciphers

- Transposition
  - Rearrange or permutate letters
  - Example: Rail Fence cipher
  - Modern systems like AES are much more complex (layers)

Top Secret

We will begin our top secret assignment at twenty three hundred hours



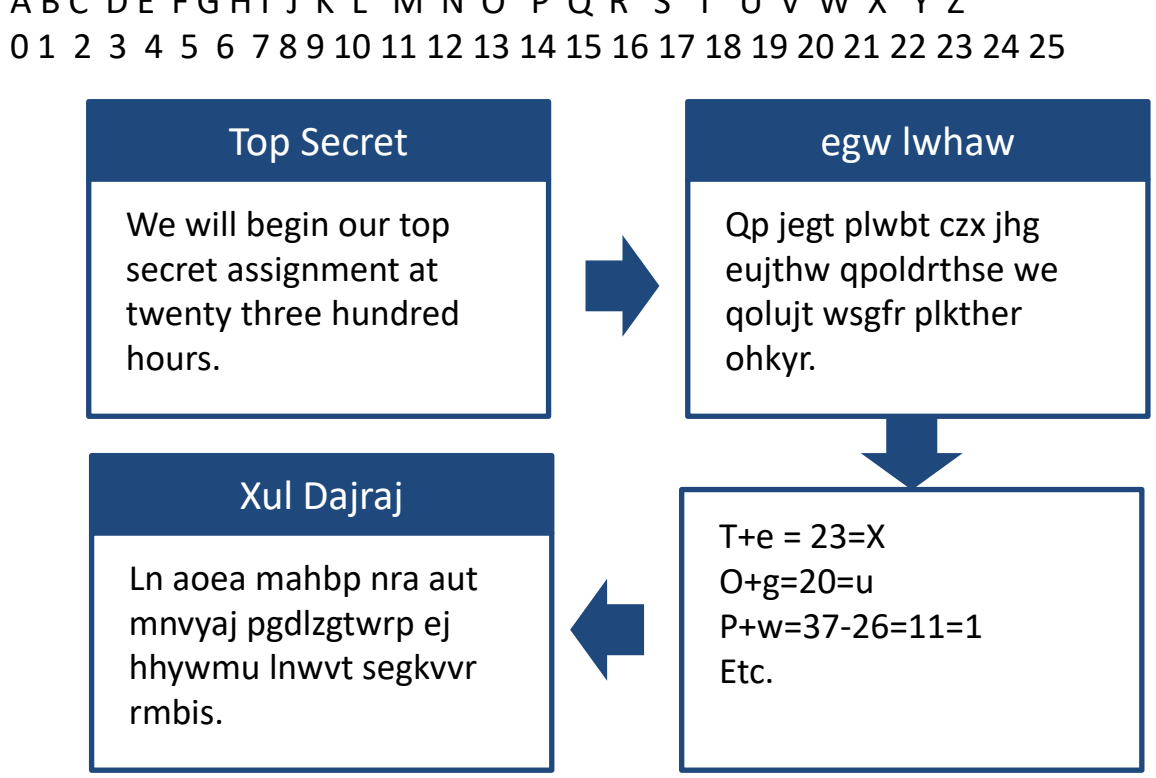
Teinp ewrrsortwli o
Tamnteheder.pc
Lgotsesnt ntendu e
E eu ersg tt u
oSWbrciayhh

Properties of Secure Ciphers

- Confusion
  - Output is drastically different from the input
    - Bits in ciphertext are a result of multiple parts of the key
    - Use non-linear table to translate data
- Diffusion
  - Single input character changes will affect multiple output characters
    - Each input bit should change half or more of the ciphertext bits
      - Avalanche effect
    - Makes patterns harder to spot

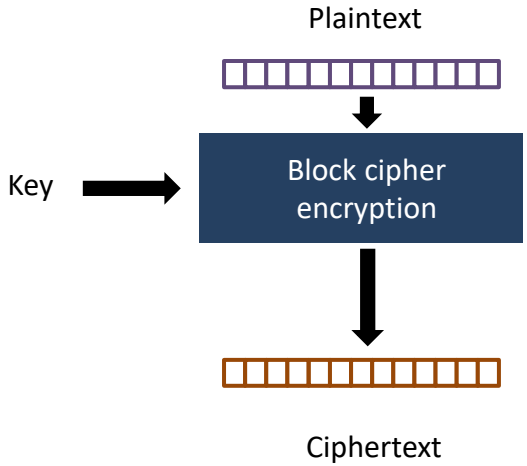
One-time Pad

- One-time pad
  - One-time random pre-shared key (PAD)
  - Key is added to plaintext bits using modular addition
  - The Vernam cipher
  - Depends on a truly random key



Block Ciphers

- Operates on fixed blocks of data (bits) based on key size
  - 64, 128, and 256 bits are common
  - Messages bigger than key size are broken into blocks the size of the key and must include padding
- Common block ciphers
  - DES
  - 3DES
  - AES-CBC
  - AES-GCM
  - Blowfish

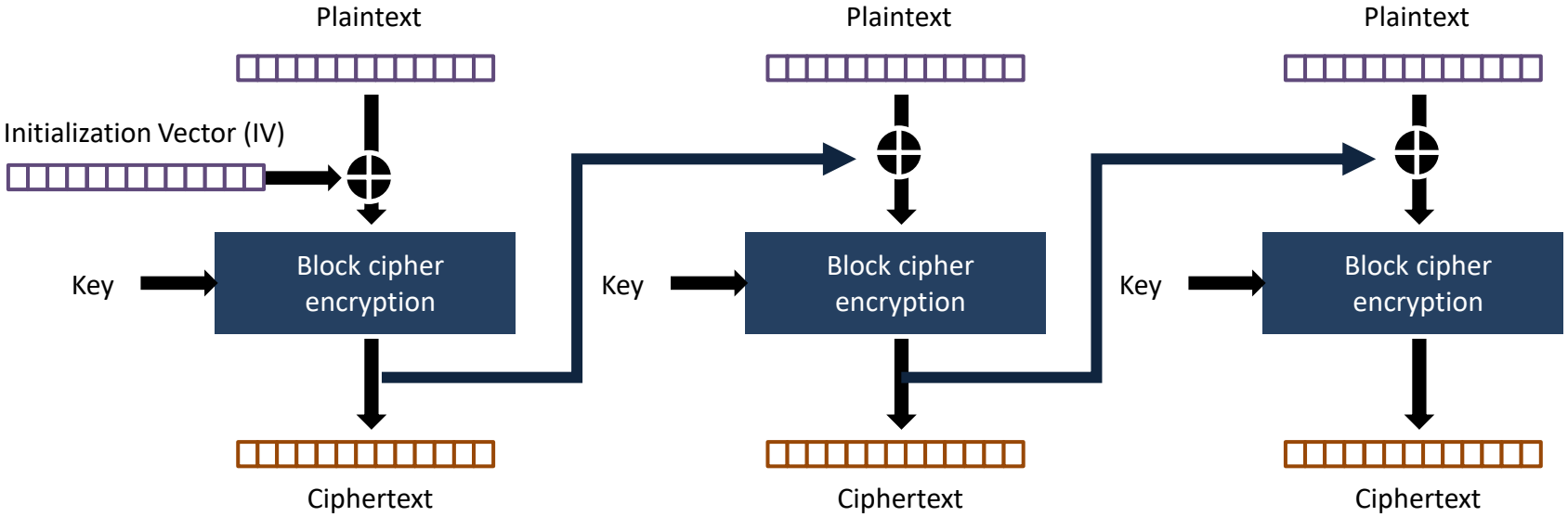


CBC (Cipher Block Chaining)

- Popular method
- Splits message into blocks the same size as the key
  - adds padding to the last block if needed
- XOR first block with IV and then encrypt with a key
- XOR second block with ciphertext of first block and then encrypt with key
- XOR third block with ciphertext of second block and then encrypt with key
- Continue until all blocks done

Block Cipher Modes

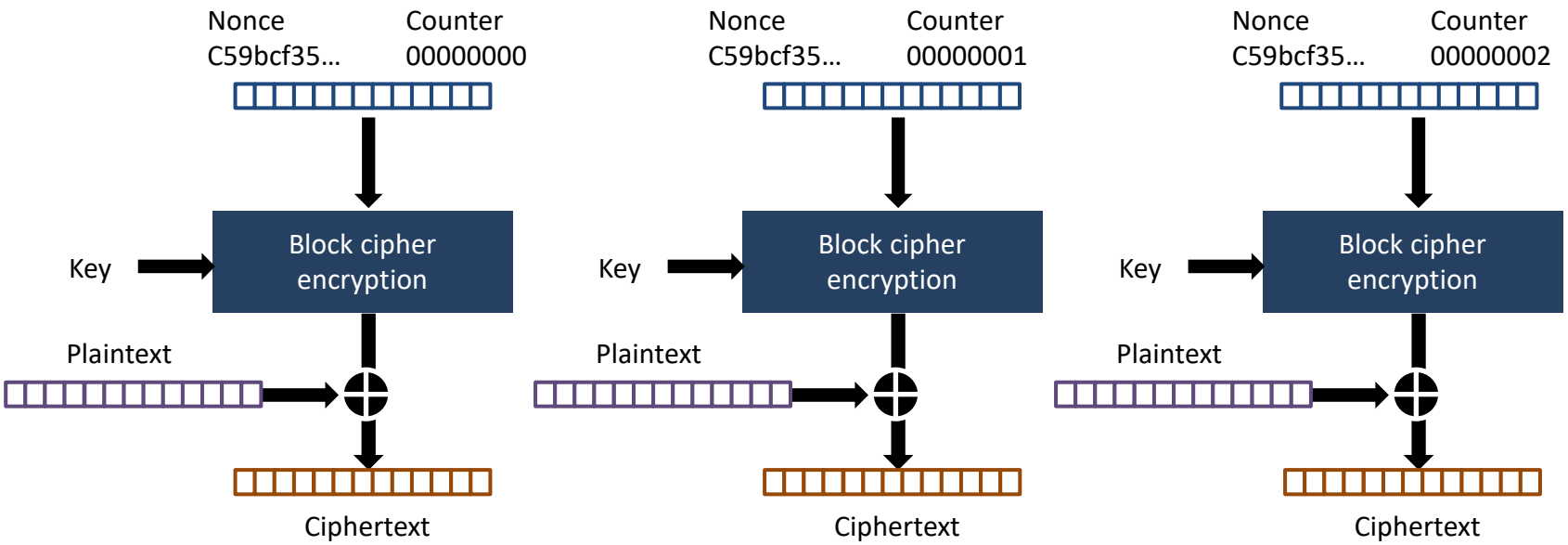
- CBC (Cipher Block Chaining)



CTM (Counter Mode)

- Splits messages into blocks the same size as the key
- Generate random or non-random nonce and concatenate, add or XOR with sequential counter
  - A nonce is additional pseudo-random input for cryptographic protocols and algorithms
  - Used only once with any given key
  - Random or Sequential (sequential provides protection against anti-replay attacks)
- Encrypts nonce/counter with key
- XOR result of encryption with plaintext to produce ciphertext
- Repeat for each plaintext block

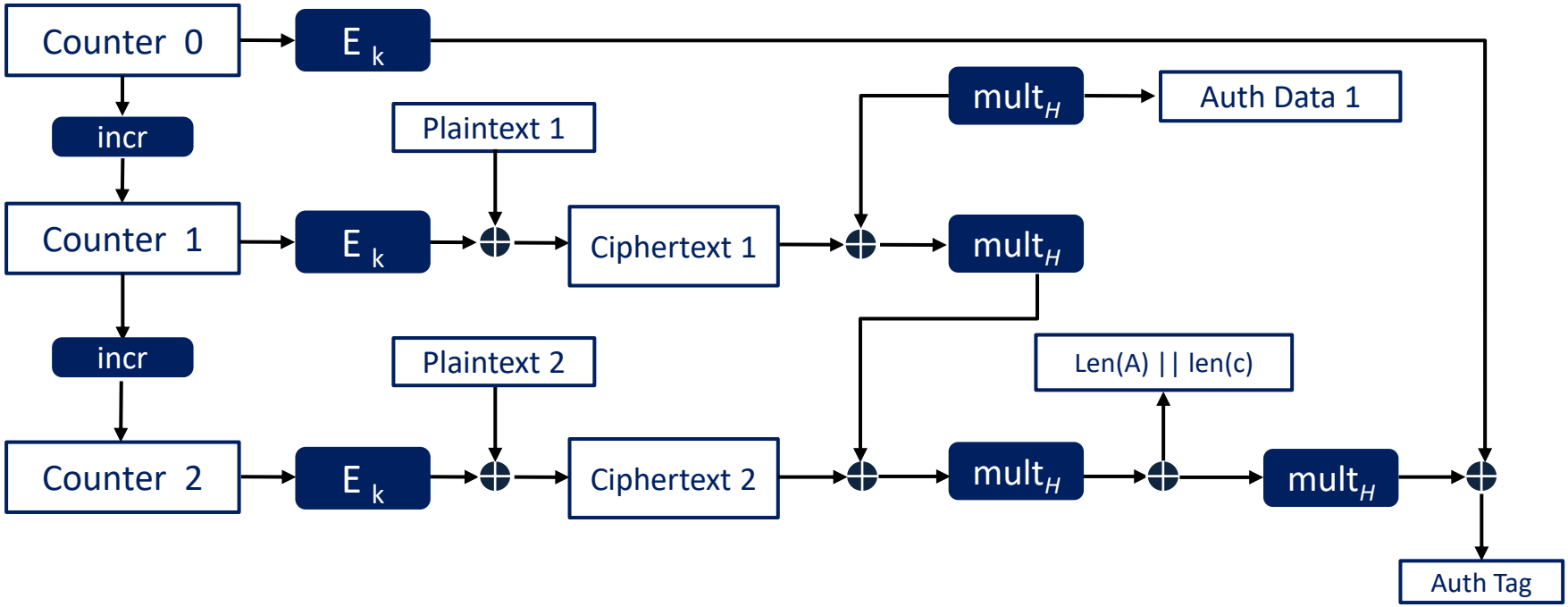
CTM (Counter Mode)



GCM (Galois/Counter Mode)

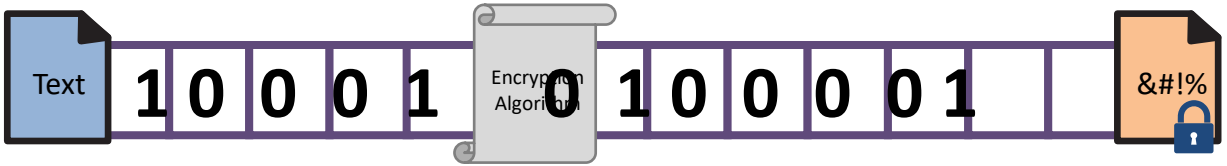
- Provides both authenticity and confidentiality (AEAD)
  - Do not need a separate HMAC like SHA-256
- Uses Counter Mode (CTM) to generate the ciphertext
- Uses Galois mode for authentication
- Uses authentication data to produce Authentication Tag to verify authenticity of data

GCM (Galois/Counter Mode)



Stream Ciphers

- Operates on a continuous stream of plaintext data
  - Encrypting 1 bit or byte at a time
- Plaintext bits are typically XORed with keystream bits
  - Keystream = random bits, bytes, numbers, characters
- Faster than block ciphers with lower complexity than block ciphers
- Modern ciphers can work in block or stream mode or both
- Examples:
  - FISH
  - CryptMT
  - Scream
  - RC4



Simple Stream Cipher in Action

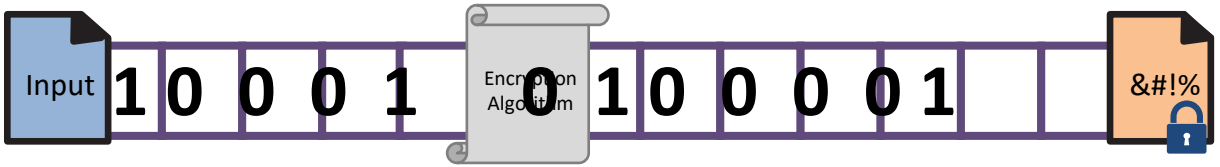
- Alice wants to use a stream cipher to encrypt the letter "A"
- In ASCII, the letter "A" has the value of 65 = 1000001
- The first cipher stream bits are 0101100
- We perform an XOR function (Modulo 2 addition):

  1000001 = A

  XOR

  0101100

  1101101 = m



- The letter "A" becomes ciphertext "m“ (ASCII value 109)

Symmetric (secret key) Algorithms

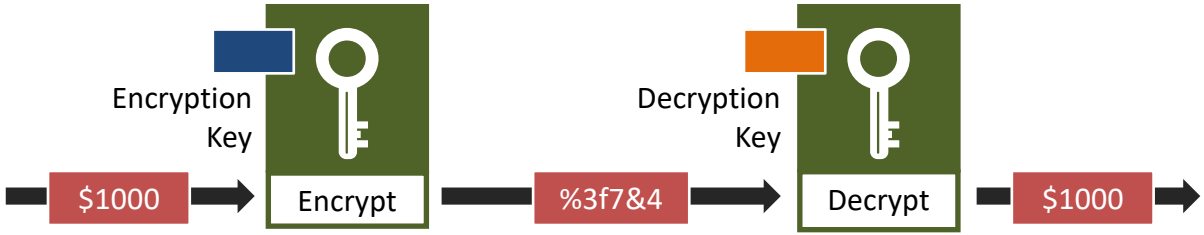
- Uses the same key to encrypt and decrypt
  - efficient, fast, handles high data rates of throughput
  - computationally cheap
  - shorter key lengths (40 to 256 bits)
  - complex key management
  - difficult to secure
  - no authentication
  - does not scale well
- DES, 3DES, RC4, Twofish/Blowfish, AES-CBC, AES-GCM

AES is Ubiquitous

- Complete replacement for DES
  - Uses the Rijndael algorithm
    - Joan Daemen and Vincent Rijmen
  - Block cipher with key sizes of:
    - 128 bits with 10 rounds
    - 192 bits with 12 rounds
    - 256 bits with 14 rounds
  - CBC and GCM modes are most common
    - IPsec
    - SSL/TLS
    - CSP data encryption (KMS)

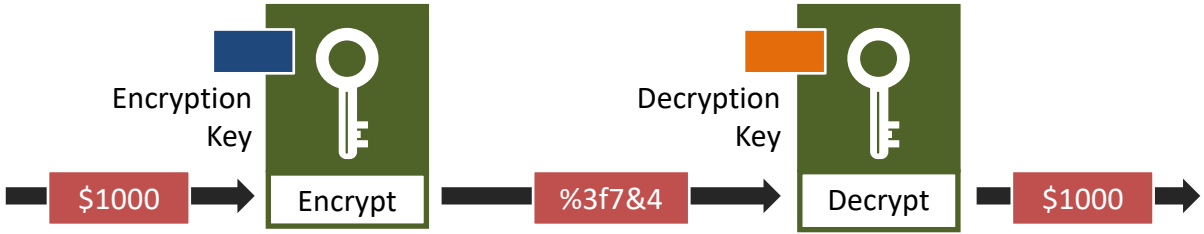
Asymmetric (public key) Algorithms

- Uses different keys to encrypt and decrypt
  - efficient key management
  - great for digital signatures and key exchange
  - scales extremely well
  - longer key lengths
  - Slower and more computationally expensive
  - does not handle high data rates of throughput well



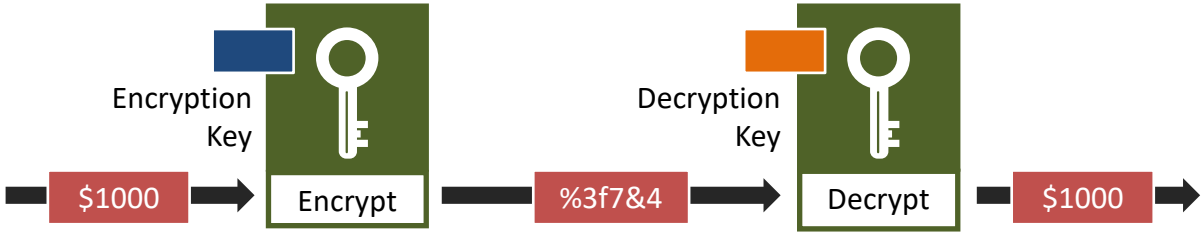
Asymmetric Algorithms

- Key pair is mathematically related based on factoring the product of large prime numbers
  - Public key is shared with many
  - Private key is kept secret for owner
- Keys are typically from 512 to 4096 bits in length
  - Longer is less susceptible to brute force attack
  - RSA
  - DSA
  - Diffie-Hellman
  - Elliptic curve (DSA)
  - PGP/GPG



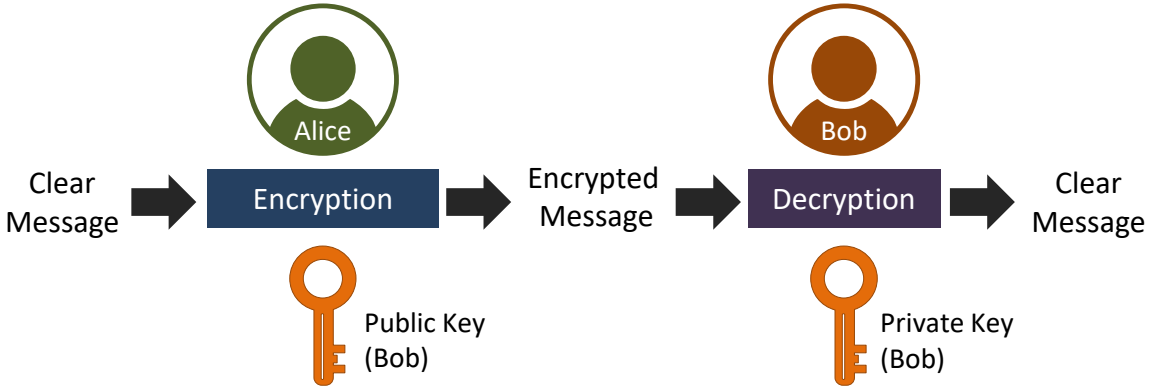
Asymmetric Algorithms

- Slow (not suitable for bulk data encryption)
- Key management is simpler and more secure
- Best suited for
  - Digital signatures
  - Key exchange or agreement
  - Protecting session keys

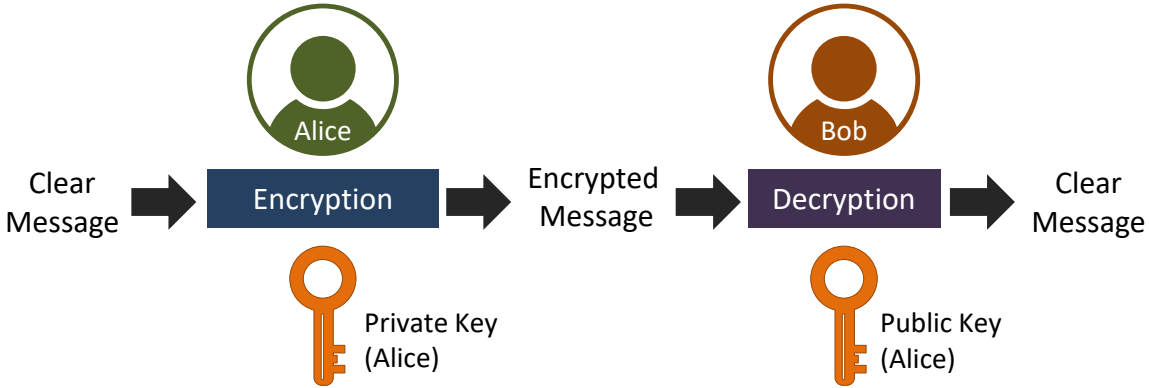


Asymmetric Algorithms

- Privacy
  - Encrypt with public key
  - Decrypt with private key

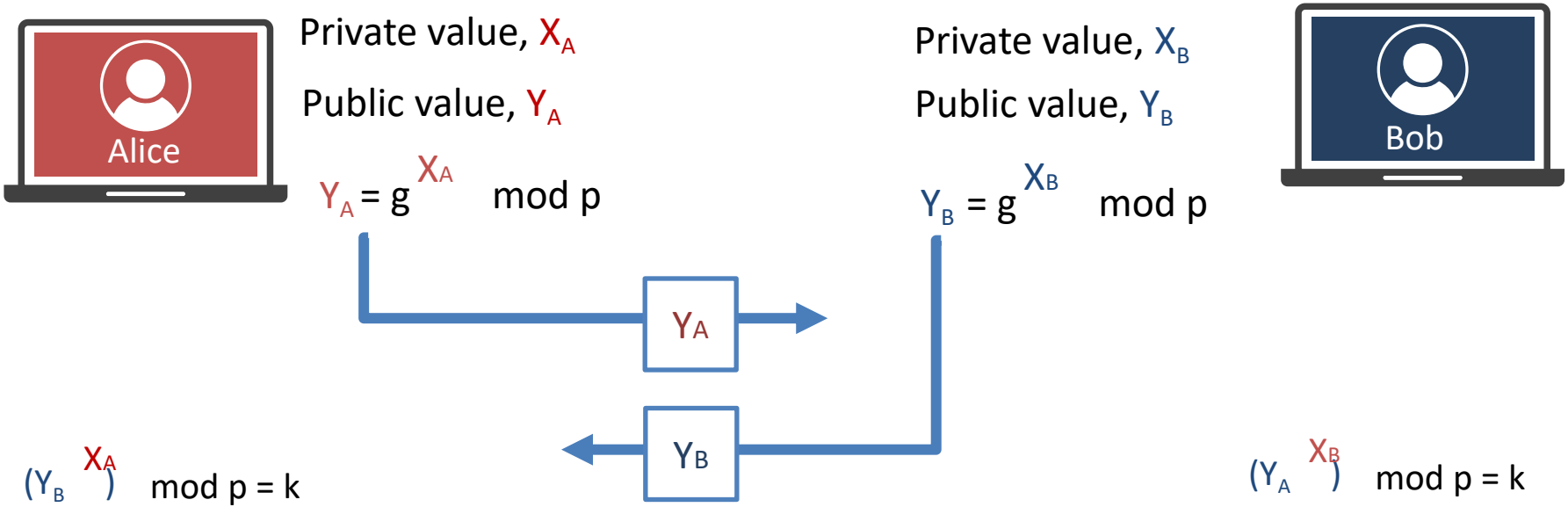


- Authentication
  - Encrypt with private key
  - Decrypt with public key



Asymmetric Algorithms

- Diffie-Hellman
  - The first key agreement asymmetric algorithm

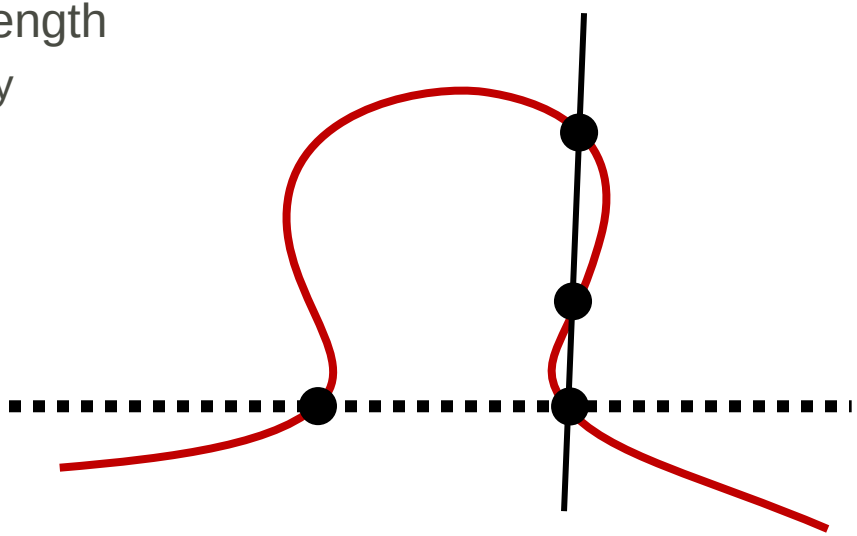


Diffie-Hellman Modes

- DH (Diffie-Hellman)
  - Same shared secret used all the time between party
- DHE/EDH (Ephemeral Diffie-Hellman)
  - Different shared secret used each time between party
- ECDH (Elliptic-Curve Diffie-Hellman)
  - Uses EC public/private key pair
  - Same shared secret used all the time between party
- ECDHE/ECEDH (Elliptical-Curve Ephemeral Diffie-Hellman)
  - Uses EC public/private key pair
  - Different shared secret used each time between party

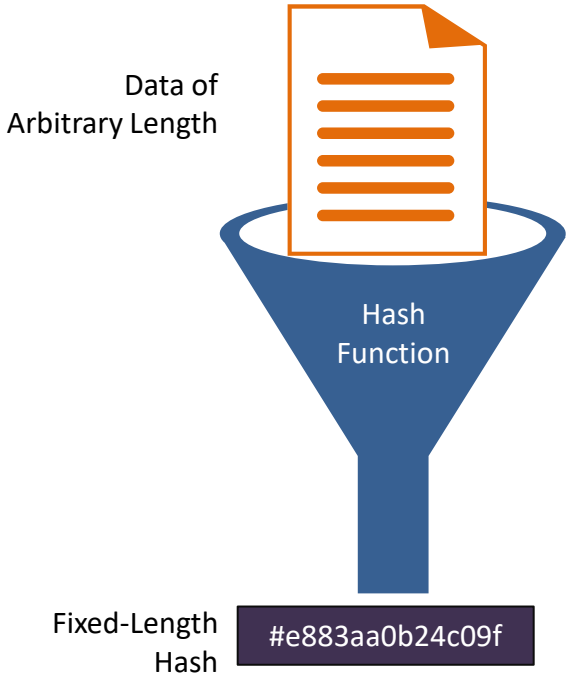
Elliptic Curve Asymmetric Algorithms

- Rich mathematical functions
  - Values of points on a curve used in formula for encryption and decryption
- Most efficient
  - Smaller keys providing exceptional strength
    - 3072 standard key = 256 elliptic curve key
  - Used in devices with limited resources
- Common uses
  - Digital signatures
  - Key distribution
  - Encryption
  - IPsec and TLS



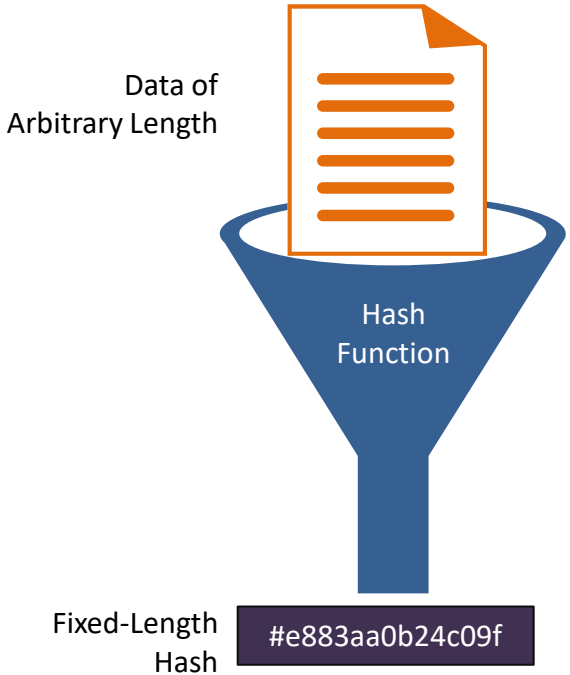
Hashing

- Maps data of any size to a fixed-length string
  - Called a hash value, message digest, fingerprint, checksum
- One-way mathematical function
  - Produces a digest 128 to 512 bits in length
- Avalanche effect and Birthday Paradox
- Used in authentication, data integrity, non-repudiation, fingerprinting, and password storage (Password + salt + hash function = hashed password



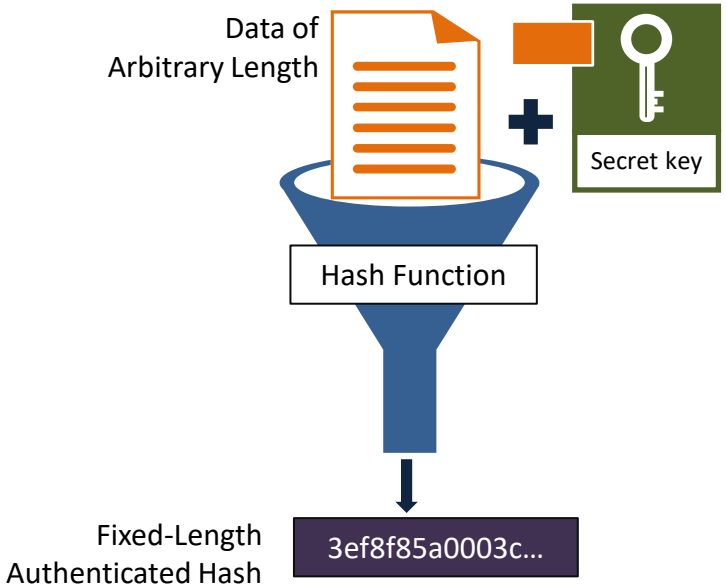
Hashing Functions

- MD5 (128-bit digest produced)
- SHA-1 (160-bit digest produced)
- SHA-2 and SHA-3
- RIPEMD (128, 160, 256, 320-bit versions)

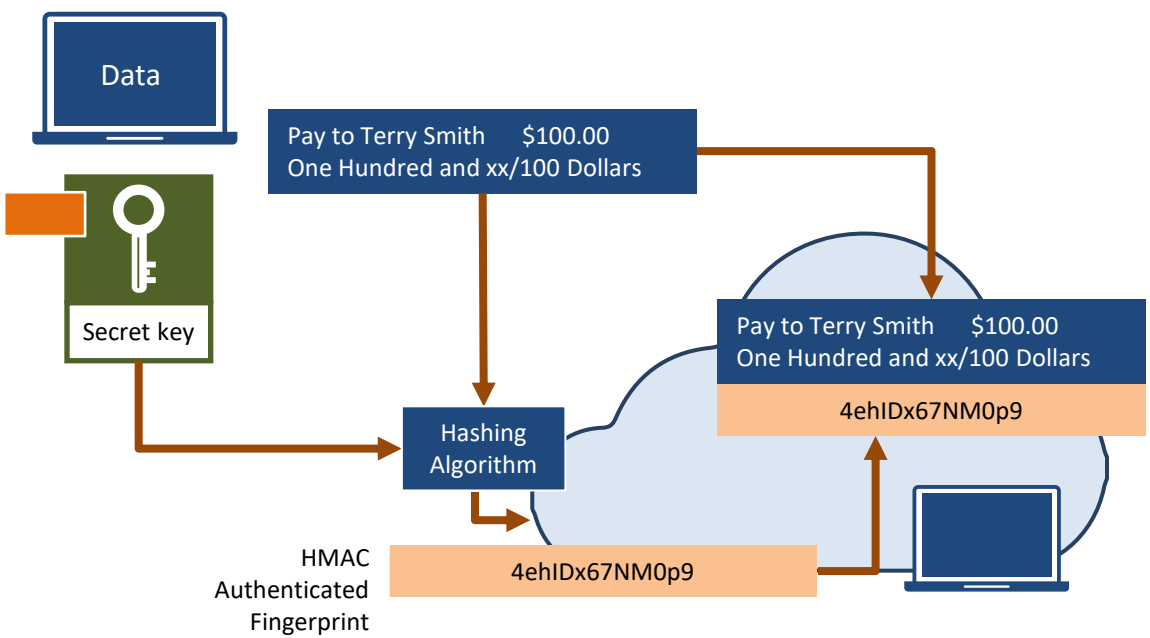


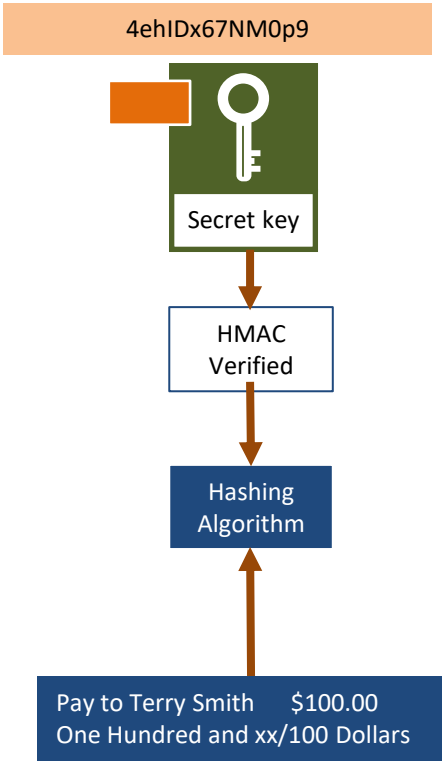
Origin Authentication with HMAC

- Verifies the sender of information
- Uses Hashed-Message-Authentication-Code (HMAC)
- Message + Hash + Shared Secret Key
  - Only as strong and safe as the key

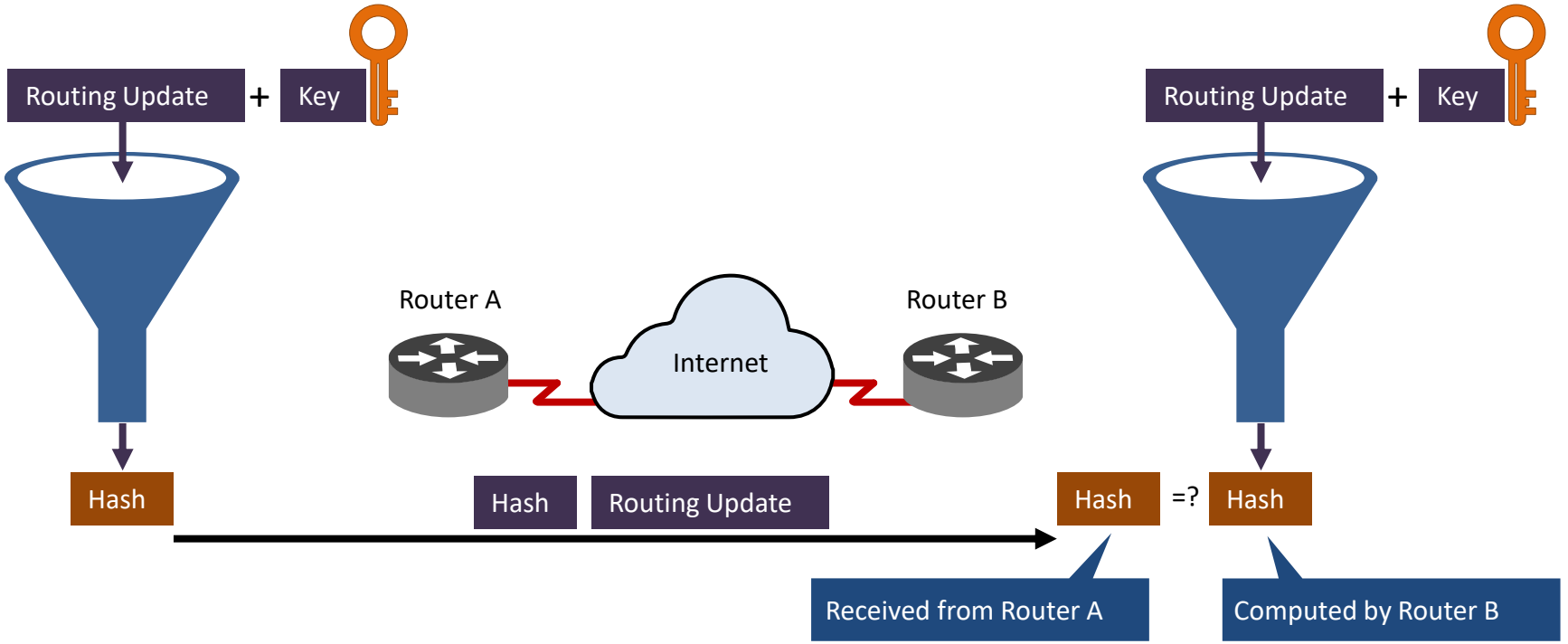


Origin Authentication and Integrity



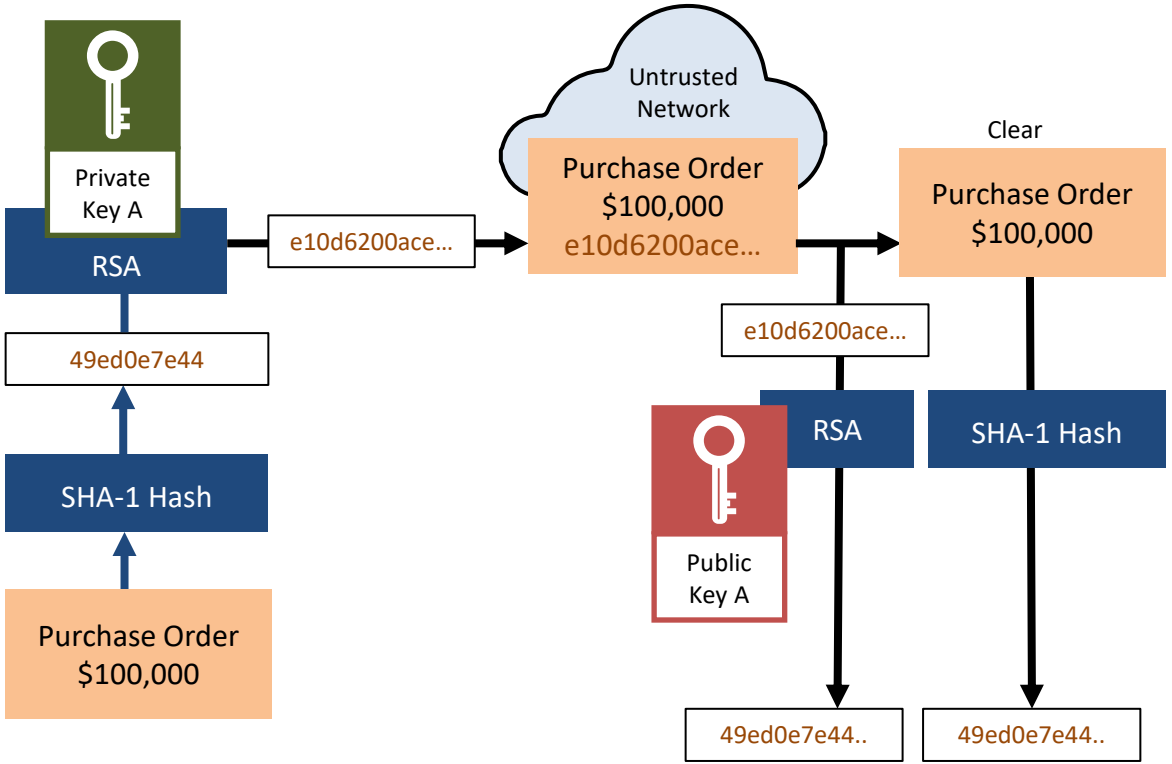


Origin Authentication and Integrity



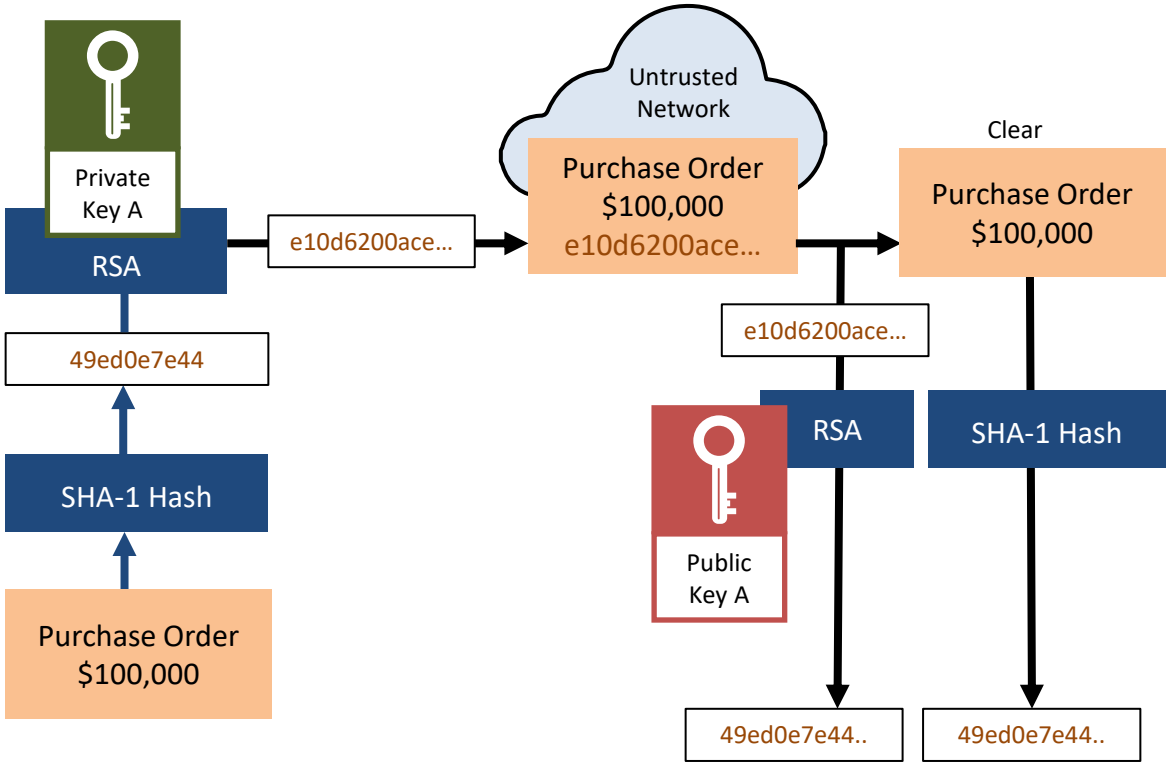
Digital Signatures

- Scalable mathematical way of providing
  - Authenticity
  - Integrity
  - Non-repudiation
- Equivalent of a handwritten signature



Digital Signatures

- Key
  - Random private/public pair
- Hash algorithm
  - MD5, SHA1, SHA2
- Signing algorithms
  - RSA (Rivest, Shamir, Adelman)
  - DSA (digital signature algorithm)
  - ECDSA



Perfect Forward Secrecy

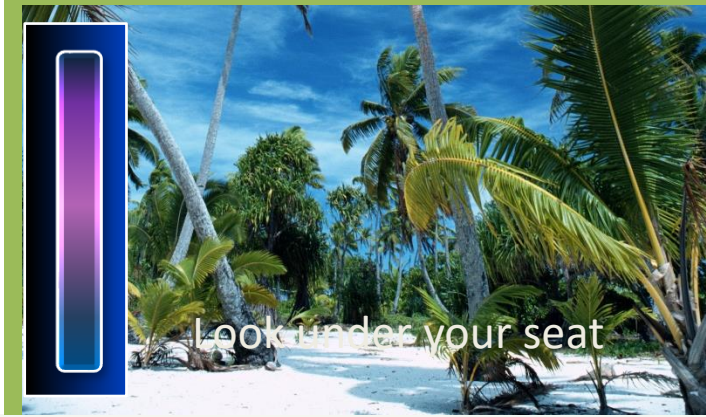
- Also simply "forward secrecy"
- Compromises long-term keys (PMKs or CMKs), not any past session keys
- Protects past sessions against future compromises of secret keys or passwords
- A public-key cryptosystem has the optional property of forward secrecy when it generates one random secret key per session to complete a key agreement without using a deterministic algorithm

Key Stretching

- PBKDF2 and BCRYPT
  - Pseudorandom functions (Password/Passphrase + salt) applied many times to produce longer and stronger cryptographic key for other uses
  - Example:
    - Passphrase = thisismypassword
    - Salt = ACB3F274509886057D924912E201EED0 (at least 64-bit)
    - Iterations = 1000
    - Key length = 128
    - Result = xvgFAWdnw035eJxsldD9xrLIhuxpGM1SIiqSZStt4ClTqHk3dluVB5r44yc1ICrfrqsGkvCVmdVF7kuk/e16FCnZsajE6ErwSB3mkx6tZOX0LELU9wutBHxGJKiXGyrTQp99lAY8ghhIt4ciu71OJvjKTbT8nSskJyZ3pzZI5UM=

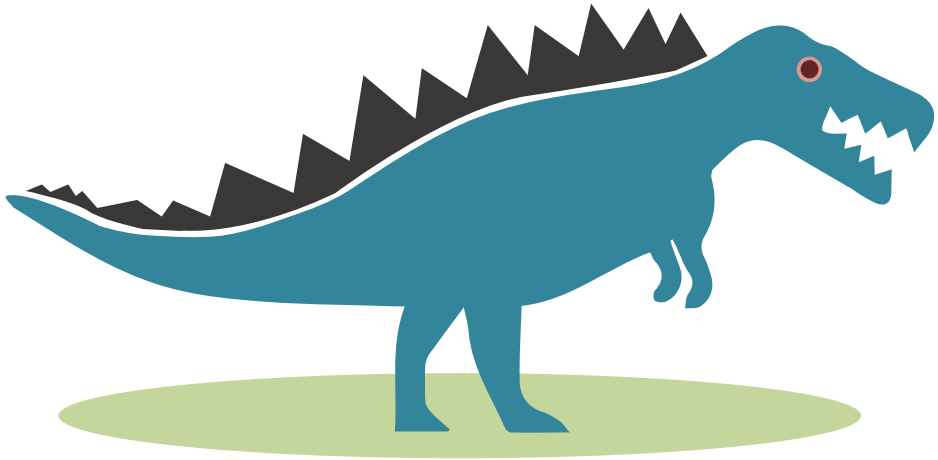
Steganography

- Steganography is the process of embedding files or text messages within images and graphics so that no third-party can detect the hidden data
- To encrypt images, specialized software applications are used to implant and extract the message or file
  - A sentence in a picture
  - An image in text
  - A file in a video
  - A cryptographic key in any of the above



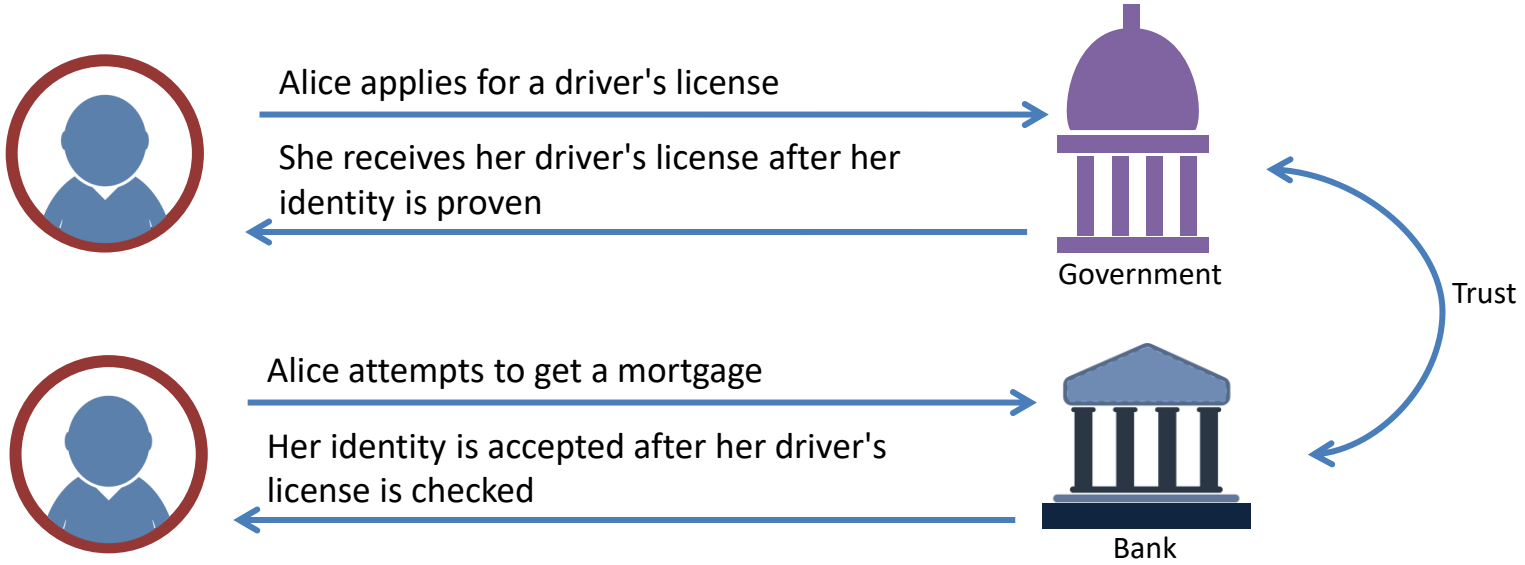
Steganography Tools

- An advantage of this security technique is that encrypted images usually need the original app to display the message so unauthorized users are prevented from decrypting the images without the right utility
  - OpenStego
  - CenoCipher
  - QuickStego
  - Xiao Steganography



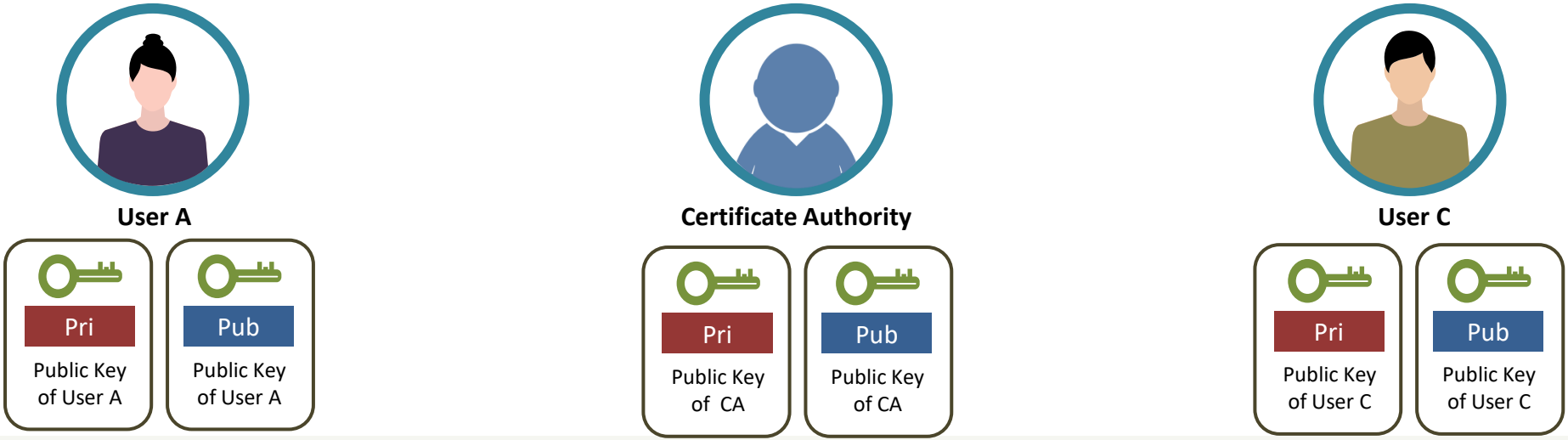
PKI Overview

- How do you distribute, verify and revoke public keys?
- Public Key Infrastructure trusted third-party system



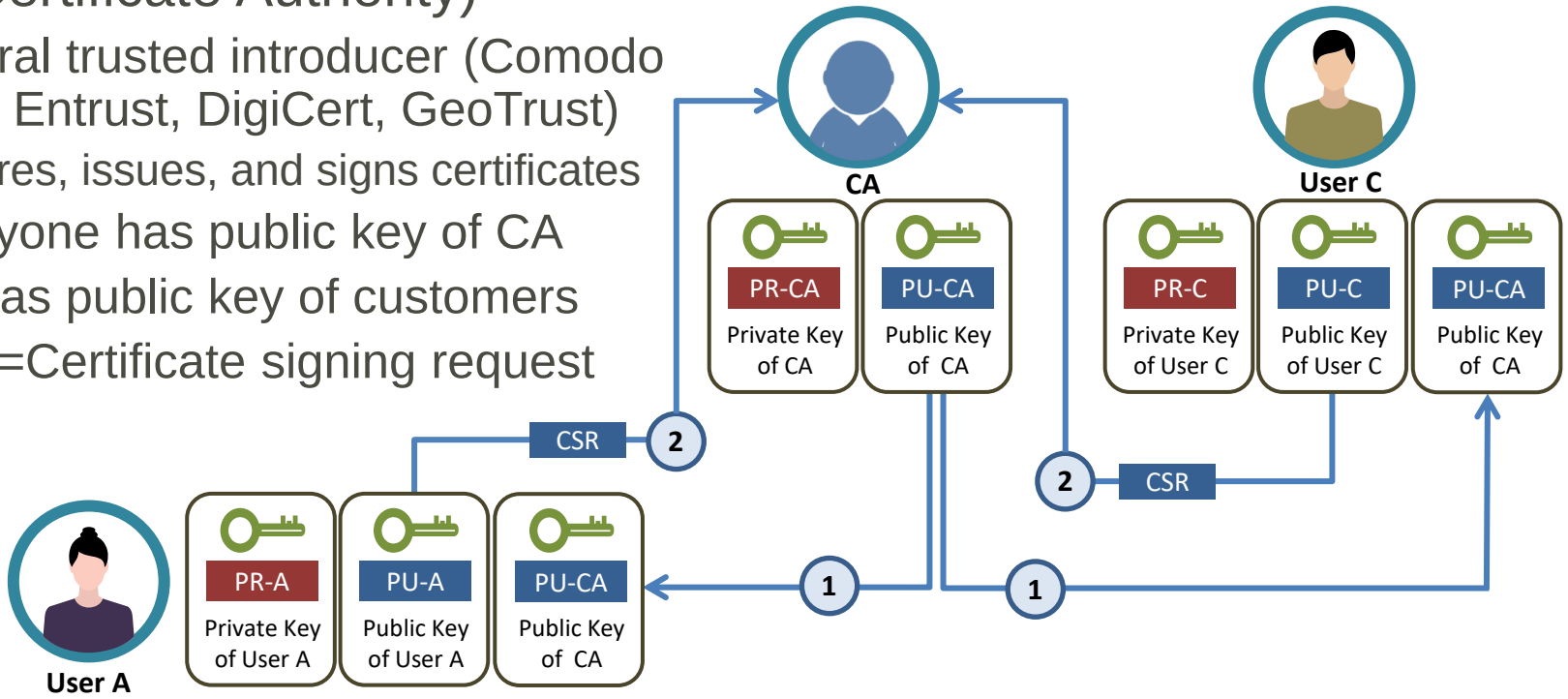
Public Key Infrastructure

- Scalable binding of a public key with an entity identity
  - A person, system or organization
  - Registering and issuing certificates by a Certificate Authority (CA)
    - Automated or manual



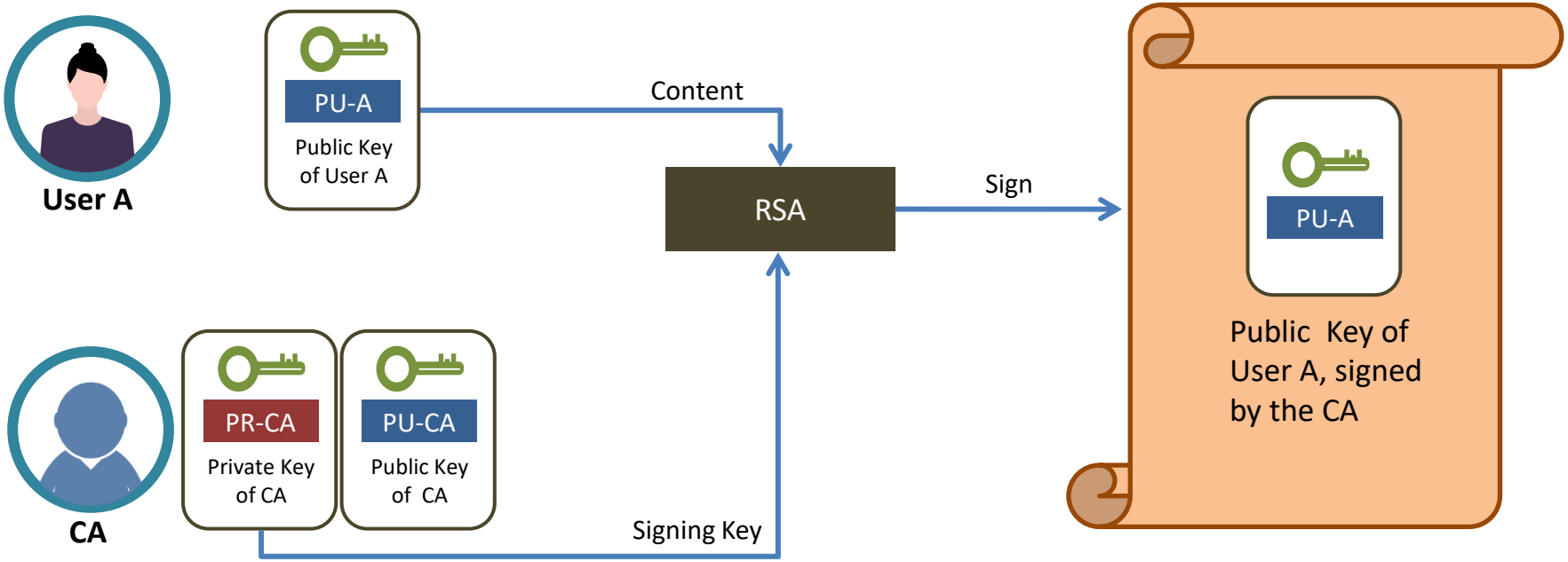
Public Key Infrastructure

- CA (Certificate Authority)
  - Central trusted introducer (Comodo SSL, Entrust, DigiCert, GeoTrust)
    - Stores, issues, and signs certificates
  - Everyone has public key of CA
  - CA has public key of customers
  - CSR=Certificate signing request



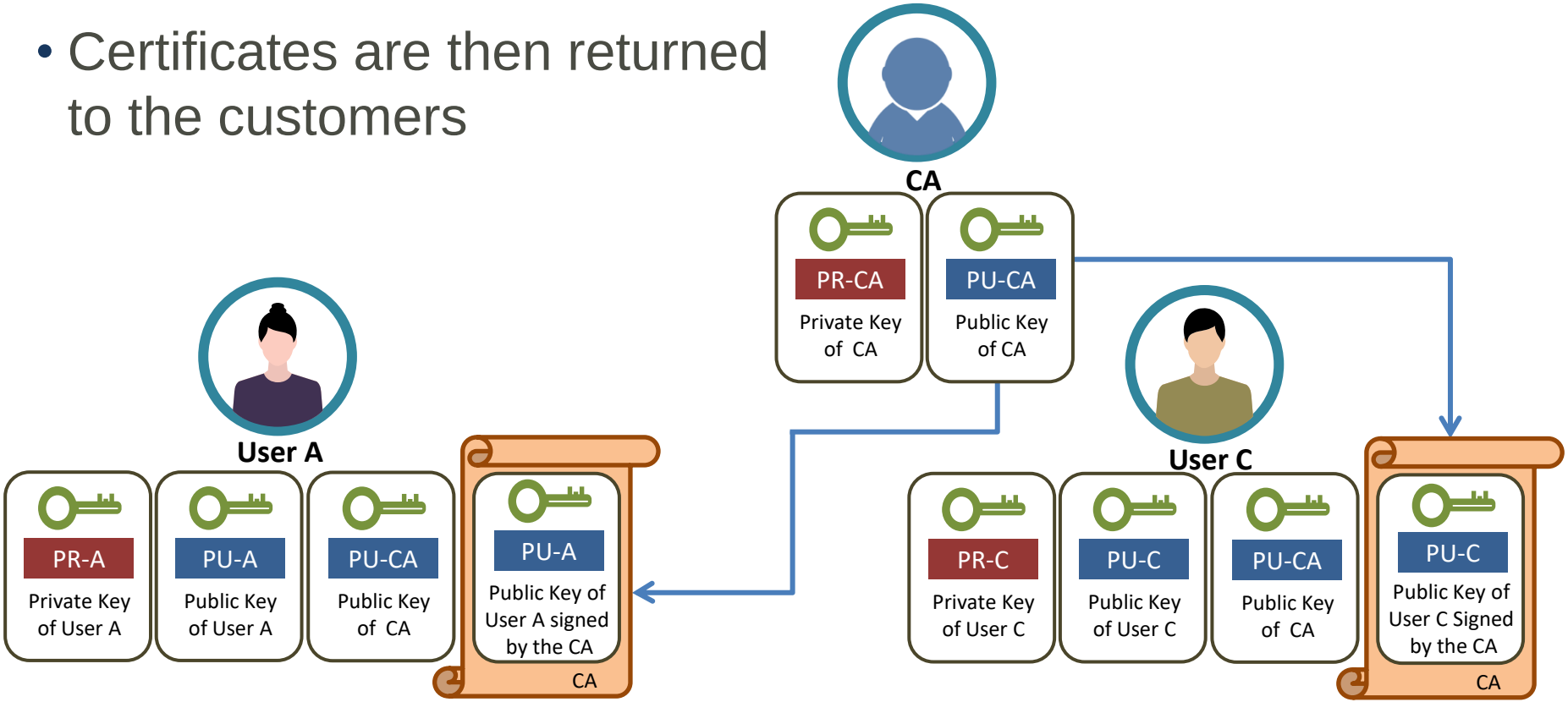
Public Key Infrastructure

- CA signs public key of customers using its private key
  - Digital Certificate



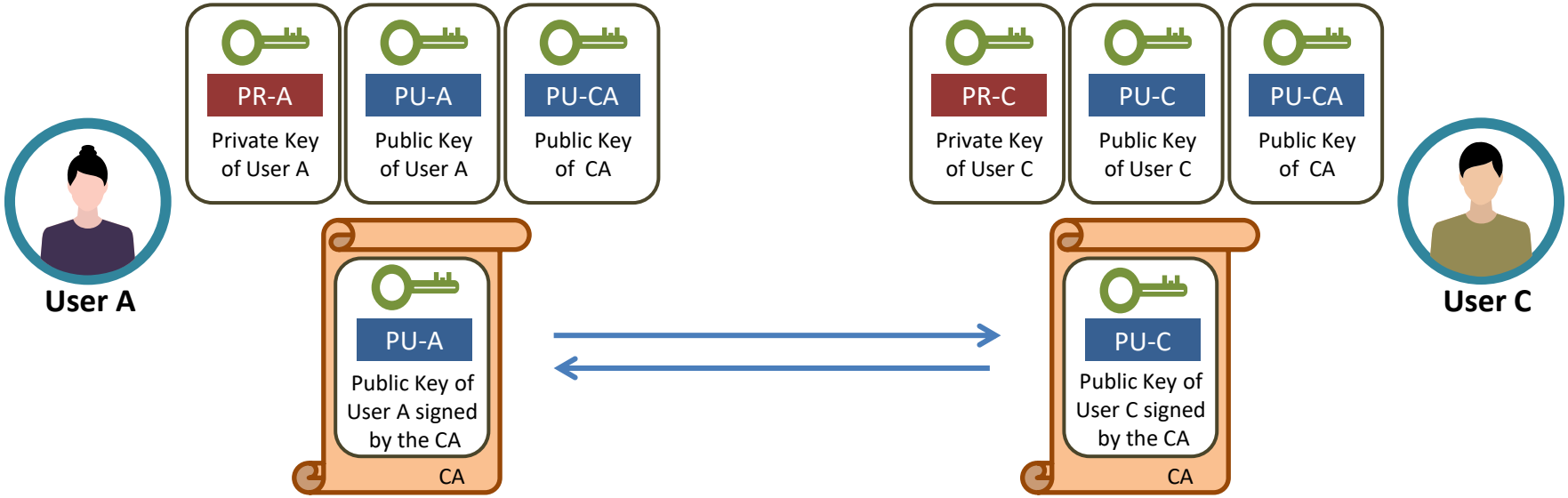
Public Key Infrastructure

- Certificates are then returned to the customers



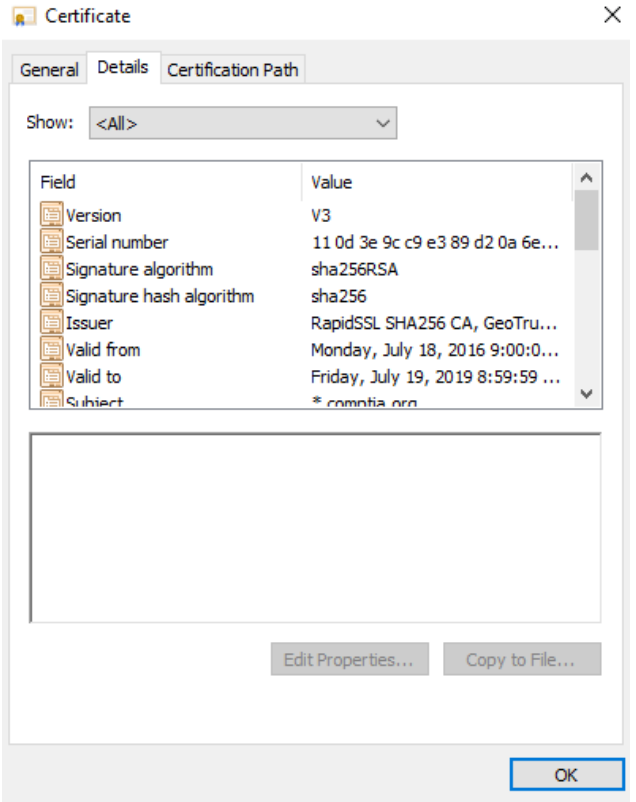
Public Key Infrastructure

- Certificates can now be exchanged over untrusted network
- Certificates/public keys of entities are now verified with public key of CA



X.509 Certificates

- Certificate format:
  - Version number
  - Serial number
  - Signature algorithm ID
  - Issuer name
  - Validity period
    - Not before
    - Not after
  - Subject name
  - Subject public key info
    - Public key algorithm
    - Subject public key
  - Issuer unique identifier
  - Subject unique identifier
  - Extensions
  - Certificate signature algorithm
  - Certificate signature

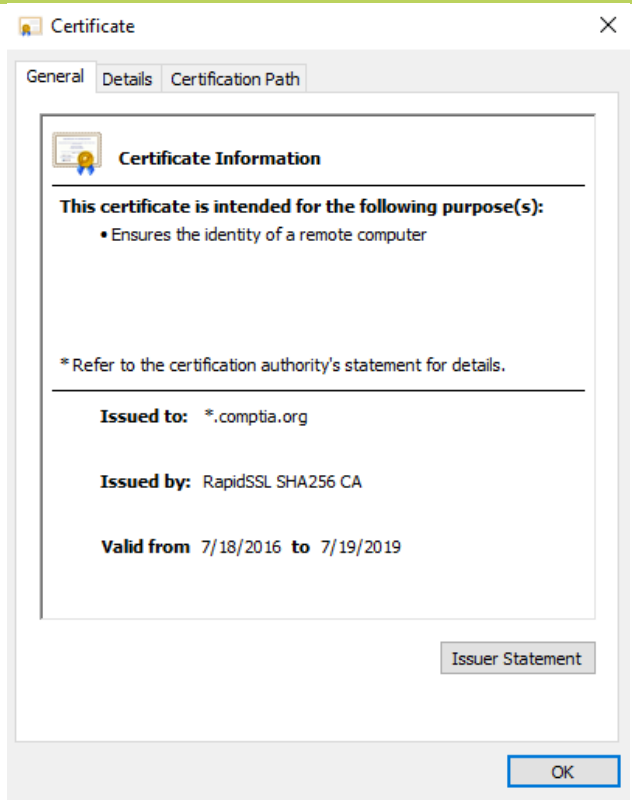


X.509 Certificates

- Extensions
  - .DER
    - Form of binary encoding using definitive length form
  - .CER
    - Form of binary encoding using indefinite length form
  - .PEM (Privacy-enhanced Electronic Mail)
    - Base64 encoded DER certificate (most common)
  - .PFX
    - Predecessor of PKCS#12
  - .P12 (PKCS#12)
    - Standard used for exchanging public and private objects such as keys
  - .P7B (PKCS#7)
    - Standard used for signing and encrypting data

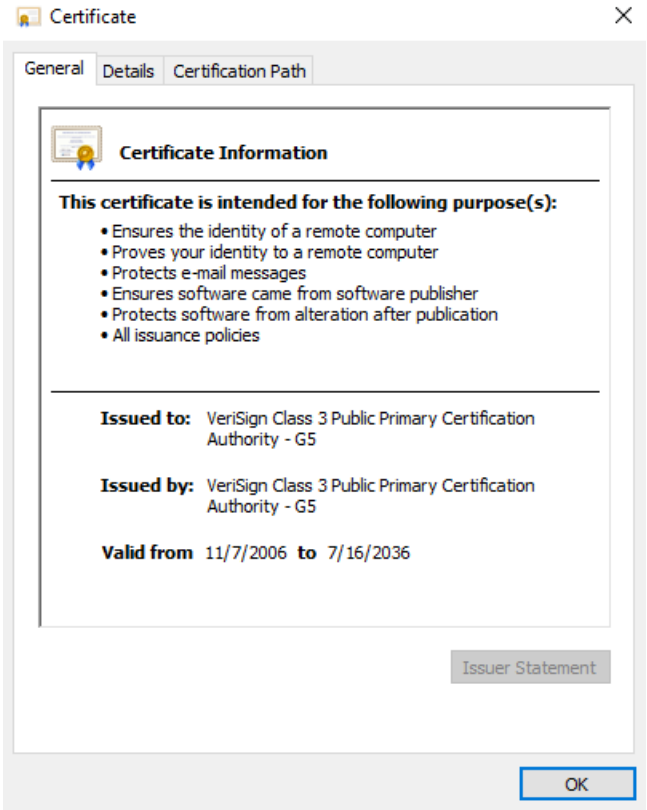
Types of Certificates

- Wildcard
  - Used with multiple subdomains
    - *.mycompany.com
- Subject Alternate Name (SAN)
  - Used to associate additional names
    - Email address, IP addresses, DNS names
- Code signing
  - Used to authenticate and the source and integrity of code
    - Drivers, applications, macros, configuration files



Types of Certificates

- Self-signed
  - Signed by the entity it certifies
    - Root CAs
- Root
  - Unsigned or self-signed that identifies the root CA
    - Trust anchor for digital certificates in the chain of trust
- Email (S/MIME)
  - Sign and encrypt email messages



Types of Certificates

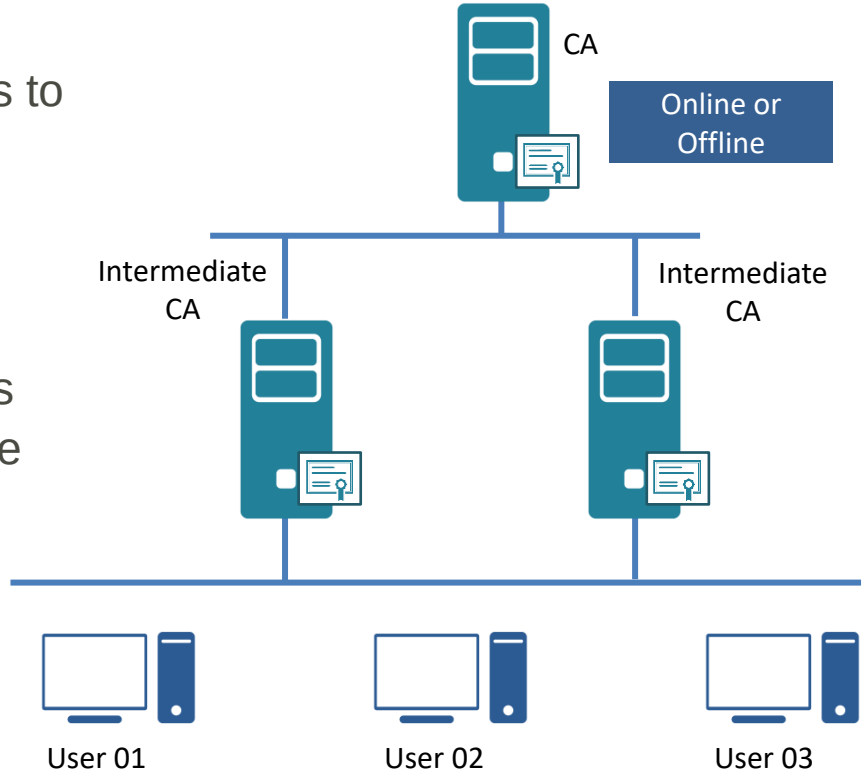
- Machine/computer
  - Used by the local machine or device
    - Authenticate to the network
- User
  - Used by an individual user entity
    - EFS, email, client authentications
- Domain Validation (DV)
  - Provides proof over the control of a domain

Certificate Validation

- Domain Validation (DV)
  - Provides proof over the control of a domain
  - Email or Domain registry check
- Extended Validation (EV) Certificate
  - Extended Validation SSL/TLS Certificates provide more confidence that you are the legal entity who owns and controls your web site
  - You must pay for this designation and it is becoming less valuable with newer browsers and mobile apps

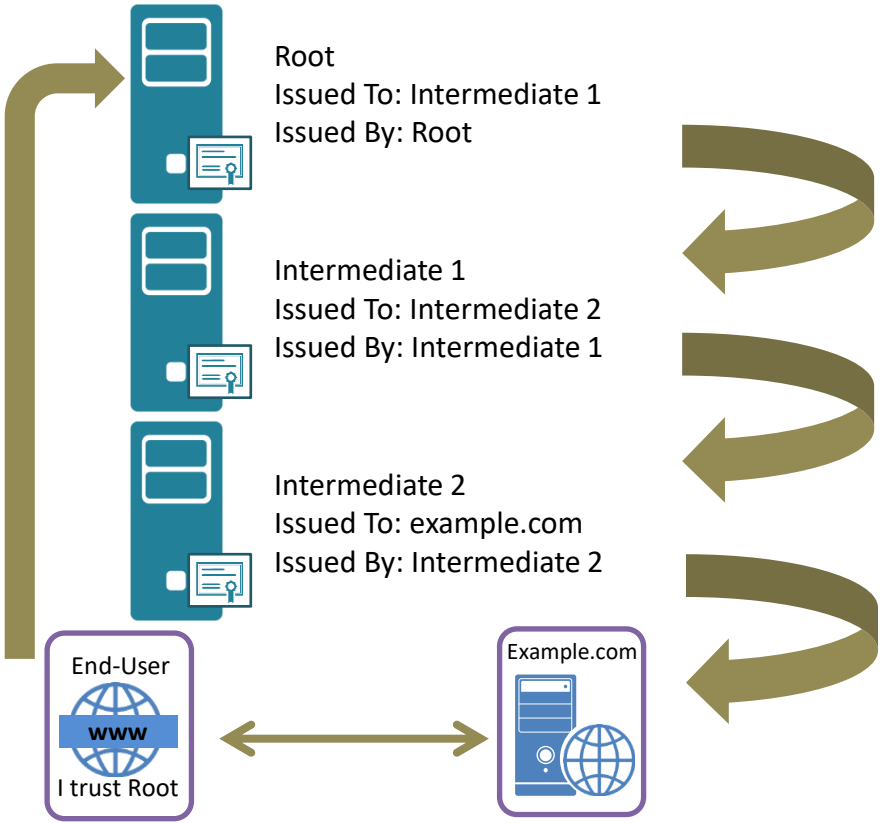
CA Trust Models

- Single CA
  - Responsible for directly providing certificates to everyone (enterprise PKI)
  - Must be online at all times
- Hierarchical
  - Root CA + intermediate CAs
  - Root provides certificate to intermediate CAs
  - Intermediate CAs provide certificates and the “chain” to users or other intermediate CAs
  - Root can be online or offline
    - Online – connected to network
      - Issues certificates over the network
    - Offline – not connected to network
      - Issues certificates on removable media



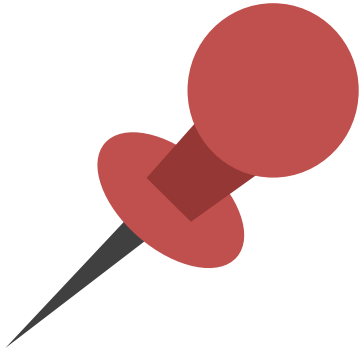
Certificate Chaining

- How do I trust certificate?
  - CA must be in trusted store
    - Not possible to include all CAs
- A chain of trust
  - "Issued To" field
  - "Issued By" field
- Website certificates are known as ”leaf certificates”
  1. Leaf certificate
  2. Intermediate certificate
  3. Root certificate



Pinning

- Manual "allow list" of digital certificates
  - Supplements or replaces chain of trust
  - Improves certificate security
    - Only pinned certificates are trusted
      - – Google pinned own web sites in Chrome
  - Pin during application development (static) or after it is automatically learned for the first time (dynamic)
  - Why pin?
    - When you need to be 100% sure of remote host's identity
    - When you are in a hostile environment

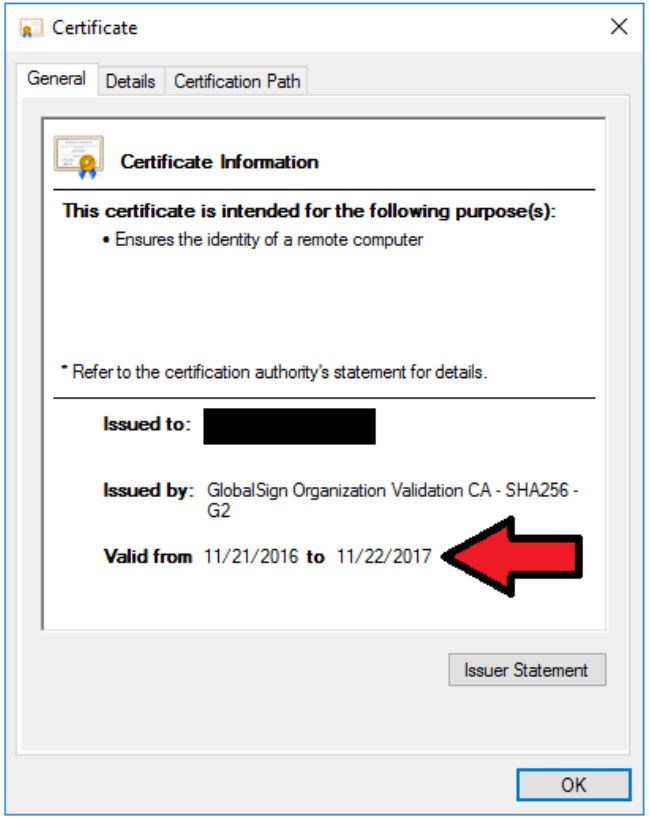


Pinning

- Certificate
  - Easiest but not flexible
    - Pin entire certificate to application
      - Certificates usually have a max life of 1 year
        - » Application has to be updated each year
      - If site rotates certificates
        - » Application has to be updated more frequently
- Public key
  - Hardest but more flexible
    - Pin only the public key from the certificate to application
      - Key must be extracted from certificate
      - If certificate is updated key does not change so pinning remains the same

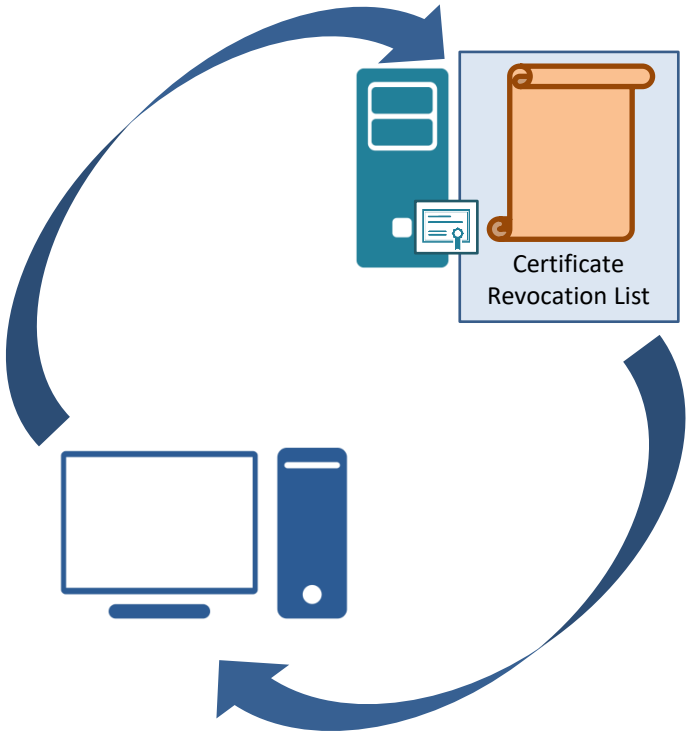
Expiration, Revocation, Suspension

- For security reasons all keys must have a finite life due to brute force attacks
- Certificates are stamped with non-deterministic serial numbers and validity dates
- Certificate can be:
  - Revoked (permanent) – never used again
  - Suspended/held (temporary) - can be reactivated
- Extension fields are critical for added functionality and security



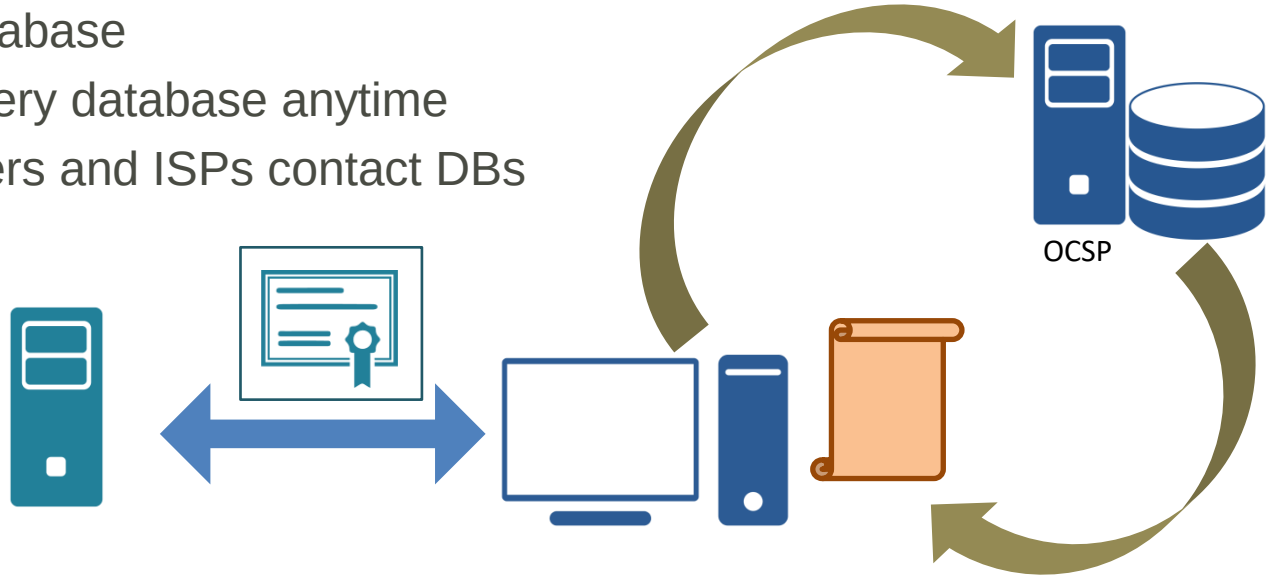
CRL (Certificate Revocation List)

- A list of certificates that are not valid
  - Serial numbers
- Issued by CA who issued certificate
- Generated and published periodically
  - Defined intervals or immediately
    - Not real-time
  - Downloaded by client regularly
    - Not real-time



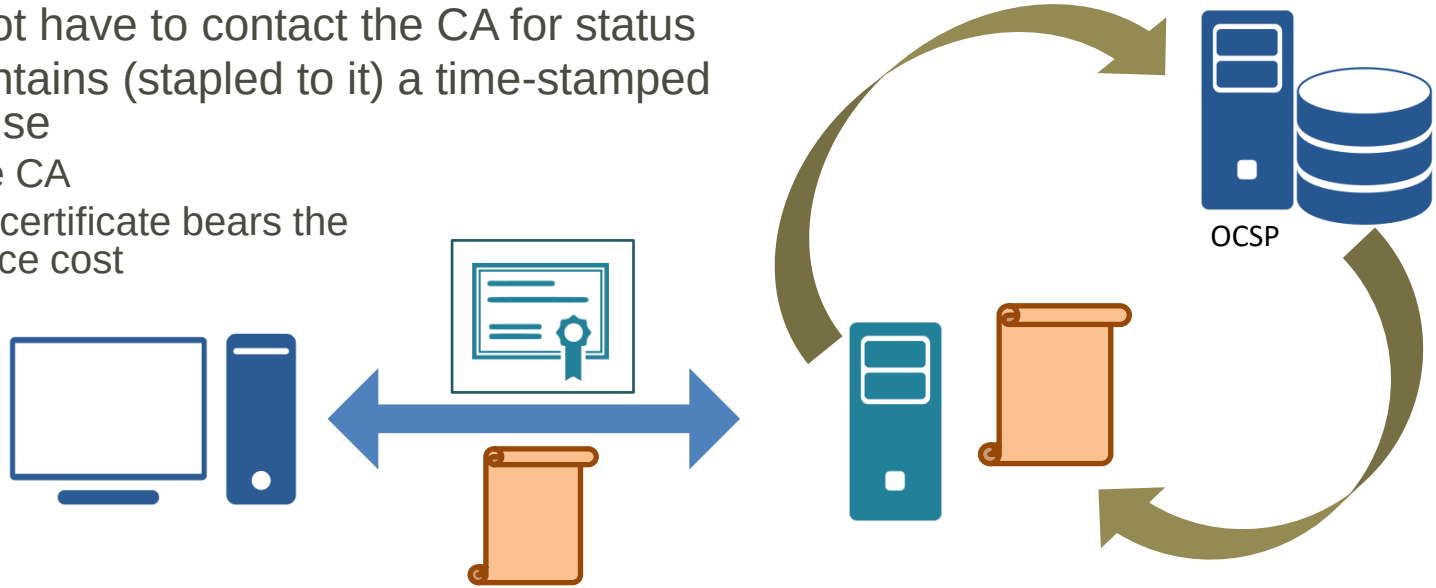
OCSP (Online Certificate Status Protocol)

- A list of certificates that are not valid
  - Serial numbers
- Generated and published immediately
  - Online database
  - Clients query database anytime
  - Web servers and ISPs contact DBs



Certificate Stapling

- Certificate stapling
  - OCSP stapling/TLS certificate status request
  - Alternate approach of checking the revocation status of certificate
    - Client does not have to contact the CA for status
    - Certificate contains (stapled to it) a time-stamped OCSP response
      - Signed by the CA
      - Owner of the certificate bears the OCSP resource cost



Improving PKI

- Use trusted third-party CA services
- Use fully-tested enterprise CA
- Validate certificate chains
- Consider secure OCSP for revocation
- Eliminate risky manual key management processes
- Tightly enforce key management policies
- Use third-party (cloud-based MSSP) services to help ensure integrity, performance, and manageability of your PKI

Weak Cipher Suites and Implementations

- Digitally sign as much as possible
- Do not use self-signed certificates
- Avoid sites with certificate errors or warnings
- Stop using RC4, MD5, SHA-1 suites
- Use AES-256 and SHA-256 if available
- Use Suite B Cryptography (IKEv2) with VPN implementations
- Have solid key management practices
- Use strong pseudo-random passwords
- Implement HSTS on web servers
- Use secure DNS (cloud-based) like Cisco Umbrella or AWS Route 53