Welcome to the Security+ Bootcamp

Your instructor:

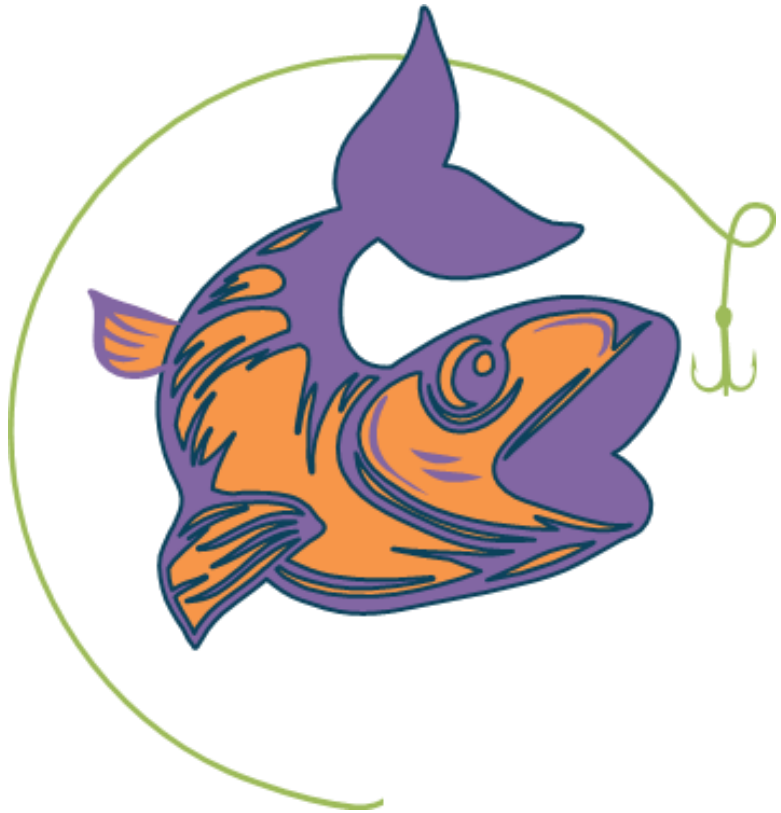
Michael J Shannon

CISSP #42221 / #524169,
CCSP
CCNP-Security, PCNSE7,
Security+, GIAC GSEC,
ITIL 4 Managing Professional

Class will begin at 10:00 A.M. Central Standard Time (CST)

Phishing Attacks and its Variants

- Phishing is a cyber attack that uses disguised e-mail as a vector
- The goal is to trick the recipient into believing that the message is legitimate so, they will click a link or download an attachment
- E-mail phishing attacks or hoaxes are one of the most common exploit vectors available to crackers



Phishing Attacks and its Variants

Common Phishing Indicators

- Vague salutations
- Suspicious domains
- URL Paths
- Wrong hypertext
- Awkward grammar
- Urgency in text
- Lack of contact info
- Spoofed headers/logos

Business E-mail Compromise (BEC)

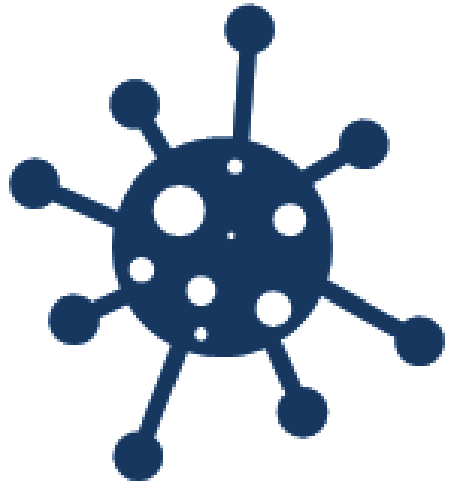
- Business E-mail Compromise (BEC) is a form of attack that targets companies who outsource, conduct wire transfers, and have suppliers abroad
- Corporate e-mail accounts of high-level employees are either spoofed or compromised through keyloggers or phishing attacks, often to perform fraudulent transfers

Common BEC Schemes

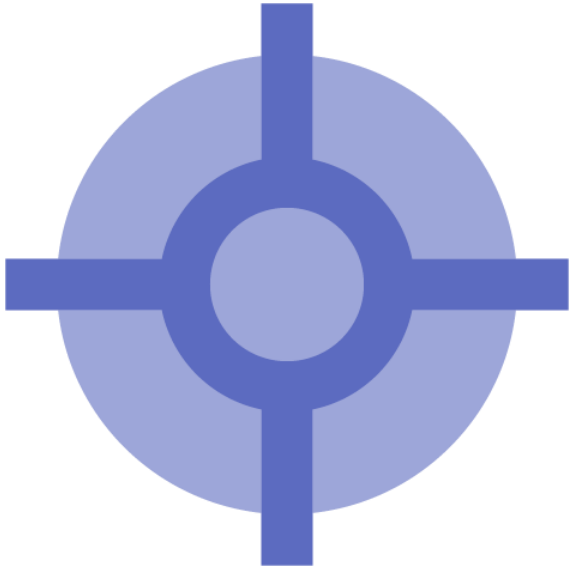
- Phony invoices and transfers
- C-Suite (C-Team) fraud
- E-mail or webmail account compromise
- Attorney impersonation and hoaxing
- Data theft of personally identifiable information (PII)

Pharming

- A blending of the words "phishing" and "farming" that describes a type of cybercrime like phishing
- A web site's traffic is manipulated or spoofed, and confidential information is stolen
- Attackers may install a virus or trojan on a target that changes the computer's hosts file to direct traffic away from its intended target and toward a fake web site
- Crackers may also poison a DNS server to re-direct multiple users to unintentionally go to the fake site, which in turn can be used to install malware on the victim's computer



SPAM



- Spam is a slang term for unsolicited commercial e-mail or junk e-mail
- E-mail spam is the most common and has traditionally consisted of:
- Advertisements
- Chain letters
- Spoofed e-mail related to phishing campaigns
- Hoaxes and money scams
- Malware warnings
- Unwanted pornography-related e-mail

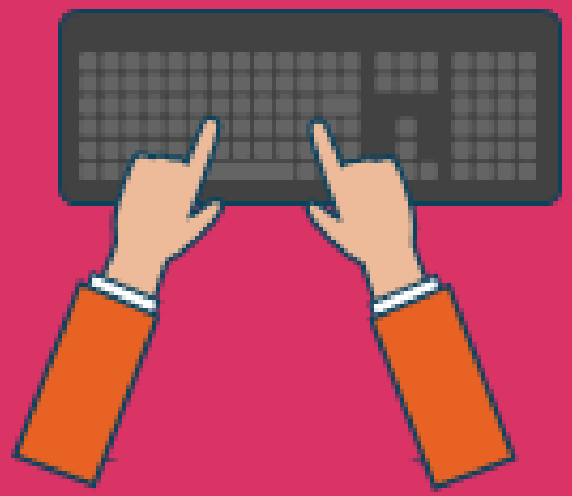
Common Categories of Spam

- E-mail spam
- Comment spam
- Trackback spam
- Negative SEO Attacks
- Spiders, Bots and DDoS Attacks

SPIM

- Spim stands for "Spam over instant messaging" and refers to unsolicited instant messages
- Spim disrupts chatting and can contain viruses or spyware
- By blocking any messages from sources not on your contact list, you can prevent spim
- Most anti-virus programs include spam and spim protection features

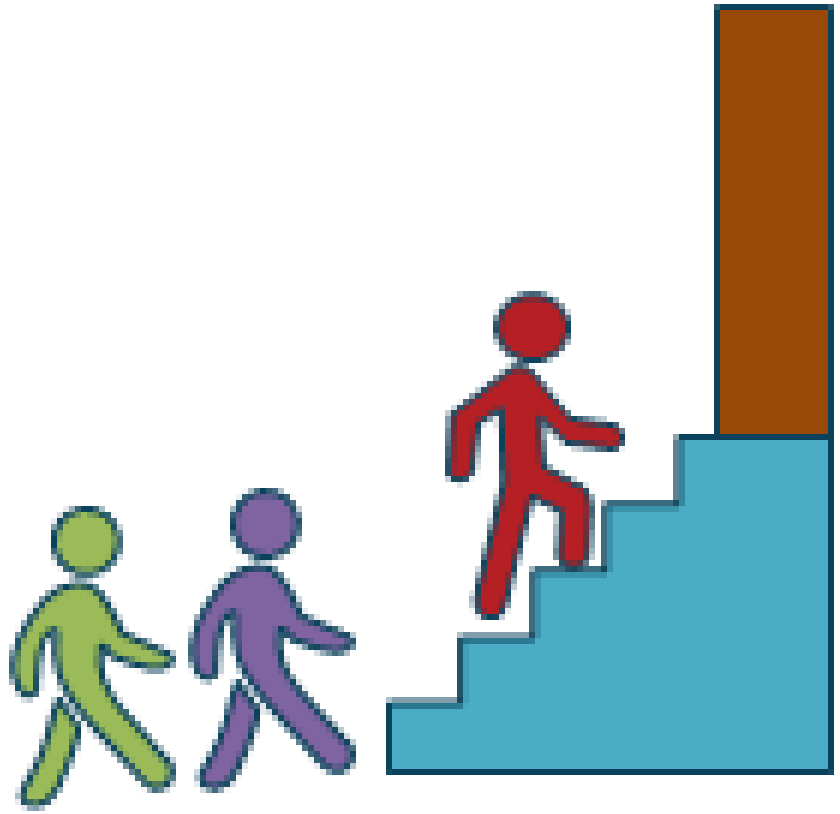
Typosquatting



- Typosquatting involves sitting on sites under someone else's brand or copyright and targeting Internet users who erroneously type a web site address into their browser address bar
- Other names for typosquatting are URL hijacking, sting sites, or fake URL
- Examples: facebool, gooogle, amason

Tailgating and Piggybacking

- 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 data centers
- Each subject fails to use their badge with the sensor every time they access a building or protected area
- Is often considered a violation of security policy (AUP)



Dumpster Diving

- Dumpster diving is an attack where the goal is to reclaim important information by searching through trash containers and dumpsters
- Attackers often look for:
  - Credit card information
  - Invoices and receipts
  - IP addressing
  - Organization charts
  - Names of key employees
  - Manuals and charts
  - Memos and sticky notes

Shoulder Surfing

Much easier to accomplish with mobile devices and Internet of Things

- 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

- Watering hole attacks leverage a compromised web server in order to target groups or associations in social networks
- 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
- Often targets the “weakest link” member of local working group, club, or conference attendee

Scams, fraud, and hoaxes

Attackers will go to great lengths to conduct their advanced persistent threat against your organization including long-term hoaxes and scams

Impersonation is first attempted remotely through IP spoofing

The next vectors use phones, e-mail, SMS, and IM

The next level involves masquerading as a legitimate entity

The goal is typically theft of financials, IP, PII, or PHI

Scams and Fraud

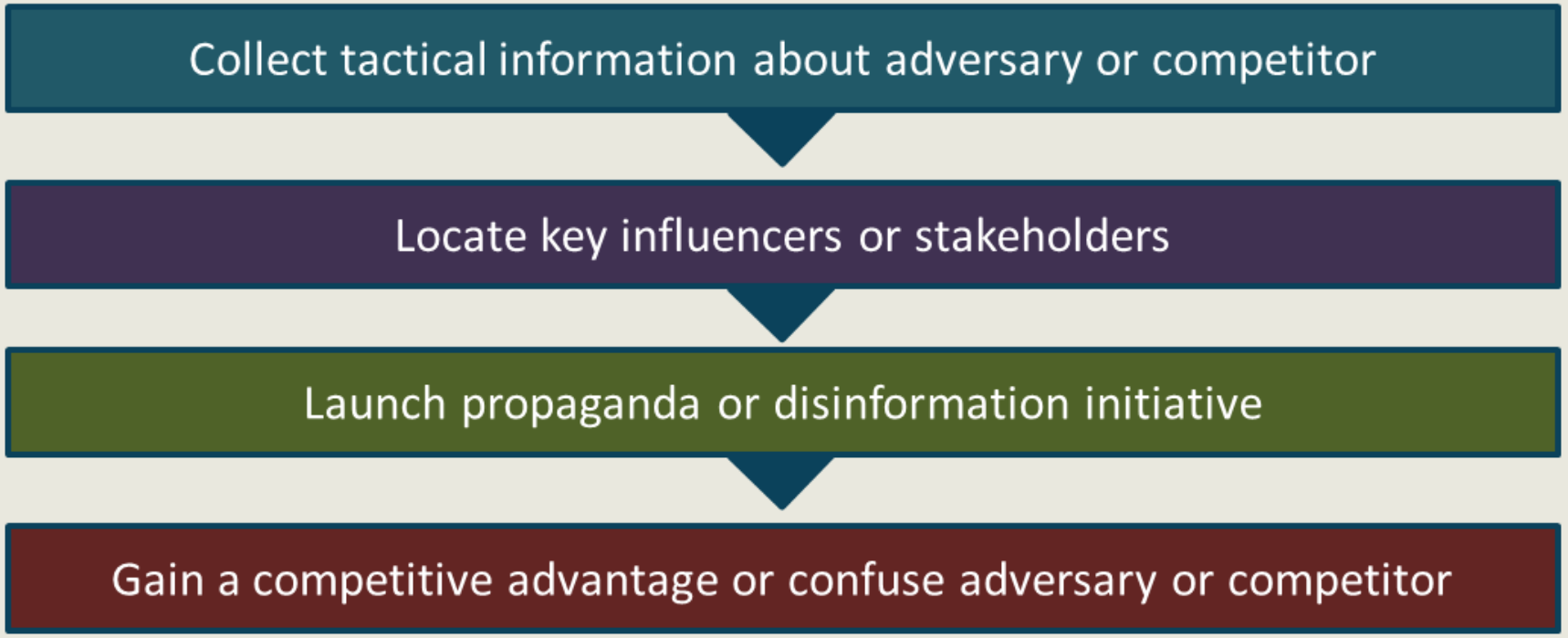
- Eliciting information and reconnaissance
- Hoaxes
- Identity fraud
- Impersonation and pretending
- Invoice scams
- Credential harvesting

Reacting to Hoaxes and Masquerading

- Employees should be well trained through security awareness programs to always be on the lookout for impersonators
- Politely ask for identification or authorization (guest badges or cards) unless policy restricts confrontations
- Policy may state that employees not confront suspects, but rather escalate suspicious people to a supervisor or security guard

Influence Campaigns

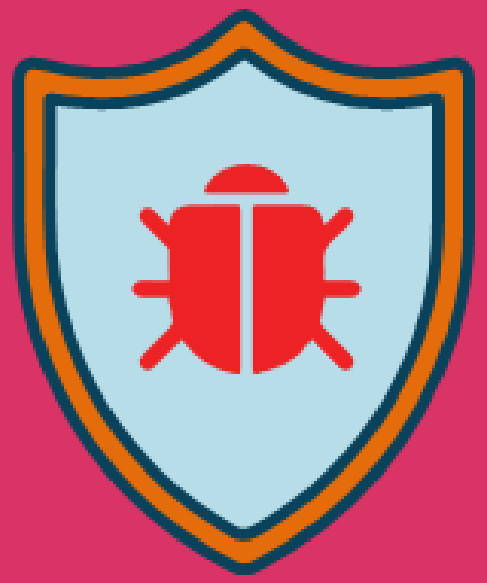
These campaigns are also called misinformation operations and influence operations



Reasons for Social Engineering Effectiveness

- Lack of proper security and awareness training
- Inadequate acceptable use policy (AUP)
- No buy-in from management and employees for prevention measures
- No enforcement of policies - no carrot and no stick
- Outdated anti-virus, DLP, and mobile device and application management tools
- Poor perimeter security controls for e-mail, messaging, telephony, and web activities

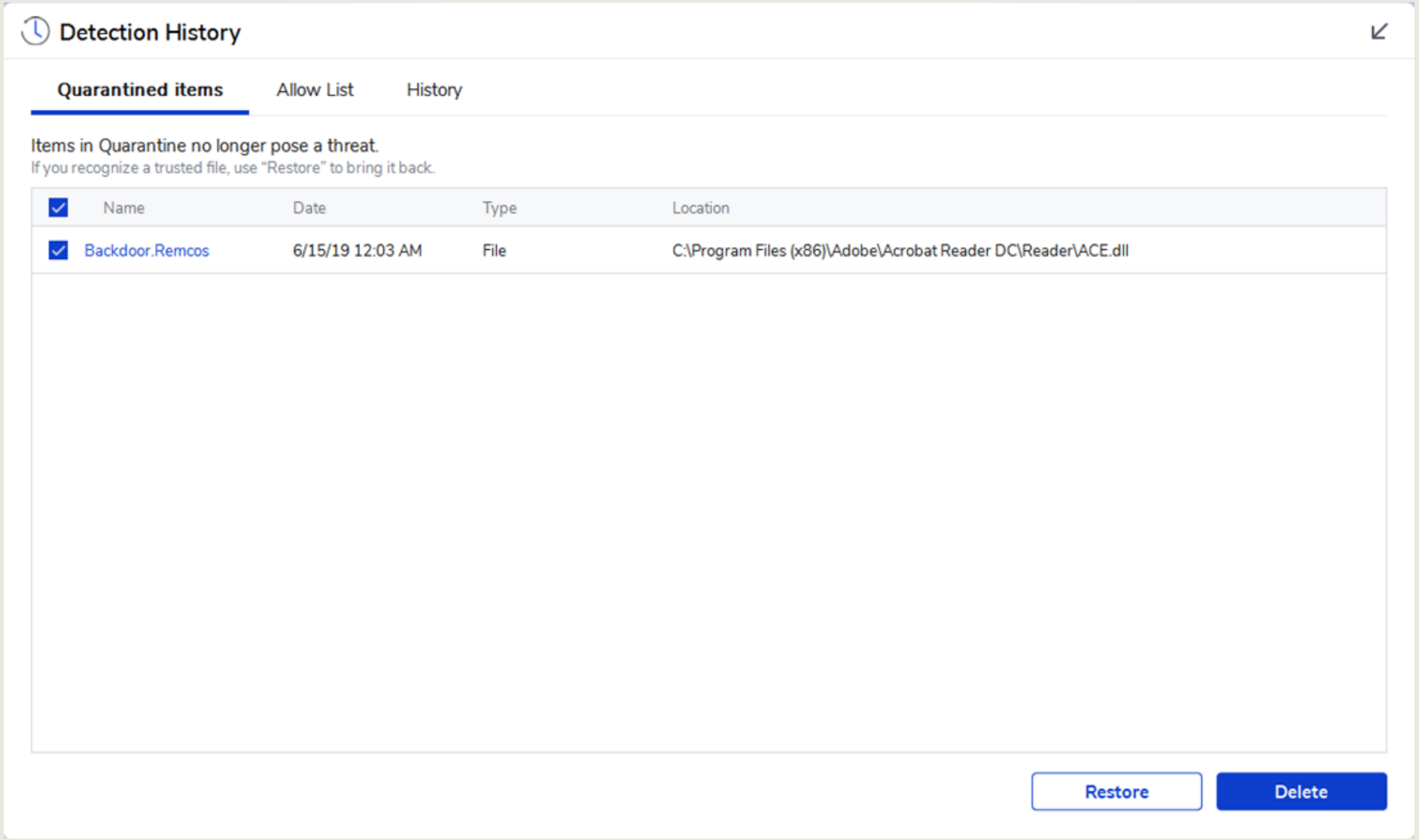
Common Malware Attacks



All malware are exploits but not all exploits involve malicious software code

- Potentially unwanted programs (PUPs)
- Ransomware
- Trojans and RATs
- Worms
- Spyware and adware
- Keyloggers

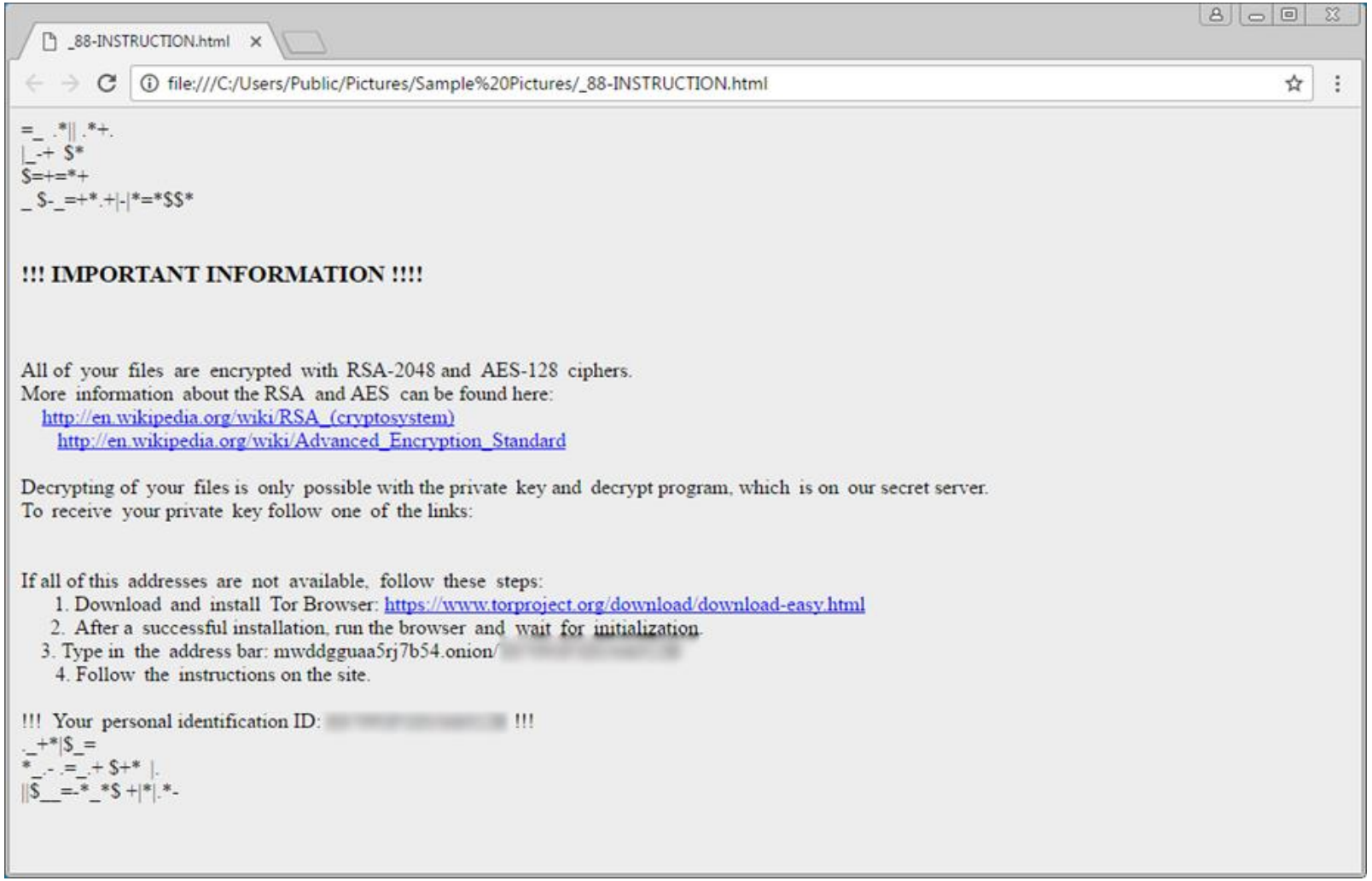
Potentially unwanted programs (PUPs)



Ransomware

- Malware encrypts key files and holds them for "ransom"
- Usually for a cryptocurrency such as Bitcoin or Monero
- Ransomware evolved from misleading "fix" apps to fake AV tools to bogus "fine" web sites
- CryptoLocker toolkits have exploded since Gpcoder in 2005
- The average ransom demand has more than doubled
- Over 30% of victims are in the U.S.
- Newest trend is Ransomware-as-a-Service (RaaS) on dark net, which is a subset of MaaS

Ransomware Campaigns



Ransomware Campaigns

1. INSTALLATION

Crypto-ransomware installs itself after bootup

2. CONTACTING HEADQUATERS

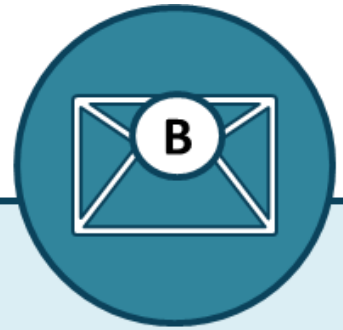
Malware contacts a server belonging to an attacker or group

3. HANDSHAKE AND KEYS

The ransomware client and server "handshake" and the server generates two cryptographic keys

4. ENCRYPTION

The ransomware starts encrypting every file it finds with common file extensions

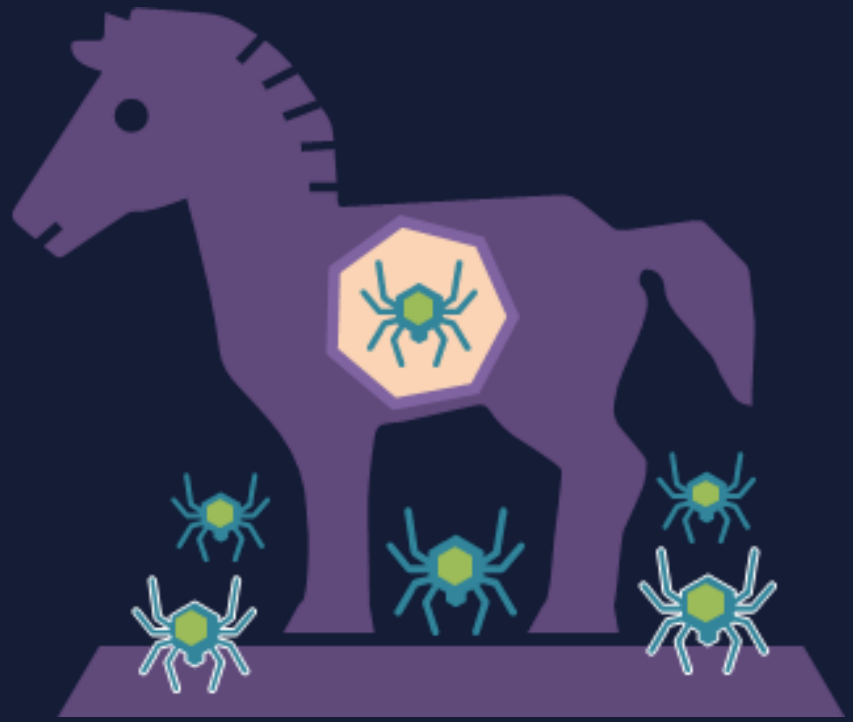


5. EXTORTION

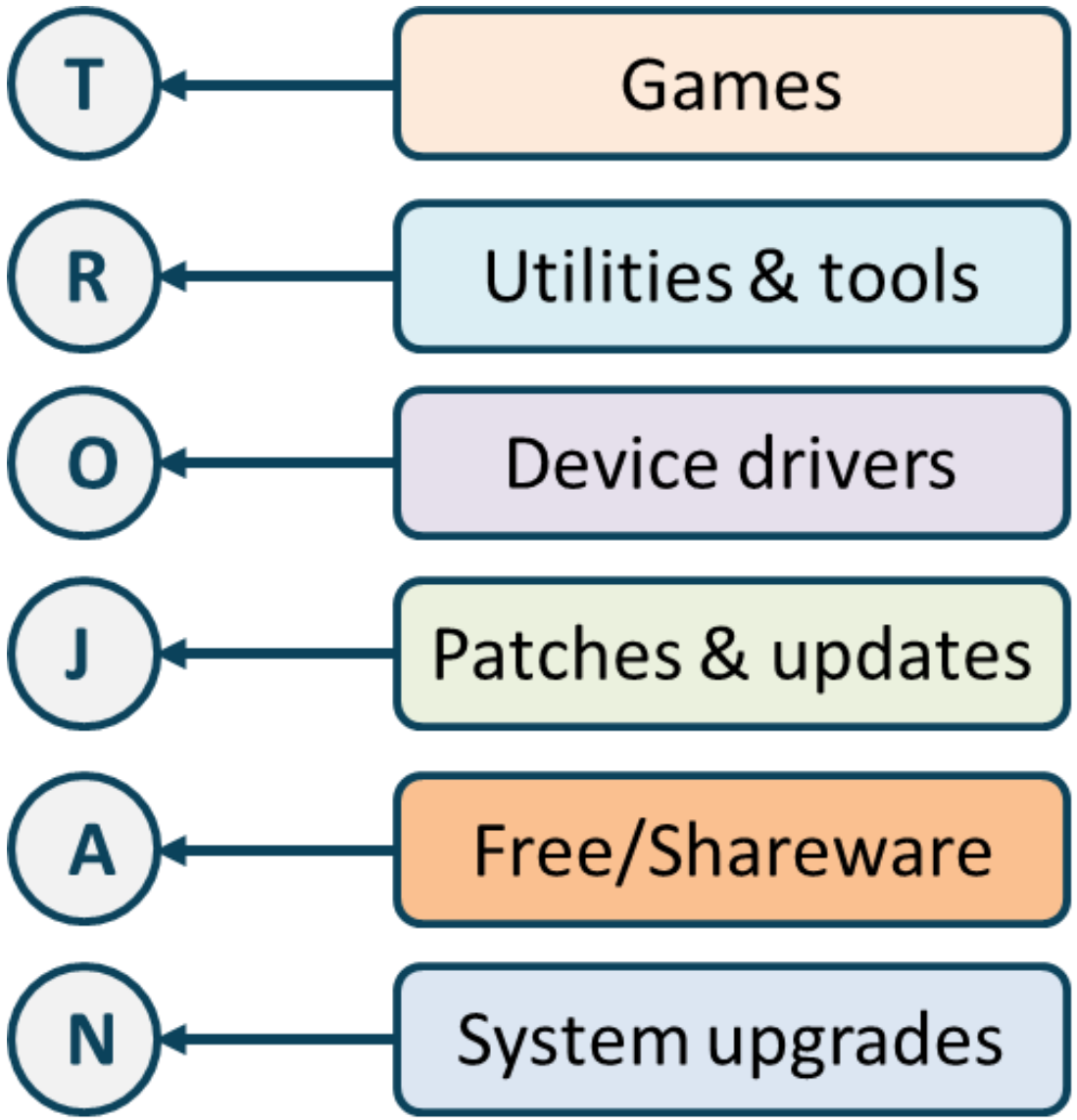
A screen displays giving a time limit to pay up before the criminals destroy the key to decrypt the files

Trojans

Beware Geeks Bearing Gifts!



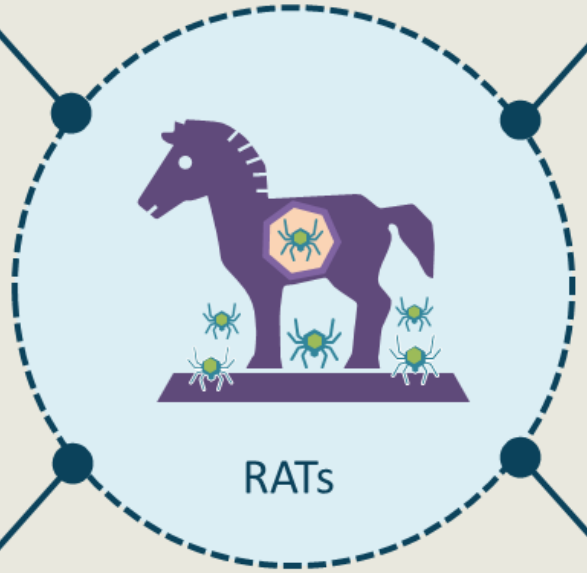
- They are malicious code and programs that masquerade as legitimate applications or are embedded in real programs
- Trojan horses have no replicating abilities like viruses or worms
- Trojans can also be part of a more elaborate distributed denial of service or botnet attack



Trojans can come in many forms

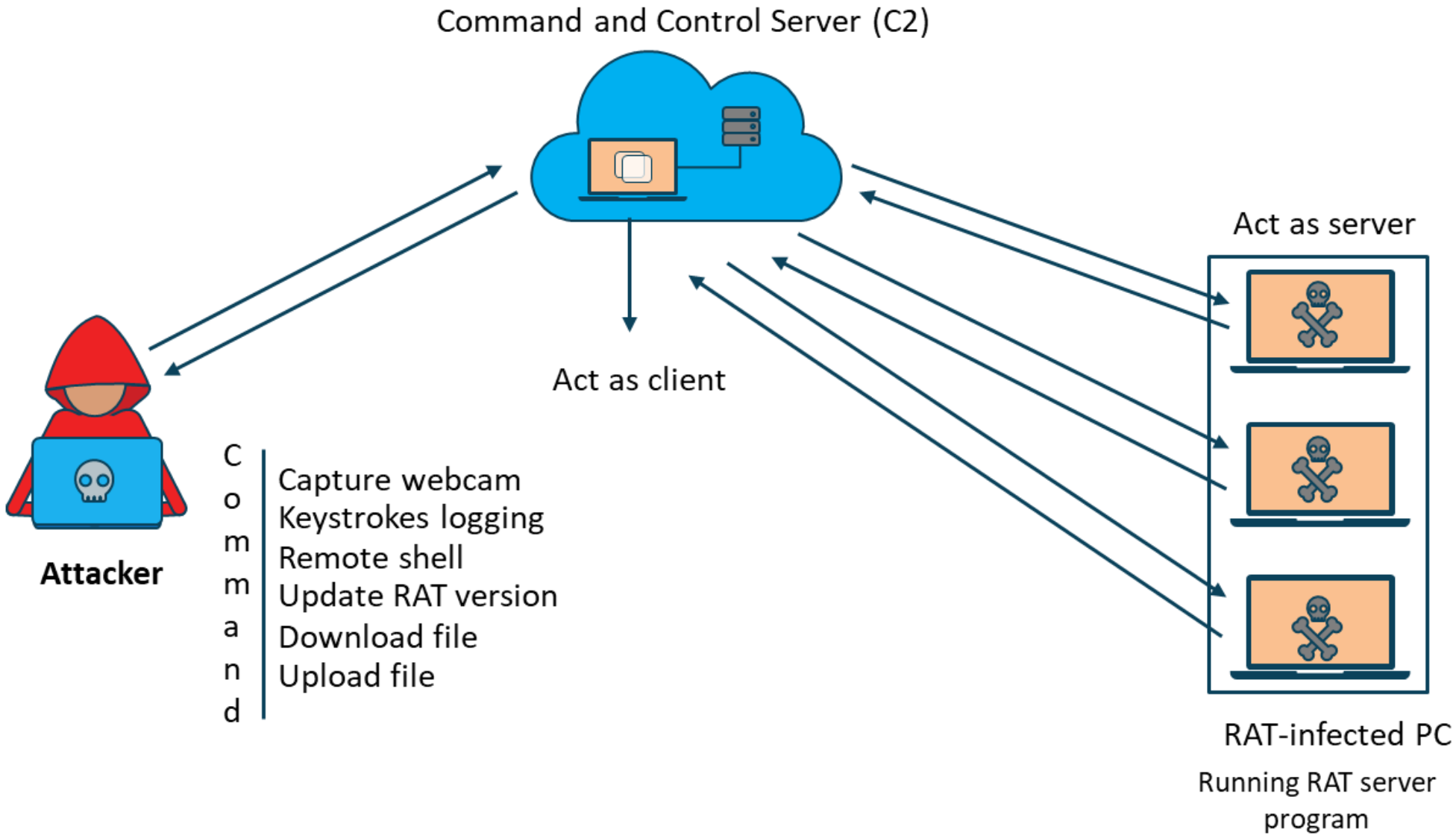
Remote Access Trojans (RATs)

Specific forms of Trojan horse malware - often part of multi-staged exploits



- Create backdoors
- Use C&C servers
- Now on mobile devices
- Gh0st, PlugX, Sakula

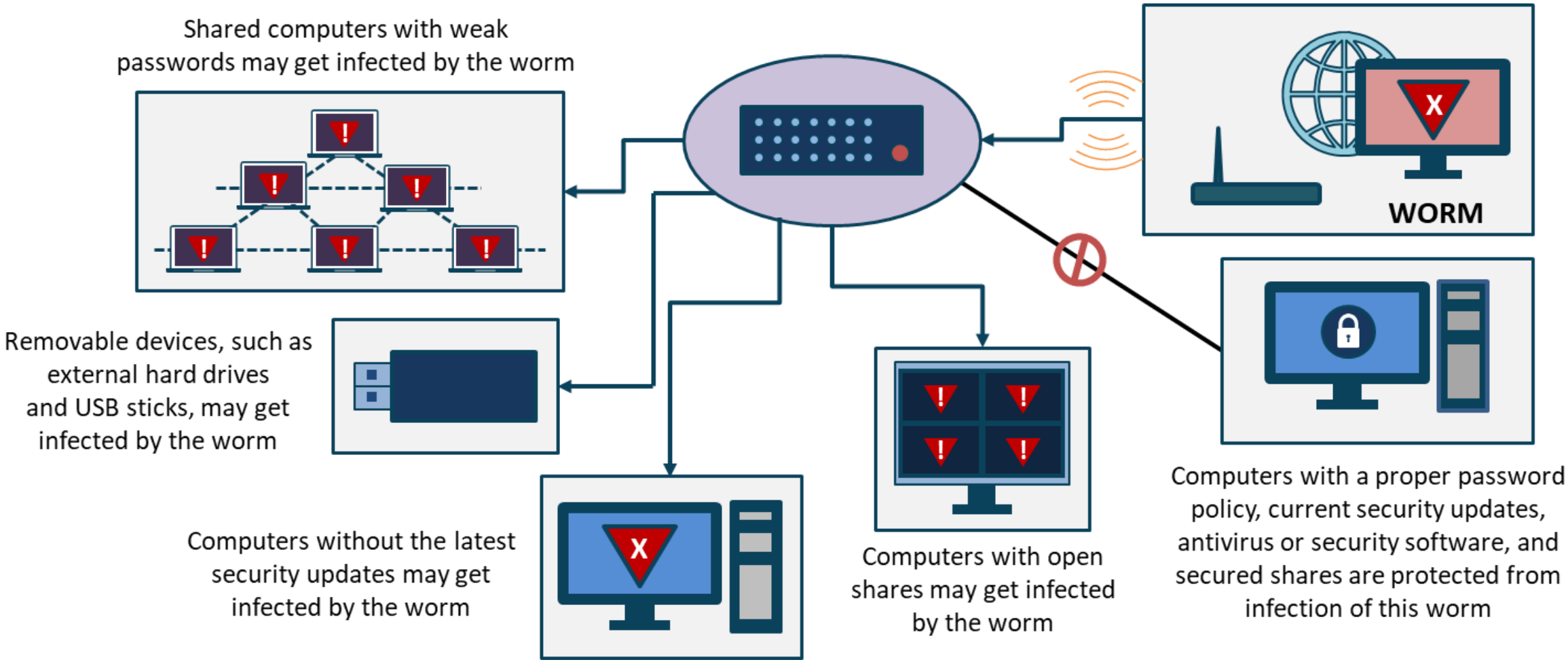
Remote Access Trojans



Worms

- Worms are a special form of self-replicating virus (malware) that generally spreads without user action
- They distribute complete copies (possibly modified) of themselves across networks
- A worm can consume resources, infiltrate data, or simply cause the CPU on the system to waste cycles resulting in a computer becoming unresponsive
- Because worms typically do not need to attach to a host program or file, they can also tunnel into a system and allow for remote control of the system or service
- Classic examples are Sasser, ILOVEYOU, Conficker, and Stuxnet

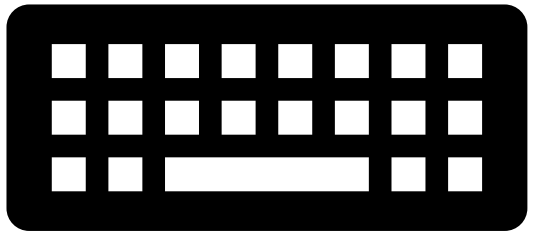
Worms


Shared computers with weak passwords may get infected by the worm
WORM
Removable devices, such as external hard drives and USB sticks, may get infected by the worm
Computers without the latest security updates may get infected by the worm
Computers with open shares may get infected by the worm
Computers with a proper password policy, current security updates, antivirus or security software, and secured shares are protected from infection of this worm

Spyware and Adware

Can be benign or malicious

- Spyware is software that gathers data about a computer user without the user's permission or knowledge
- 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



Keyloggers

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

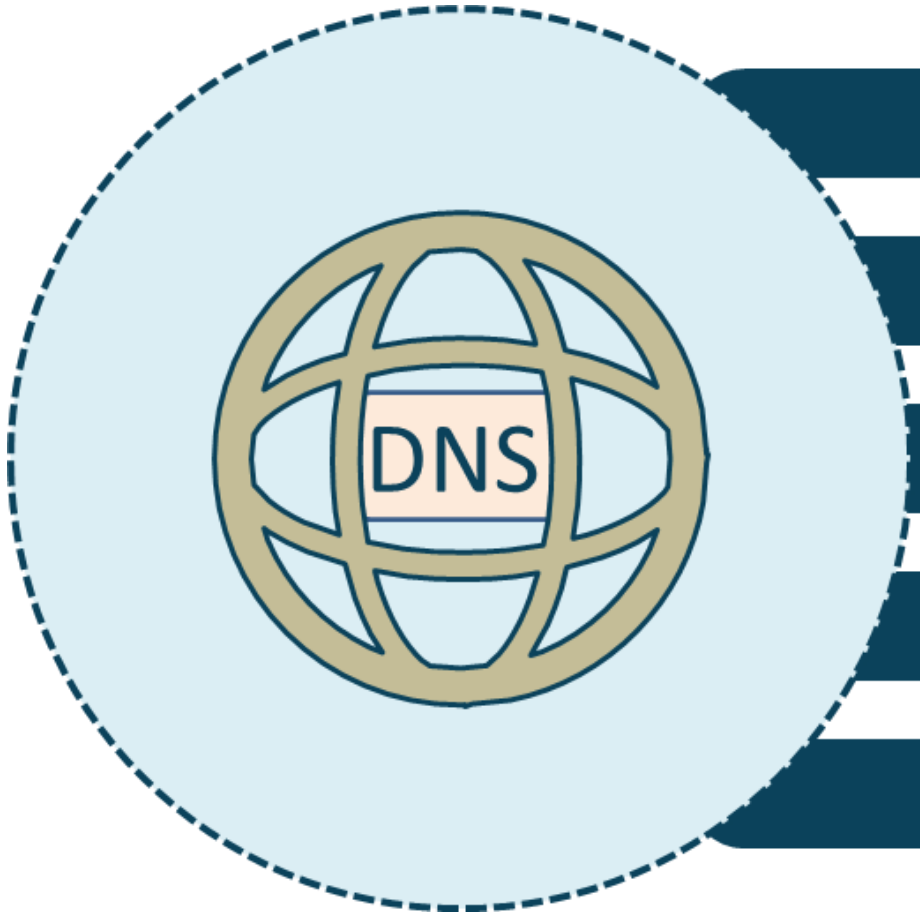
Domain Hijacking

- Domain hijacking or clickjacking, is 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
- This can also be done through URL redirection

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 web sites
- This is accomplished by name server misconfiguration, improper software design, and malicious exploits designed for the DNS system

Domain Reputation Attacks



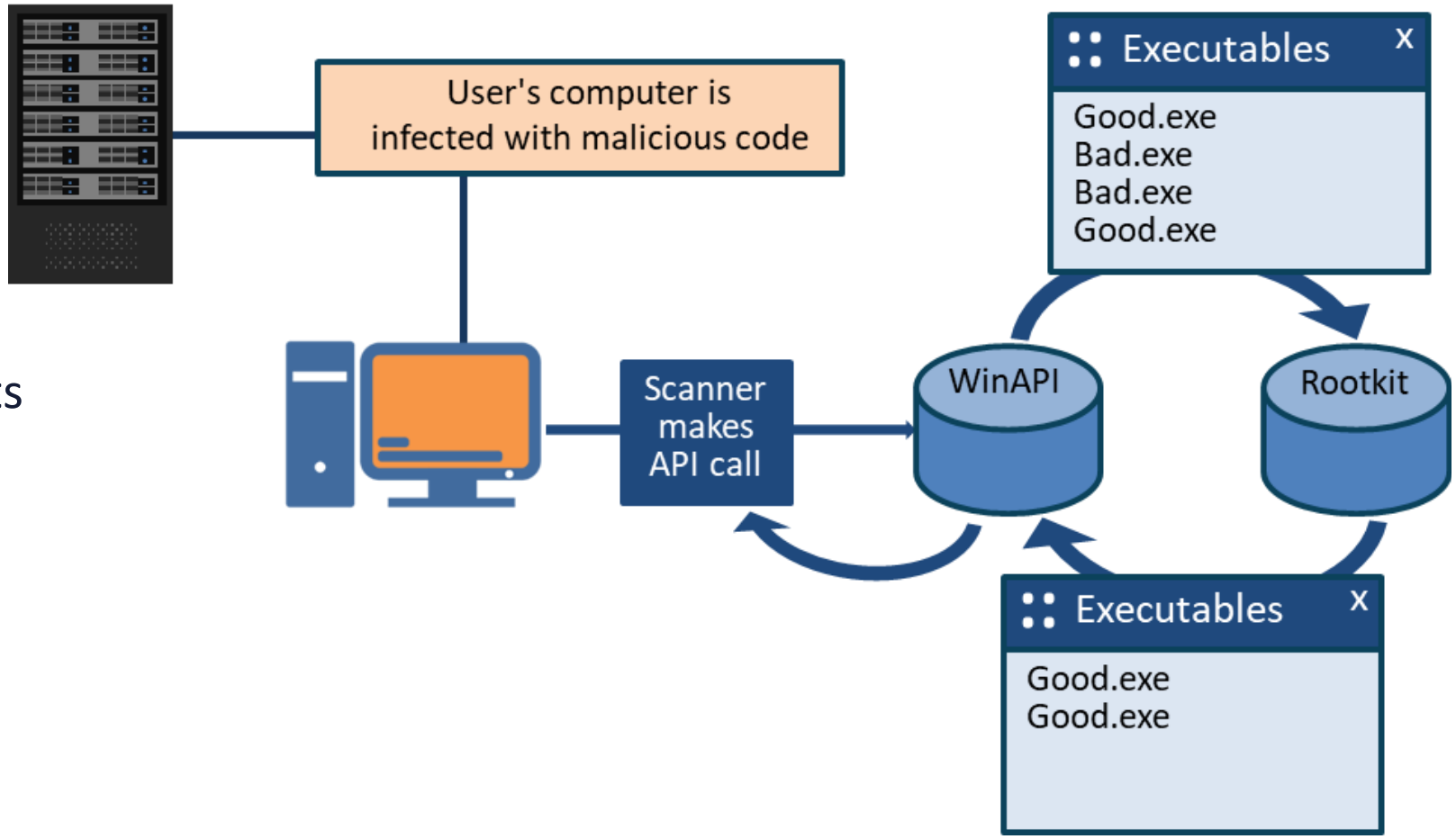
- Monitor domain interactions
- Bad domain associations
- Could be a spamming platform
- DDoS botnet takeovers
- Involves pentesting and threat intel

Complex Malware Types

Rootkits	Backdoors
Fileless viruses	Botnets
Crypto malware	Logic bombs
Stegomalware	Polymorphic packers
Multipartite virus	Emerging variants

Rootkits

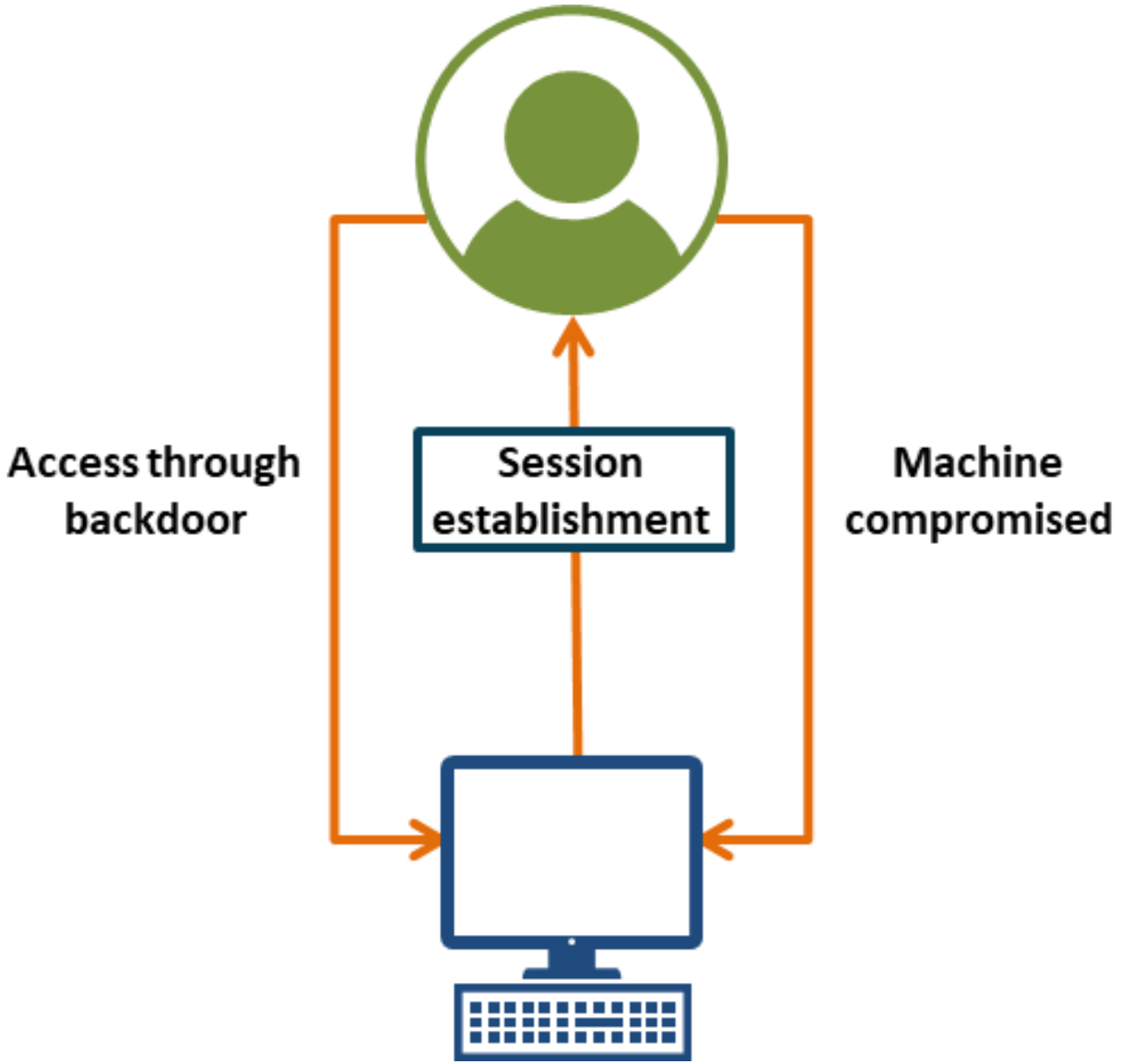
- Rootkits are malicious modules that are placed in unauthorized areas to:
  - Access data
  - Monitor actions
  - Escalate privileges
  - Modify programs
  - Conduct further exploits



Backdoors

A form of trojan malware

- Closely related to results of a botnet attack
- Generates a covert channel
- Remote attacker controls systems
- Common now on mobile devices



Backdoor Exploits

- Collect system and personal data from the system and even attached storage devices
- Perform DoS attacks on other systems (DDoS and botnet)
- 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

Fileless Viruses

Fileless operates in memory without being stored in a file or installed directly on a machine
Fileless viruses go directly into memory and the malicious content never reaches a hard drive

An evolutionary strain of malicious software

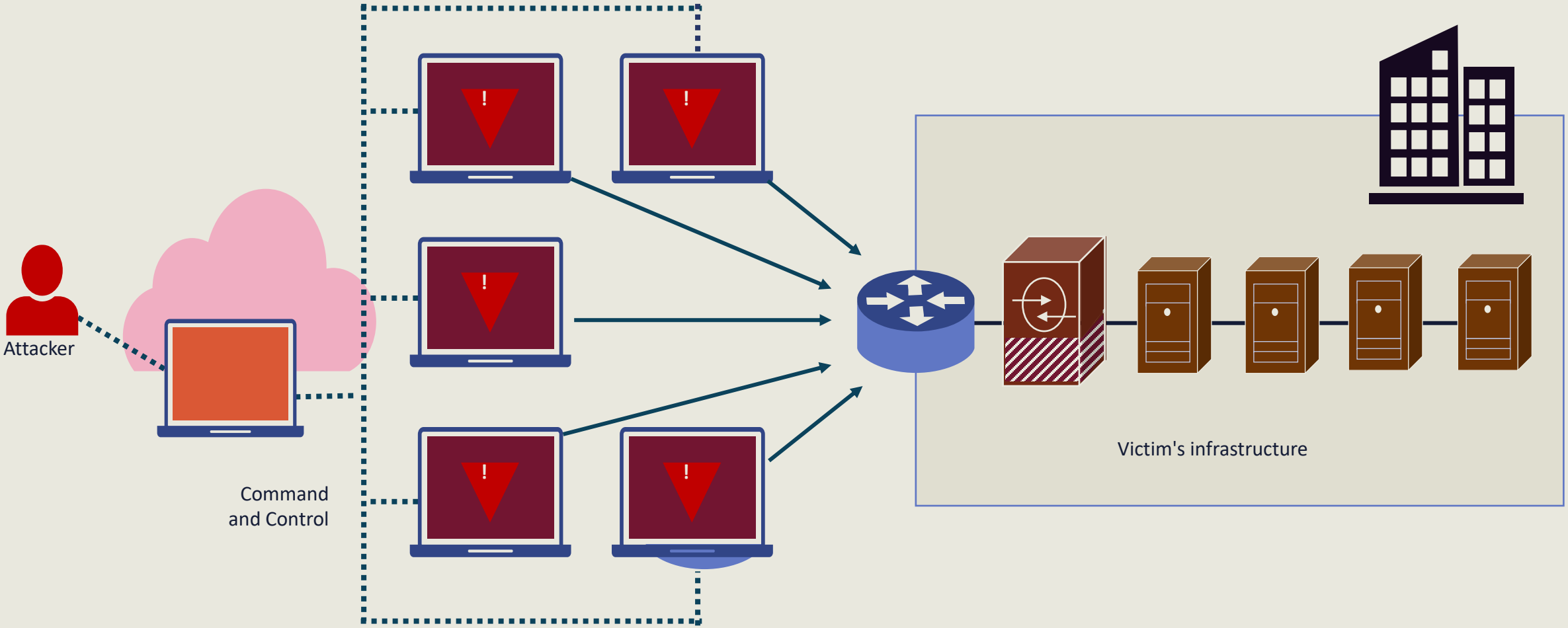
Banks, telecoms, and government agencies are top targets

Frodo and Dark Avenger

Bots and Botnets

- 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, force a system to participate in mining cyber currency, and more

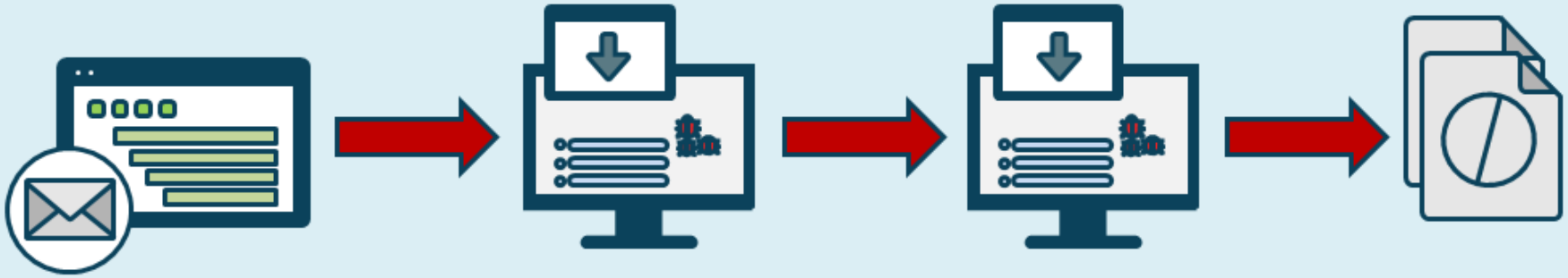
Bots and Botnets



Crypto Malware

Crypto malware is an advanced and evolving form of ransomware that encrypts a user's files and demands ransom

Sophisticated cryptomalware uses advanced encryption mechanisms so files can't be decrypted without a unique key



User receives spam with a malicious attachment

The malicious attachment, usually a UPATRE variant, downloads a ZBOT variant

The ZBOT variant exhibits several routines, including downloading CRILOCK variant

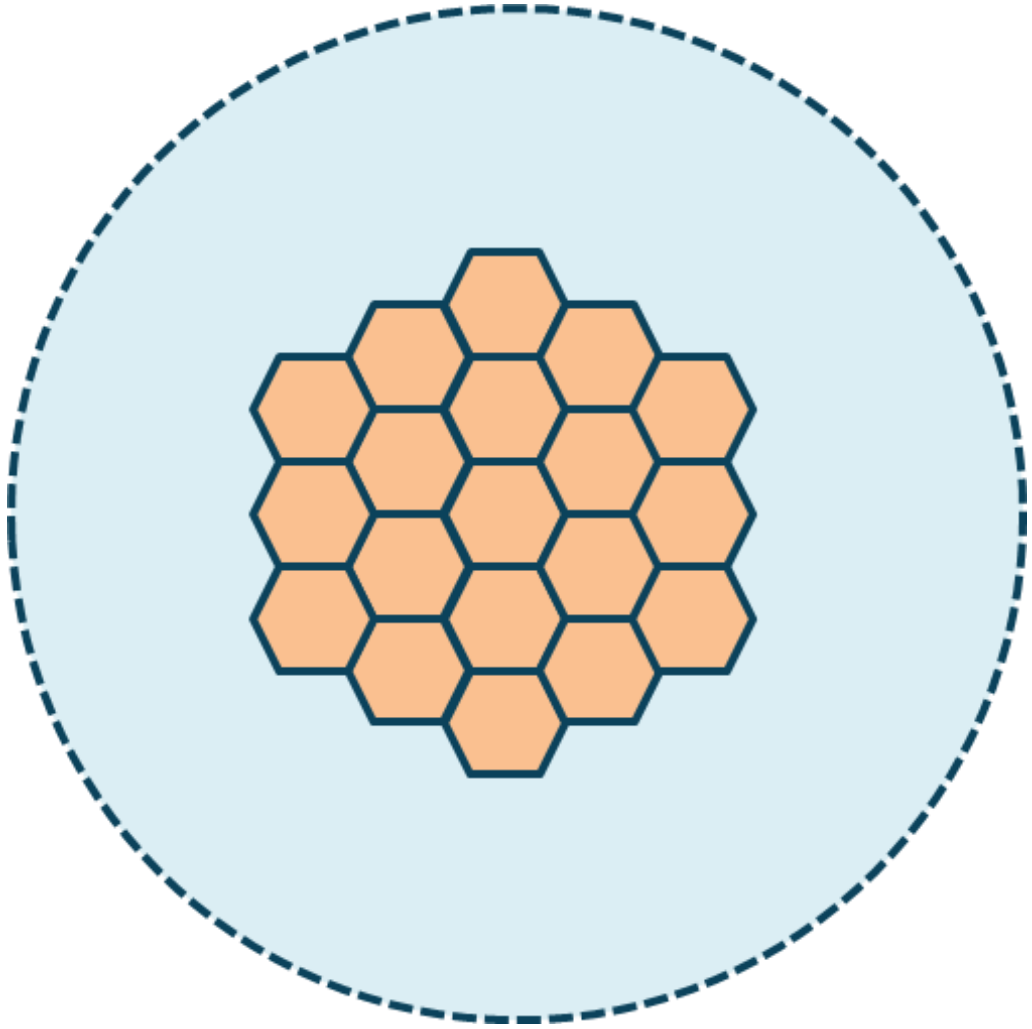
The CRILOCK variant encrypts files to force users to purchase the private encryption key

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

Stegomalware

- Steganography can be broadly defined as anything done by a cracker to hide data in an unexpected channel
- A JPEG picture of "a dog playing with bubbles" may actually contain destructive malware
- A dangerous banking RAT has hidden its settings in the icon file of a web site
- Many stegomalware hosting sites are buried deep in the Tor network
- Common tools are Steghide, rSteg, and Crypture



Polymorphic Packers

- Polymorphic malware has the ability to change and move in stages
- For example, starting out in RAM memory then moving into compressed RAR files deep in the file system
- Polymorphism is used in e-mail attacks and drive-by exploits, and also in APTs once the cracker has a foothold
- Polymorphic packers are tools that bundle up different types of malware in a single package (an e-mail attachment)

Multipartite Viruses

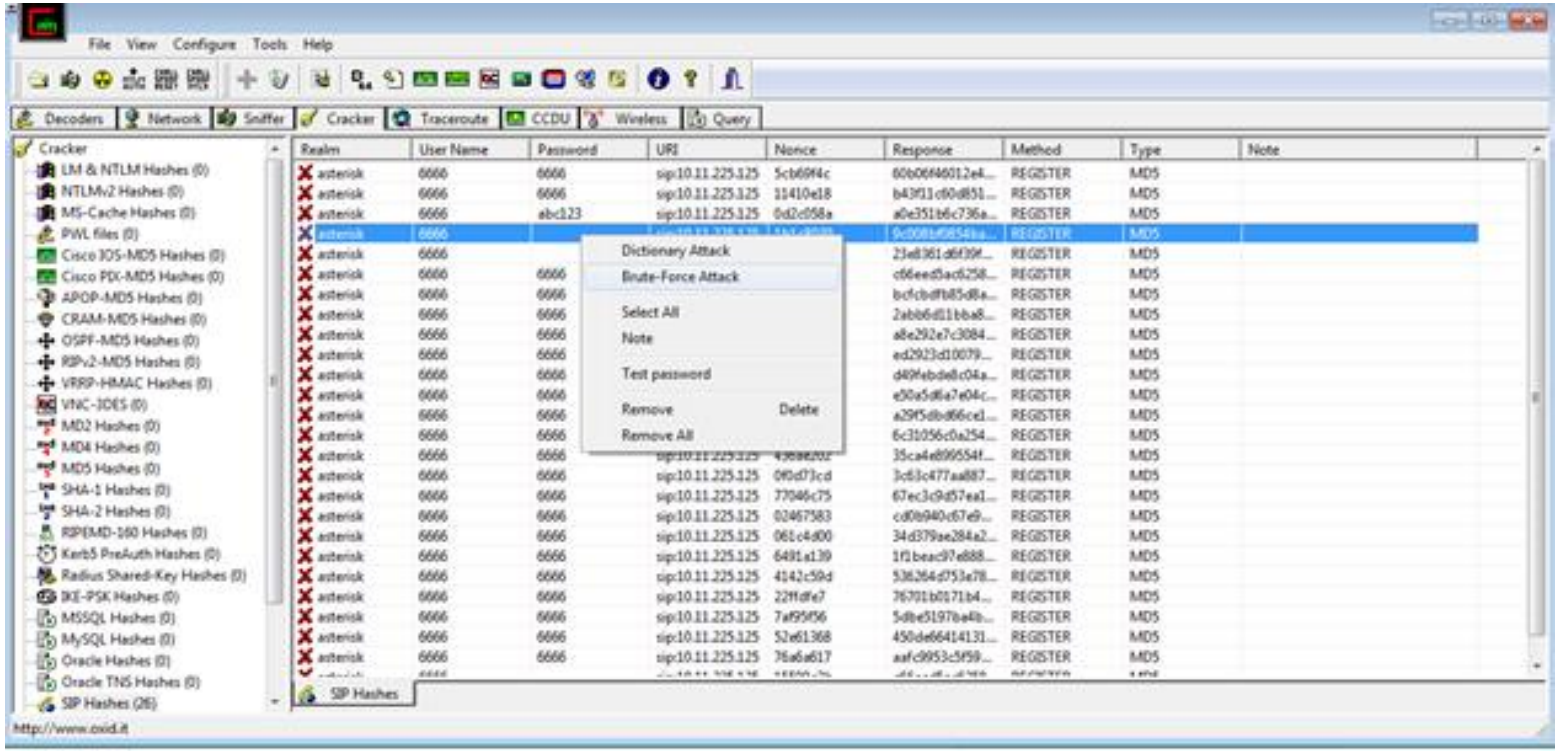
Also known as a multipart virus or malware

Often combines file and boot/system infector viruses

Simultaneously attacks the boot sector and executable files

Password Attacks

- Repeated attempts to identify a user account, password, or both
- Also runs against stored hashes on systems
- Attackers use many tools and techniques to crack passwords
  - Online brute force
  - Offline brute force
  - Dictionary and word lists
  - Cracked password lists
  - Rainbow tables
  - Spraying
  - Hybrid cracking



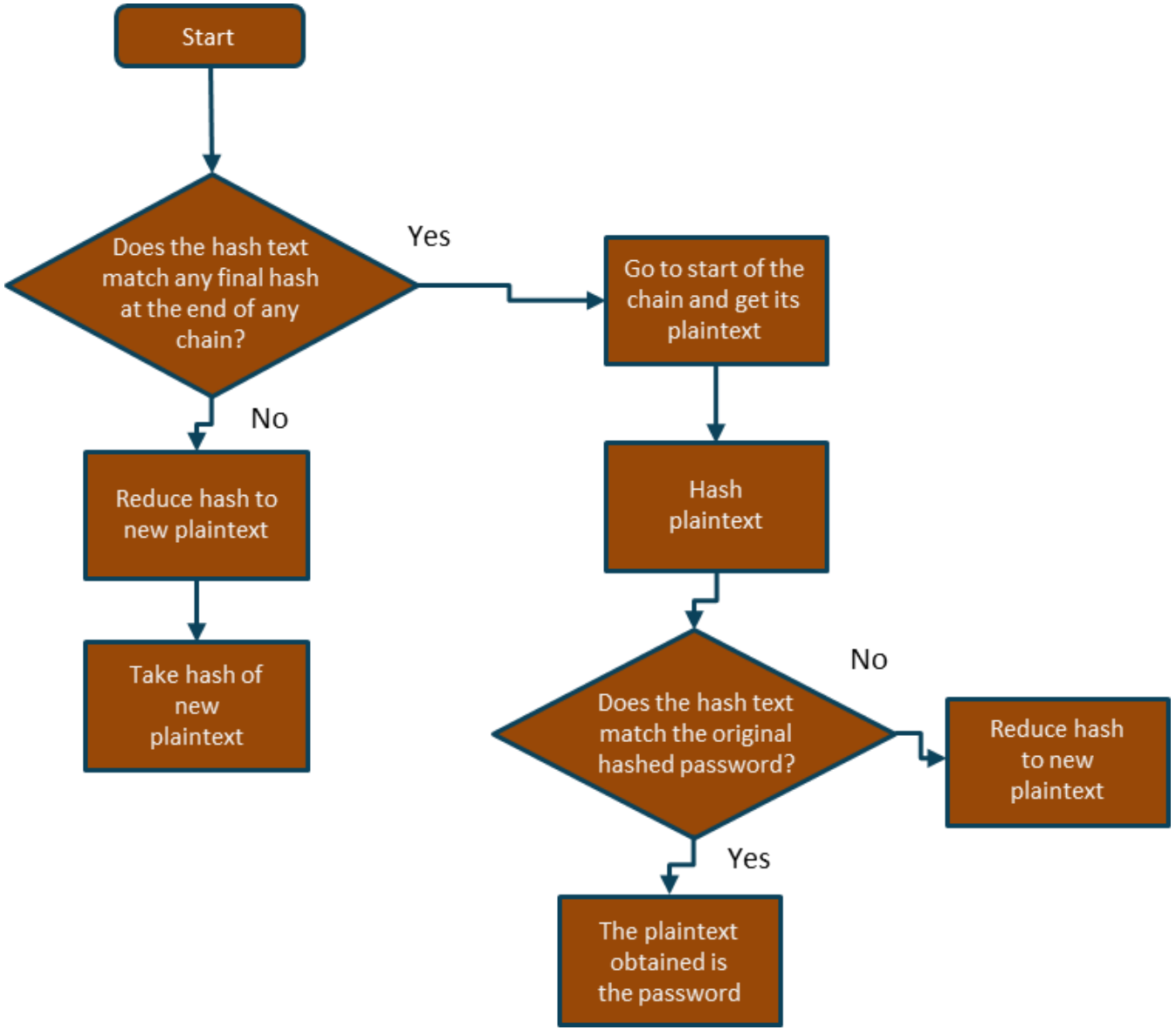
Spraying

- Attempts to access many accounts, typically targeting single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols
- Attackers use a few commonly used passwords instead of traditional brute-force attacks that can quickly result in the targeted account getting locked-out
- These "low-and-slow" methods involve the threat actor attempting a single frequently used password against many accounts before moving on to attempt a second password
- Allows the actor to remain undetected by avoiding rapid or frequent account lockouts

Rainbow Tables

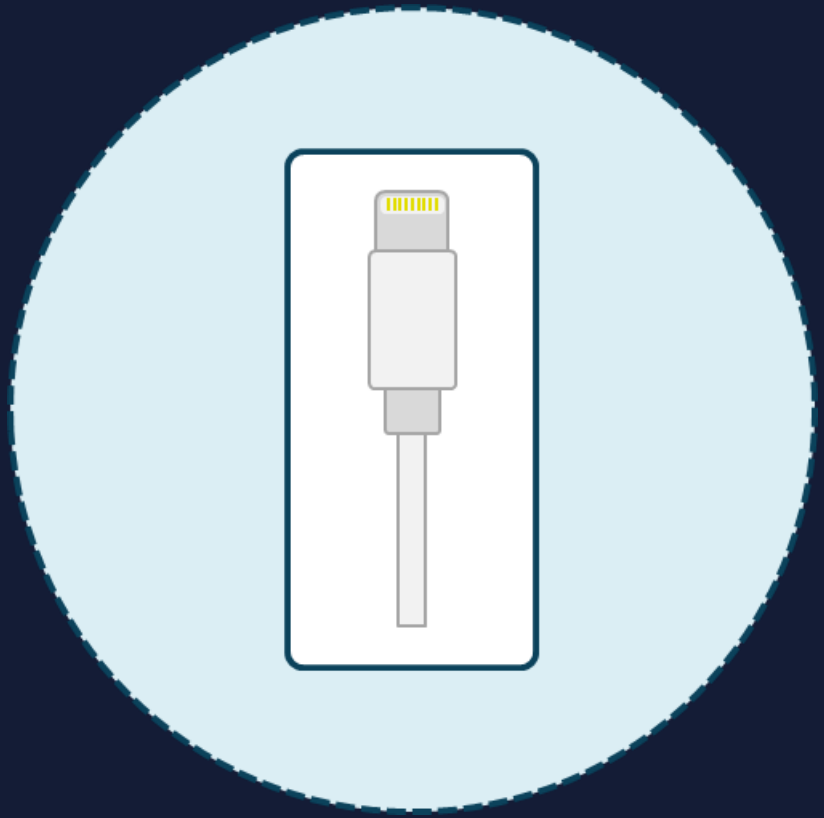
- Passwords in a computer system are not stored directly in plaintext, but are protected by a cryptographic hash function
- A rainbow table is a precompiled dictionary database of plaintext passwords
- It is a list of plaintext passwords and their corresponding hash values that can be used to find out what plaintext password produces a certain hash value

Using Rainbow Tables



Malicious USB Cables

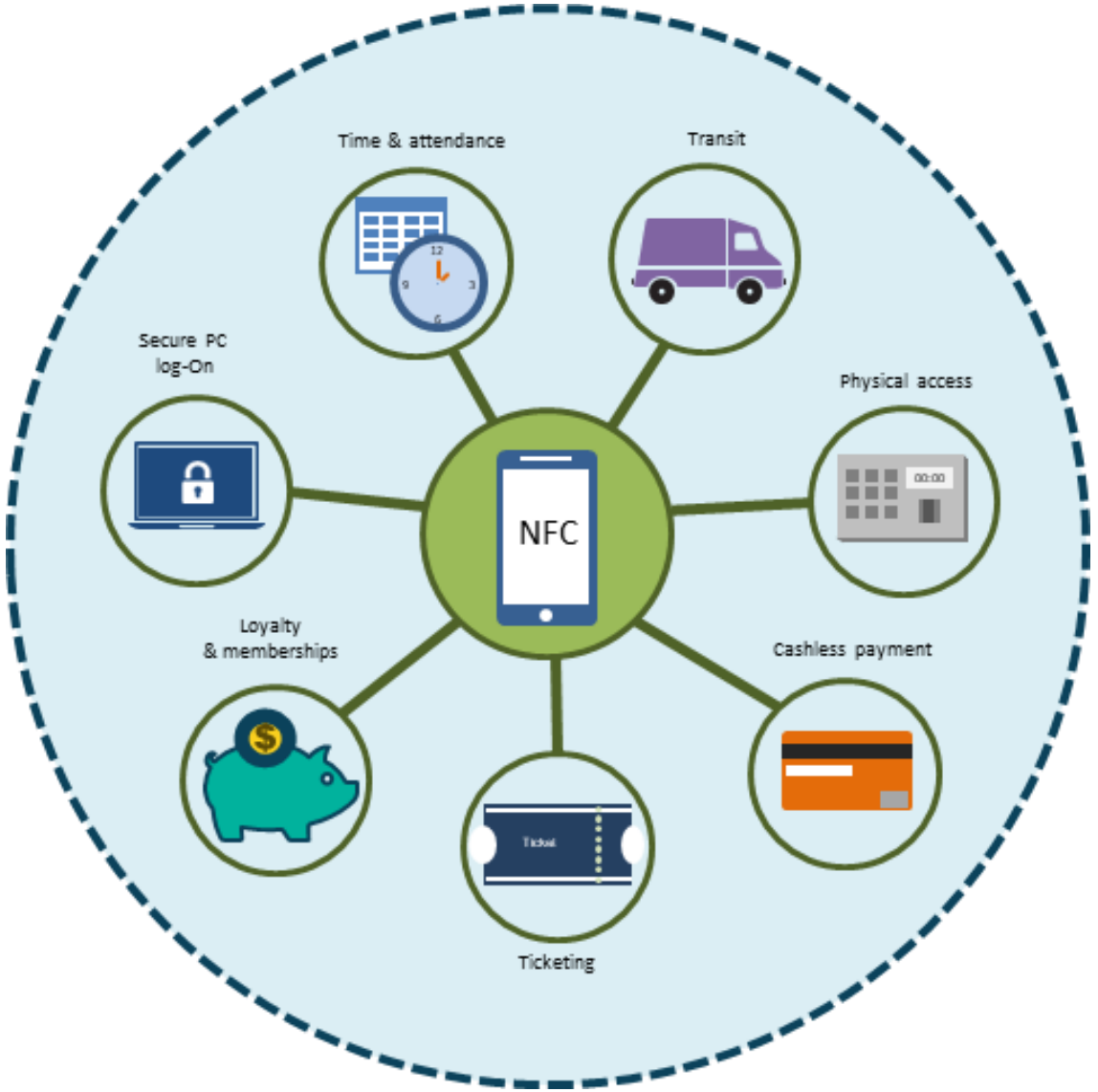
- Also know as an "evil" or "lightning" cable
- Attackers use a generic-looking USB cable that gets commands from a smartphone and runs them on the PC it's plugged into
- Some USB-to-lightning cables are tailored with a Wi-Fi chip inside one of the sockets
- Unfortunately, the cable will be detected by the computer as a Human Interface Device that resembles a keyboard or mouse
- It can also be connected to a malicious flash drive



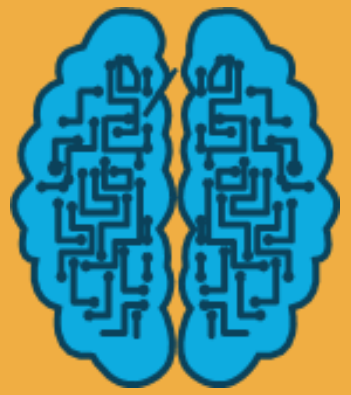
Skimming and Card Cloning

The benefits of RFID/NFC for travelers and shoppers are numerous - the tech is here to stay

- RFID and NFC devices are vulnerable to a variety of physical attacks
- Data stored on RFID chips can be stolen, skimmed, and scanned by anyone with easily obtained RFID readers
- Skimming uses devices that overlay an ATM machine or point-of-sale scanner to steal the information from the victim
- Crackers can also clone credit and debit cards by stealing the name, account number, expiration date, and 3-digit code



Adversarial Artificial Intelligence



- Artificial intelligence (AI), machine learning (ML), and robotic technologies with learning, reasoning, and decision-making abilities are rapidly being incorporated into security, analysis, defense, and military systems
- There is increasing apprehension about the solidity and safety of these emerging technologies
- A widely-discussed attack involves deceiving image classification algorithms
- Attackers can also taint the training data used for machine-learning algorithms and AI to skew or damage the results
- Cybersecurity experts have identified three types of attacks that can compromise unsupervised machine learning algorithms and systems: evasion attacks (adversarial input), data poisoning, and model stealing

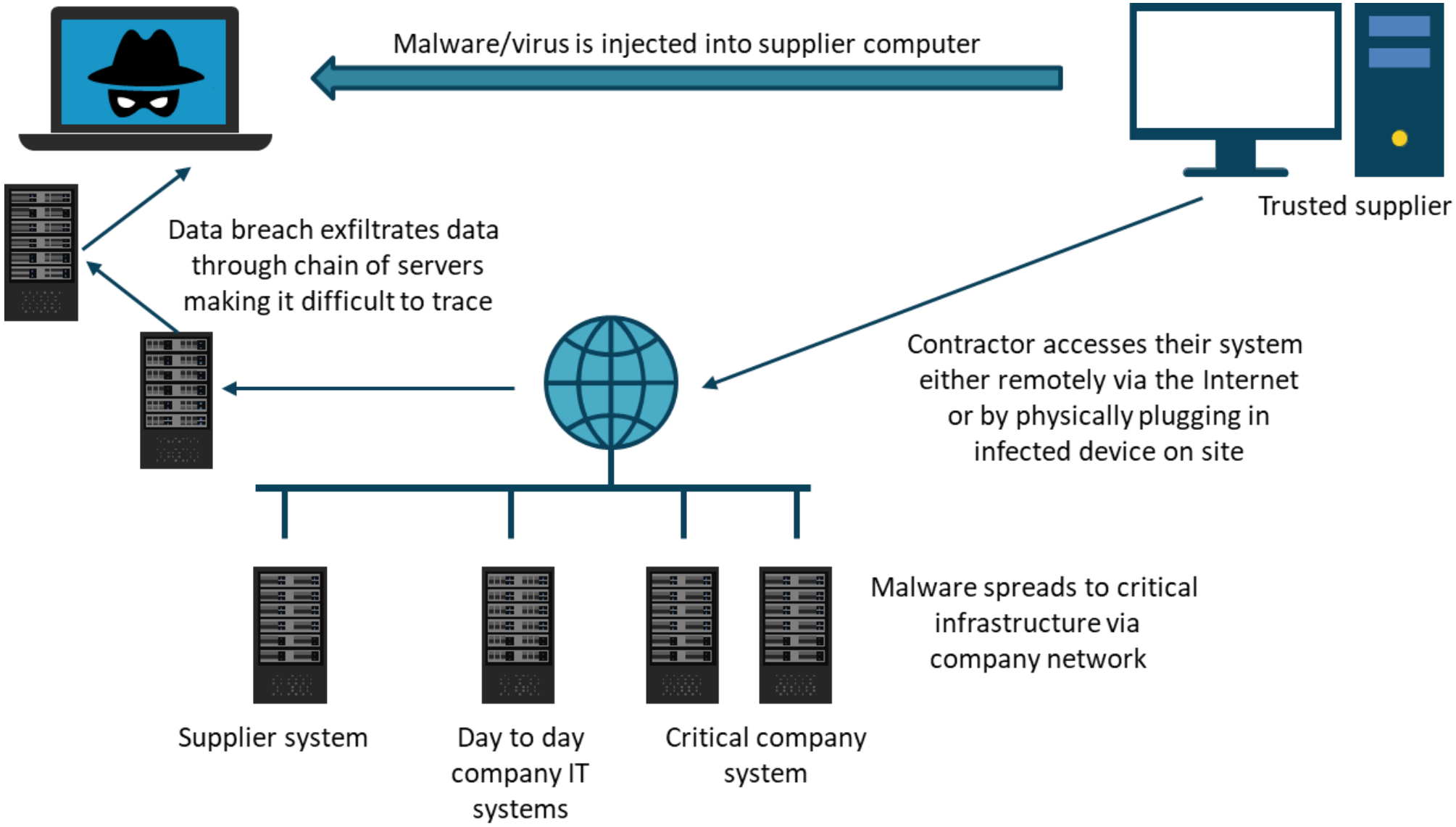
Supply Chain Attacks

Attacker infiltrates a system through an outside partner, vendor, or provider with access to your systems and/or data

Risks of supply chain attacks against sectors and software are growing due to new attack variants, growing public awareness, and increased oversight from regulators

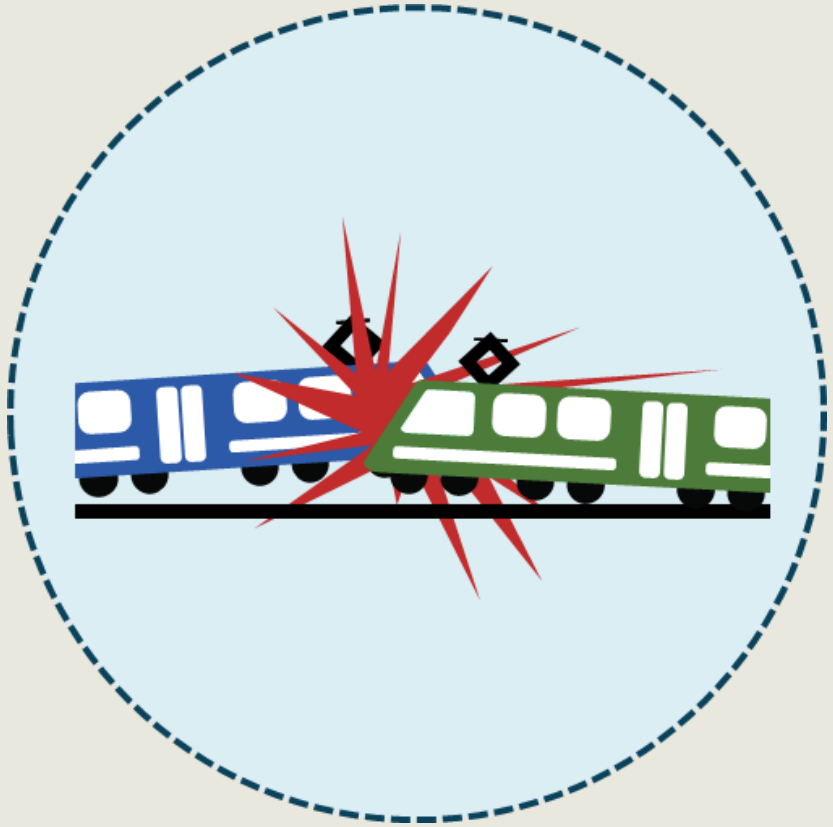
In 2018, 56 percent of organizations had suffered a breach that was caused by one of their vendors or partners

Supply Chain Attacks



Cryptographic Attacks

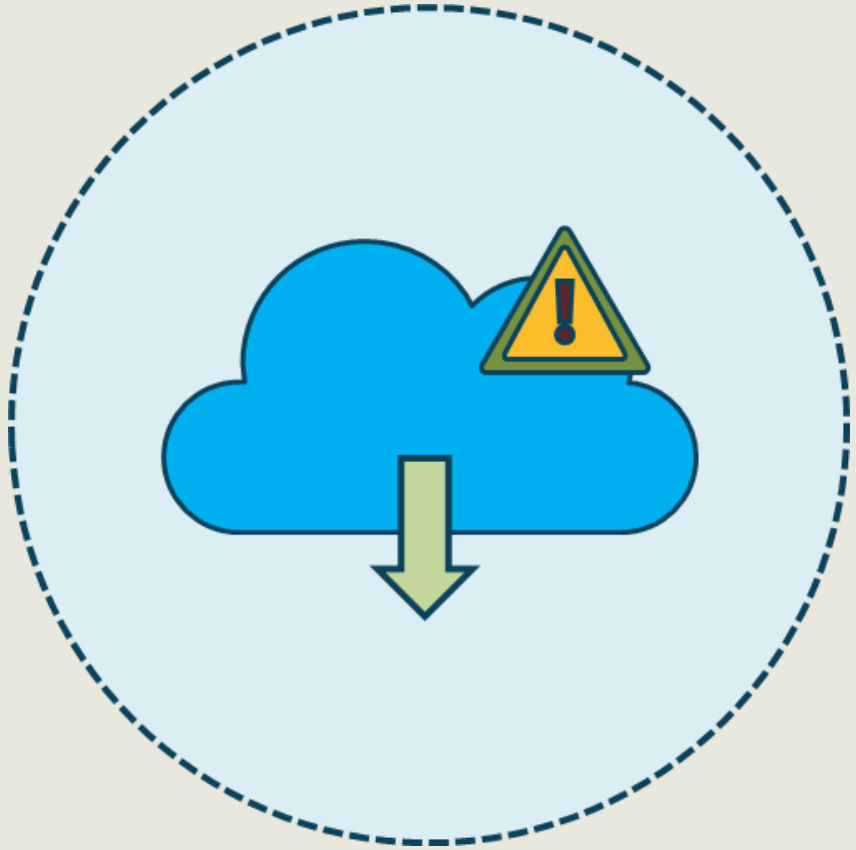
Collision Attacks



- 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
- In 2005, security flaws were found for SHA-1 in theoretical exploits that exposed weaknesses to collision attacks
- The SHA-2 family of hash functions was permitted by NIST for use by federal agencies in 2006 for all applications using SHAs

Cryptographic Attacks

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
- ESMTP is vulnerable since security had to be retrofitted into the protocol and the upgrade for encrypted delivery relies on a clear text STARTTLS command.
- SSL/TLS is particularly vulnerable (OpenSSL)

Cryptographic Attacks

- **Birthday attacks** – named from the birthday paradox, which is a known statistical probability where 2 individuals in a group of 32 will have the same birthday 50% of the time
- **Known plaintext attacks** - 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**s - 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

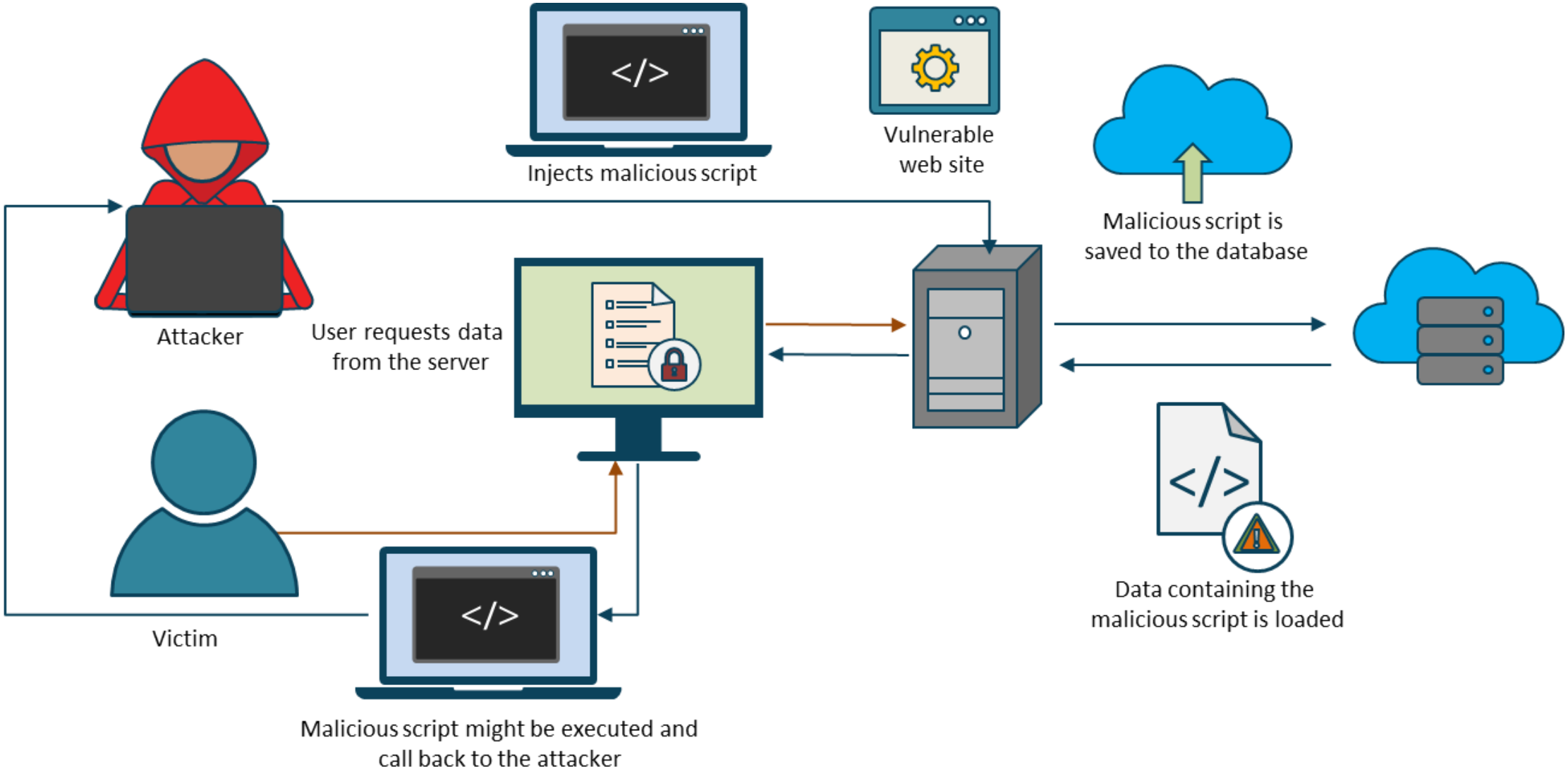
Privilege Escalation

- Advanced Persistent Threats (APTs) often attempt an escalation of access privileges soon after the initial compromise phase
- 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, and the more potential there is to damage or exfiltrate critical data
- Exploits programming errors and system design flaws to give an attacker elevated access to the network and related systems, data, and applications
- Privilege escalation can occur during the attack kill chain or as part of penetration testing
- Can be vertical vs. horizontal
- Least privilege principles are key

Cross-Site Scripting (XSS)

- Flaws in pages rendered by web servers and not the web server code itself (i.e. Apache, IIS) where malicious scripts or code are injected into trusted or innocent web sites pages
- Malicious scripts can steal cookies, session tokens, or other sensitive data stored by the browser and used with the site
- 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

Cross-Site Scripting (XSS)



Cross-Site Scripting (XSS)

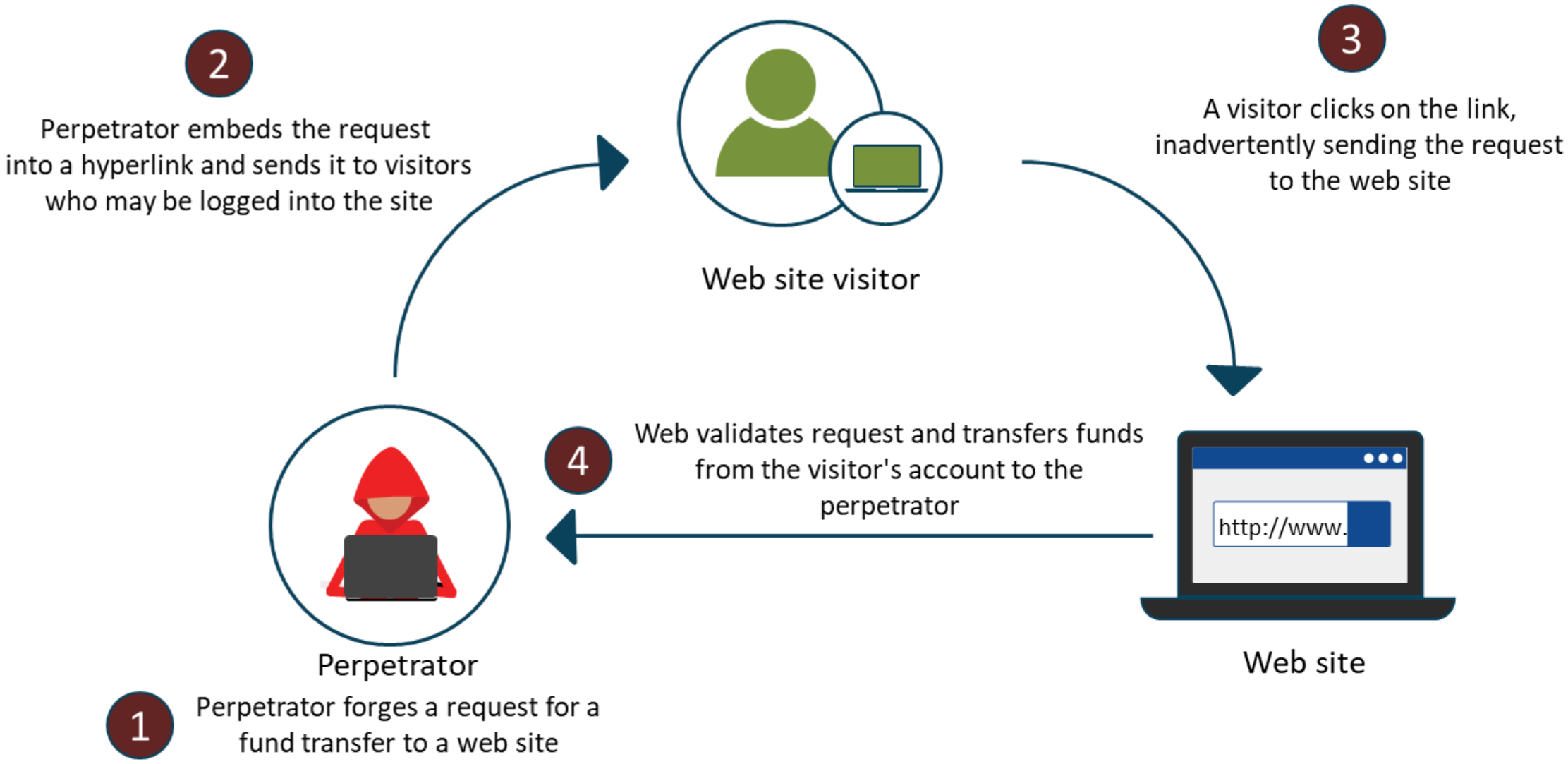
- DOM-based XSS (Local or Type 0)
- Reflected XSS (Nonpersistent or Type 1)
- Stored XSS (Persistent or Type 2)

Cross-Site Request Forgery (CSRF/XSRF)

Leverages authenticated sessions

- Attack forces an end user to perform undesirable actions in a web application in which they are authenticated
- An effective CSRF/XSRF 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

Cross-Site Request Forgery



Malicious Code and Script Execution

Malicious code

- This is the generic term from which malware is derived
- 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

Malicious script

- Script viruses are written using script languages
  - This type of virus either infects other scripts or forms a part of multicomponent viruses
- It affects only those applications for which it has been written
- Script viruses are spread through e-mail attachments

Injection Attacks

Often the result of MITM exploit or Remote Access Trojan attack

- Malware can inject false MAC or IP addresses
- DLL injection is where malicious code forces itself to run in place of other benign code
- This "injected" code is usually code written by a third-party developer, designed to perform some malicious function

SQL Injection (SQLi)

- Involves inserting a SQL query through input data from client to server application and can allow for several exploits
  - Read sensitive database data (SELECT FROM)
  - Change database data (INSERT, UPDATE, DELETE)
  - Execute administrative functions (e.g., shutdown DBMS)
  - Get contents of files on database management system (DBMS)
  - Run commands on operating system

LDAP Injection

- LDAP is often used in web applications over the Internet or a corporate intranet
- The web applications take the input from the client in order to process it further, so the attacker exploits the data not being properly sanitized or going directly to a back-end database
- The attacks can render sensitive user information or change information in the LDAP directory

XML Injection

- XML or SOAP injection vulnerabilities occur when user input is inserted into a server-side XML document or SOAP message in an insecure manner
- May be possible to use XML metacharacters to modify the structure of the resulting XML
- Depending on the XML function, it may be feasible to interfere with the application's logic and conduct unauthorized actions or access sensitive data
- This kind of vulnerability can be difficult to detect and exploit remotely

Targeted Coding Attacks

- Pointer/object dereference
- Directory traversal
- Buffer and integer overflows
- Race conditions - time of check/time of use
- Improper error and input handling
- Session replay attacks

Pointer/Object Dereference

An attacker can supply a pointer for memory locations that the program is not expecting

A null-pointer dereference occurs when a pointer with a value of NULL is used as if it actually points to a valid memory area

A program can possibly dereference a null pointer, and in doing so, raise a NullPointerException

Null pointer errors are frequently the result of one or more programmer assumptions being violated

Directory Traversal

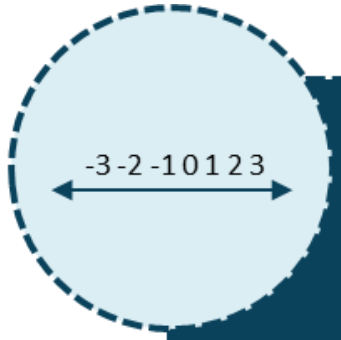
- The Directory Traversal attack is also known as path traversal attack or a "dot slash" and is most often launched though web browsers and other clients
- This HTTP exploit allows an attacker to access restricted files, directories, and commands located outside of the root directory
- Attackers can modify a URI or URL to force the web server into exposing the restricted files
- Examples include

	Forward slash character (../)	Backslash character (..\)
URL encoded characters	..%2e%2e%2f	..%2e%2e%5c
Unicode encoding	..%u2216	..%c0%af
Double encoding	..%252F	..%255C

Buffer and Integer Overflows

Buffer overflows

- Attacker sends larger than expected input, for example when a server accepts it and writes to memory areas
- 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



Integer overflows

- A type of an arithmetic overflow error when the result of an integer operation does not fit within the allocated memory space
- Instead of an error in the program, it usually causes the result to be unexpected
- These are in the top 10 of the most dangerous software errors, mostly because they often lead to buffer overflows

Race Conditions

- A race condition is when a system or software tries to do two or more things simultaneously, but due to the type of system, the operations must be done in the correct sequence in order to function properly
- Race conditions are classically related to synchronization errors in software code
- Crackers can leverage a known race condition vulnerability to get unauthorized access to a system or network

Time-of-check vs. Time-of-use (TOC/TOU)

- A time-of-check vs. time-of use (TOC/TOU) attack is a race condition and occurs when an attacker tries to gain privilege to a system by "racing" it to the resource it is attempting to access
- The types of programming flaws that allow for race conditions occur when the system (or application) splits up the operations of verifying credentials and providing access to a resource
- It can do things such as replacing a config.sys file with a different file that compromises the system before the system even loads its operating system

Improper Error and Input Handling

- Poorly defined validation rules used in verifying the correctness, completeness, and acceptability of input data
- Software applications and web servers are notorious
- Must establish data input, data flow, and data output requirements with designed security features in mind
- Collisions are in this category when the chance that two unique inputs will produce the same output (MD5 and SHA-1 are vulnerable)

Session Replay Attacks

- An attacker steals a valid session ID of a user and reuses it to impersonate an authorized user
- Example: web applications that allow reusing old session IDs or session credentials for authorization are also vulnerable to these attacks
- IPsec and TLS have anti-replay mechanisms to protect the secure session

API Attacks

- An API DDoS attack often involves sending traffic from many clients to overwhelm an API service
- Even if rate limiting controls are in place to prevent servers from crashing, they cannot always prevent service disruption and severe degradation of the API's user experience
- If API calls are not digitally signed or if they have embedded credentials, they can be compromised
- API attack vectors:
  - Login attacks
  - DDoS attacks
  - MITM
  - Leveraging credentials

Pass The Hash Attack

- Example: on Windows networks, hackers do not need the plaintext passwords to access certain services
- 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
- Windows Safe Mode is vulnerable - it is an OS diagnostic mode of operation that has been around since Windows 95

Driver Manipulation

- A common vector is the hardware drivers that we install in our operating systems
- This is privileged code that is trusted by the operating system
- Can be trojans, RATs, or hacked driver software to deliver the payload

Shimming

- Shimming is the process of stealing information and money from Point-of-Sale systems, credit card readers, and ATM machines
- The attack is common at gas stations, convenience stores, and kiosks
- It can be an overlay attachment or sometimes an entirely replaced device

Refactoring

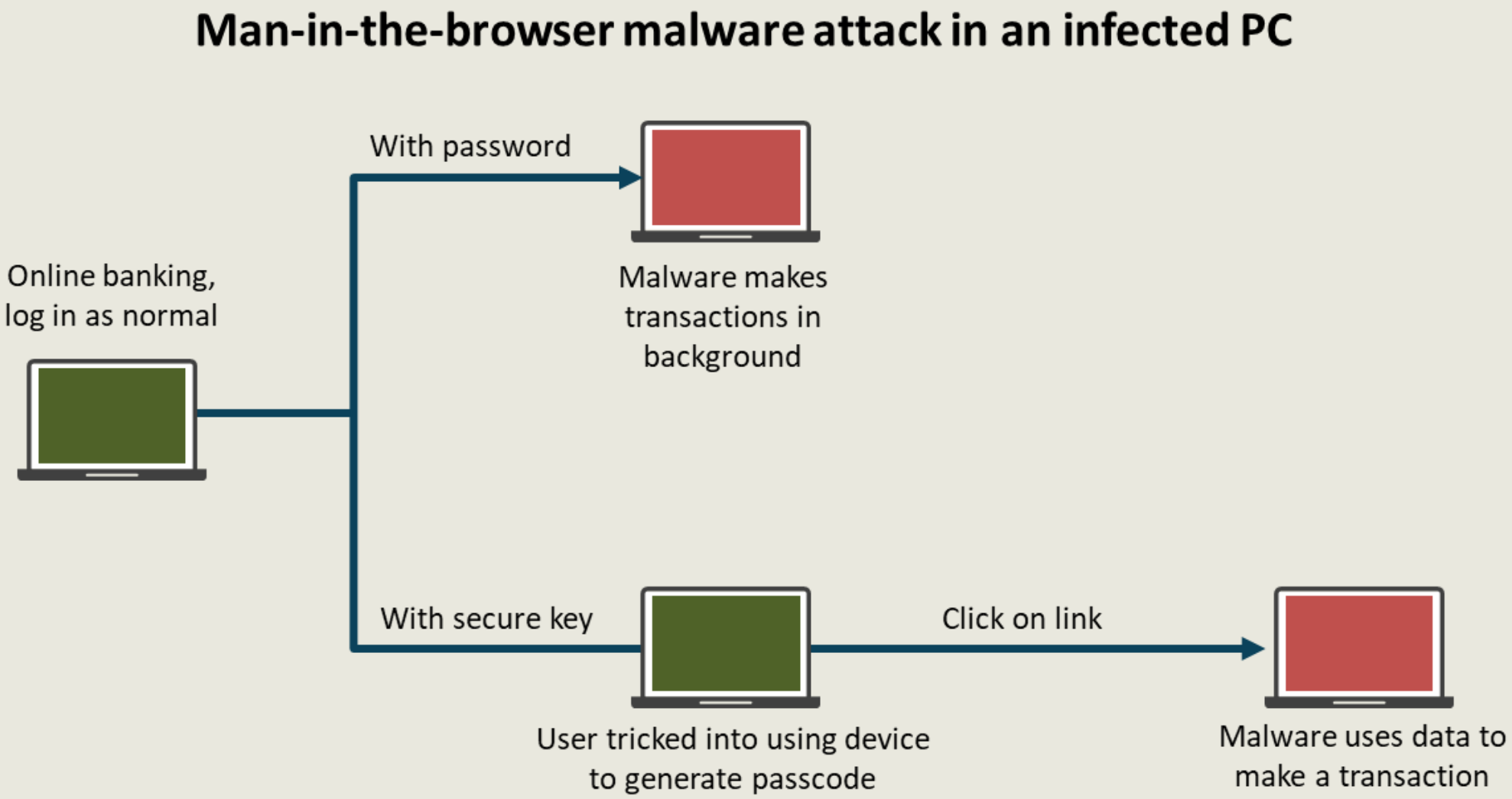
- Refactoring involves changing an application's source code without modifying the characteristics
- Often used to introduce legacy applications into new computer systems and devices
- Can also re-engineer classic attack code to create variants, hybrid viruses, and worms

Man-in-the-Browser Attack

A variant of the MITM attack

- Man-in-the-browser attack uses the same tactics as MITM except that a Trojan horse is used to capture and manipulate calls between the main browser and its security mechanisms (or libraries) on an ad-hoc basis
- The most common usage is financial fraud, which manipulates transactions of Internet banking and brokerage sites
- Works even when other authentication factors are being used

Man-in-the-Browser



Evil Twins

- Malicious rogue APs, used to take sensitive data like usernames, passwords, and PII, fall into two categories - honeypots and evil twins
- An evil twin AP replaces an existing network so users will connect to the fake one instead of the real one
- Evil twin is described as a wireless man-in-the-middle attack
- Evil twin is similar to a honeypot, except that the attacker attempts to appear as the valid network
- Evil twins spoofing a public hotspot can also be a serious concern

Disassociation Attacks

- Stations use control and management frames
- AP impersonation is common
- DoS attacks against infrastructure
- Use Management Frame Protection (MPP)
- Use WPA3 which mandates MPP

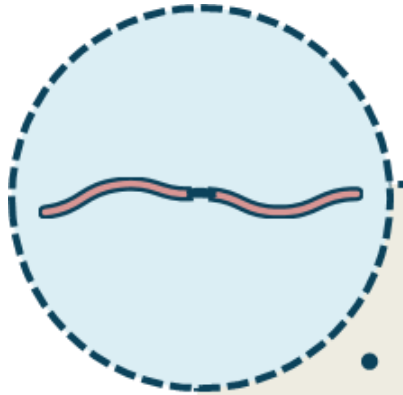
Man-in-the-Middle Attacks

- Honeypot AP "induces" users to connect to it
- AP is usually unsecured and allows any user to connect so that the data that users send through the AP is captured
- Connection can be used to infect the connecting client with various malware variants
- Example: an ad hoc network called "Free Wi-Fi"

Jamming Attacks

- A form of wireless DoS attack is jamming
- Jamming floods the RF with interference or excessive traffic so that wireless links cannot be sustained
- Exploit kits have several jamming modules and scripts included for hard and soft APs
- Some DoS attacks may not be due to malicious activity, but rather poorly written drivers on endpoint wireless NICs

Weak Initialization Vector (IV)



- WEP has been deprecated due to the following reasons
  - Hackers can easily obtain challenge phrase and encrypted response to crack the WEP key
  - Crackers have decrypted captured data traffic
  - Provides only weak encryption of data
  - The initialization vector is a clear-text 24-bit field - a pseudo-random number used along with the secret key for data encryption

WPA3 Dragonblood Attack

- One of the main advantages of WPA3 is that the Dragonfly handshake makes it near impossible to crack the network password
- However, the Dragonblood attack gives someone within range the ability to recover a password
- CVE-2019-13377: timing-based side-channel attack against WPA3's Dragonfly handshake when using Brainpool curves

Bluejacking

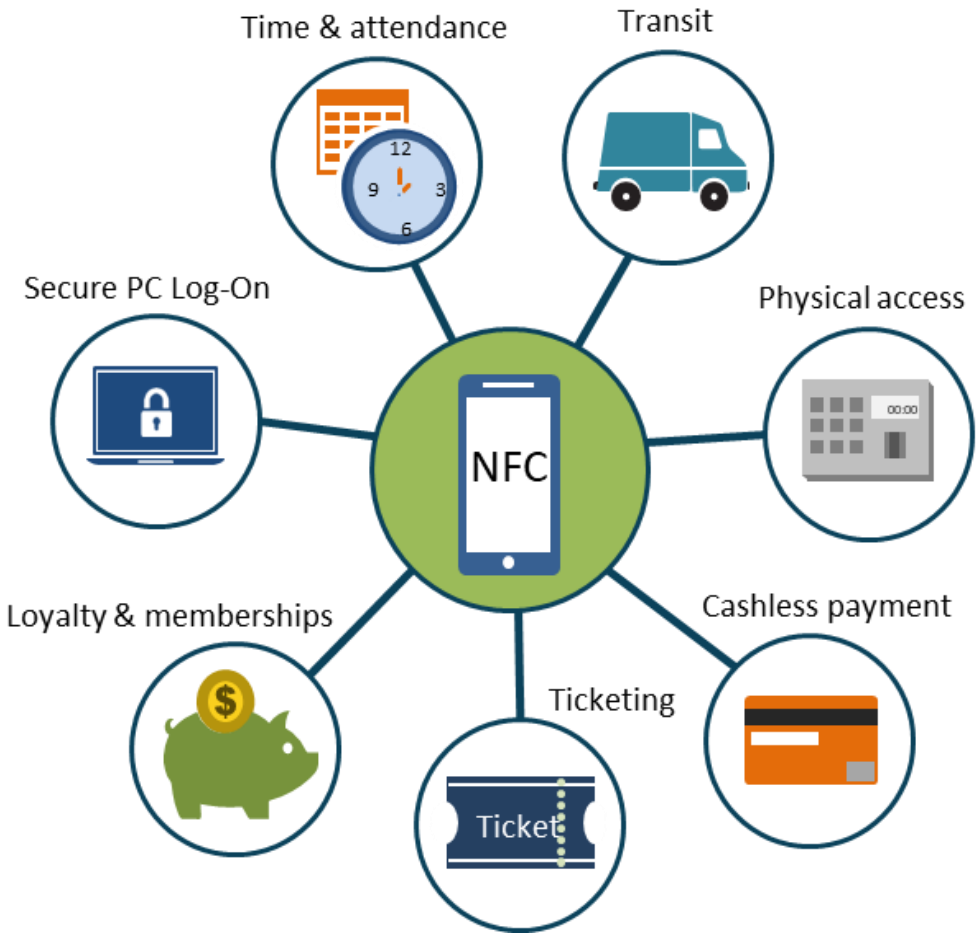
- Bluejacking is really an old Bluetooth prank that takes advantage of sending contact information automatically without authentication or authorization
- The cracker creates an address book object and a contact in the contact list
- They spoof a name to appear on your phone saying they have sent you some contact information and would like you to accept it
- Then, a message says something annoying like "You are bluejacked and I'm taking over your phone"
- Information and data is not being stolen - more of an annoyance

Bluesnarfing

- Bluesnarfing is much more dangerous than bluejacking
- Bluesnarfing steals data from a wireless device using a Bluetooth connection
- Often between iPhones, Android phones, iPods, iPads, laptops, and assorted PDAs
- Can access contact lists, calendars, e-mails, and text messages
- Any device with Bluetooth enabled and set to "discoverable" is vulnerable to attack
  - Turning off this feature is one simple countermeasure to bluesnarfing
- It is illegal in many countries due to privacy laws

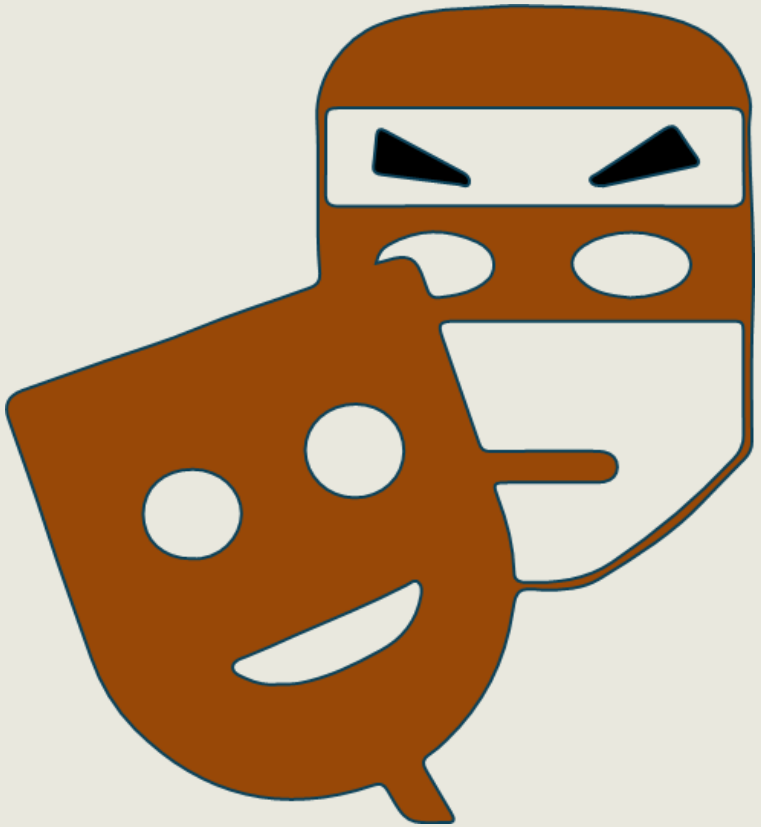
RFID and Near Field Communication (NFC)

- The benefits of rapid and contactless payments and entry/exit without long waiting times are very tempting
- The benefits of RFID/NFC for travelers and shoppers are numerous, and the tech is here to stay
- However, data stored on RFID chips can be stolen, skimmed, and scanned by anyone with easily obtained RFID readers
- Common attacks include
  - sniffing, spoofing, and MITM replay
  - Cloning and emulation
  - Jamming and blocking (DoS)



Threat Actors and Agents

A realized “threat” needs an agent



- Threat agents (or actors) 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
- Threats are not realized without an agent or catalyst
- Can be an individual or group
- The attacks can also be totally automated

Actors and Threats

- Human errors
- Hostile cyber attacks
- Data breaches and theft
- Cognitive threats via social networking
- Exploiting consumer electronics
- Interference with critical infrastructure (SCADA, PLCs)
- Natural disasters and structural failures

Attributes of Actors

Internal or external and structured or unstructured

Intent and motivation

Sophistication levels or skillsets

Threat event frequency

Resources and funding

Structured vs. Unstructured

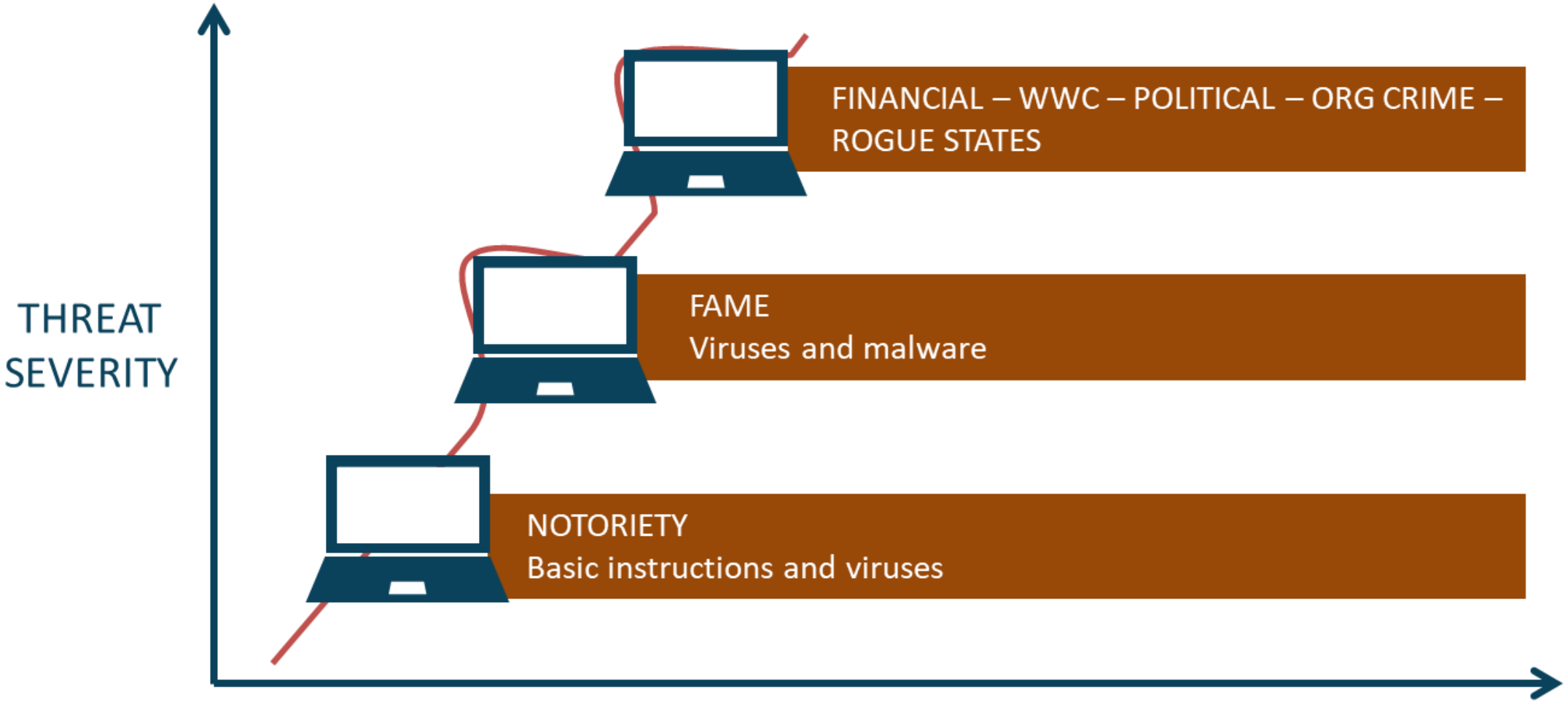
Structured

- Planned
- Organized
- Persistent
- Multi-phased
- Can be internal or external
- Exploit kits, zero-days, modules, ransomware

Unstructured

- Accidental
- Non-malicious
- Drive-by web surfing
- No AUP
- Poor awareness
- E-mail and webmail
- USBs and personal electronics

Intent and Motivation



Common Threat Vectors

- Direct physical access (removable media)
- Local network access
- Remote access (VPN or no VPN)
- Wireless, satellite, and cellular
- E-mail, webmail, or messaging
- Supply chain
- Social media
- Personal or public cloud computing

Script Kiddies

Little or no skills

- Originate from the combination of inexperienced crackers using script viruses and prepackaged malicious code (exploit kits and Malware-as-a-Service campaign)
- 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 in the dark web through ToR browsing

Crackers and Attacker Syndicates

White hat hackers have extensive knowledge of the target system and application

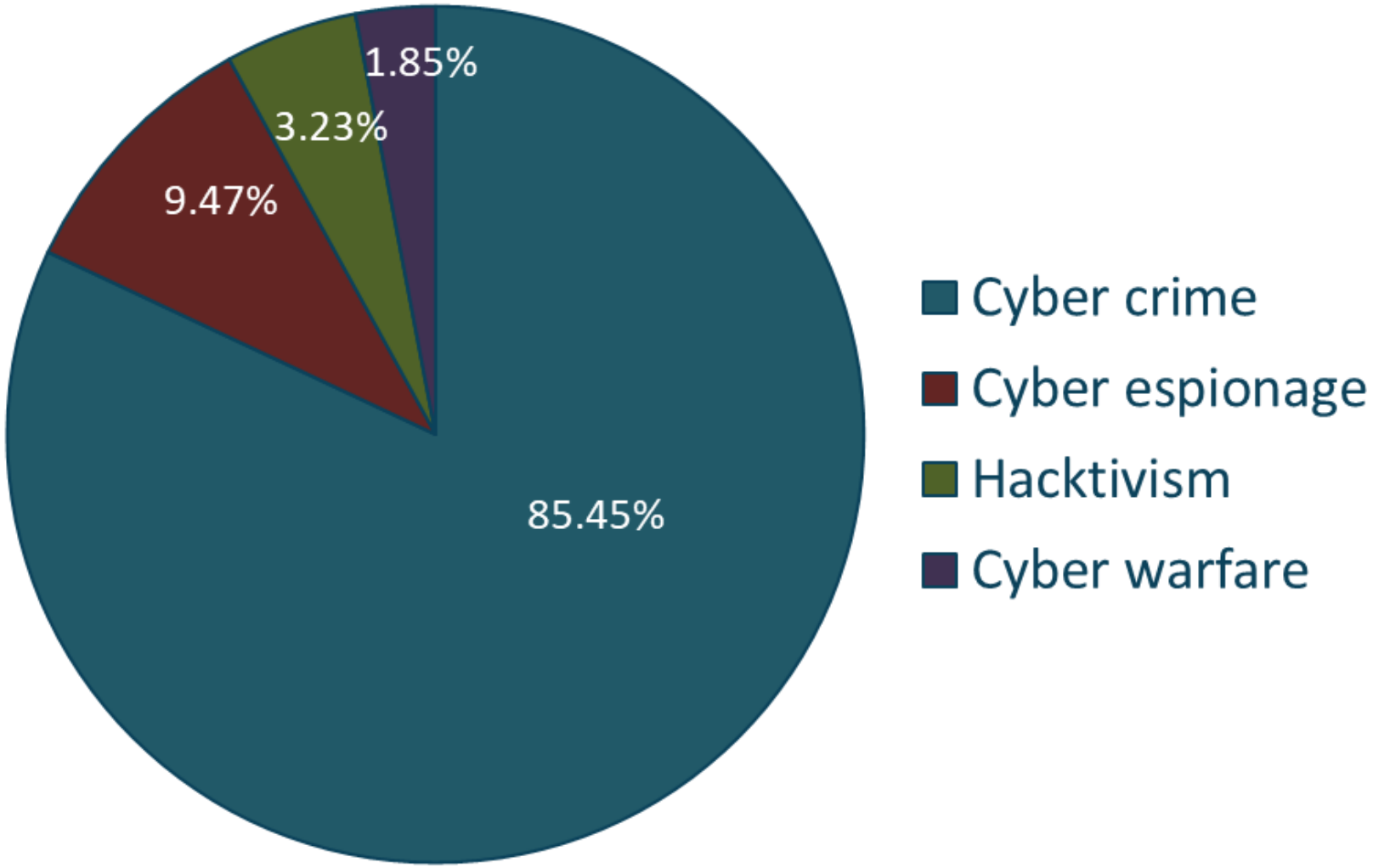
Gray hat attackers have some level of information about the target but need more

Black hat crackers have very little or no knowledge of the victim and are most often external

Insider Threats

- Look for disgruntled or desperate employees' elevated privileges
- Possible blackstortion or intimidation
- Always consider ex-employees after a breach
- APTs can involve employee with fake ID or someone using "Shadow IT"
- Background checks and ongoing audits are critical as mitigation techniques

State Actors

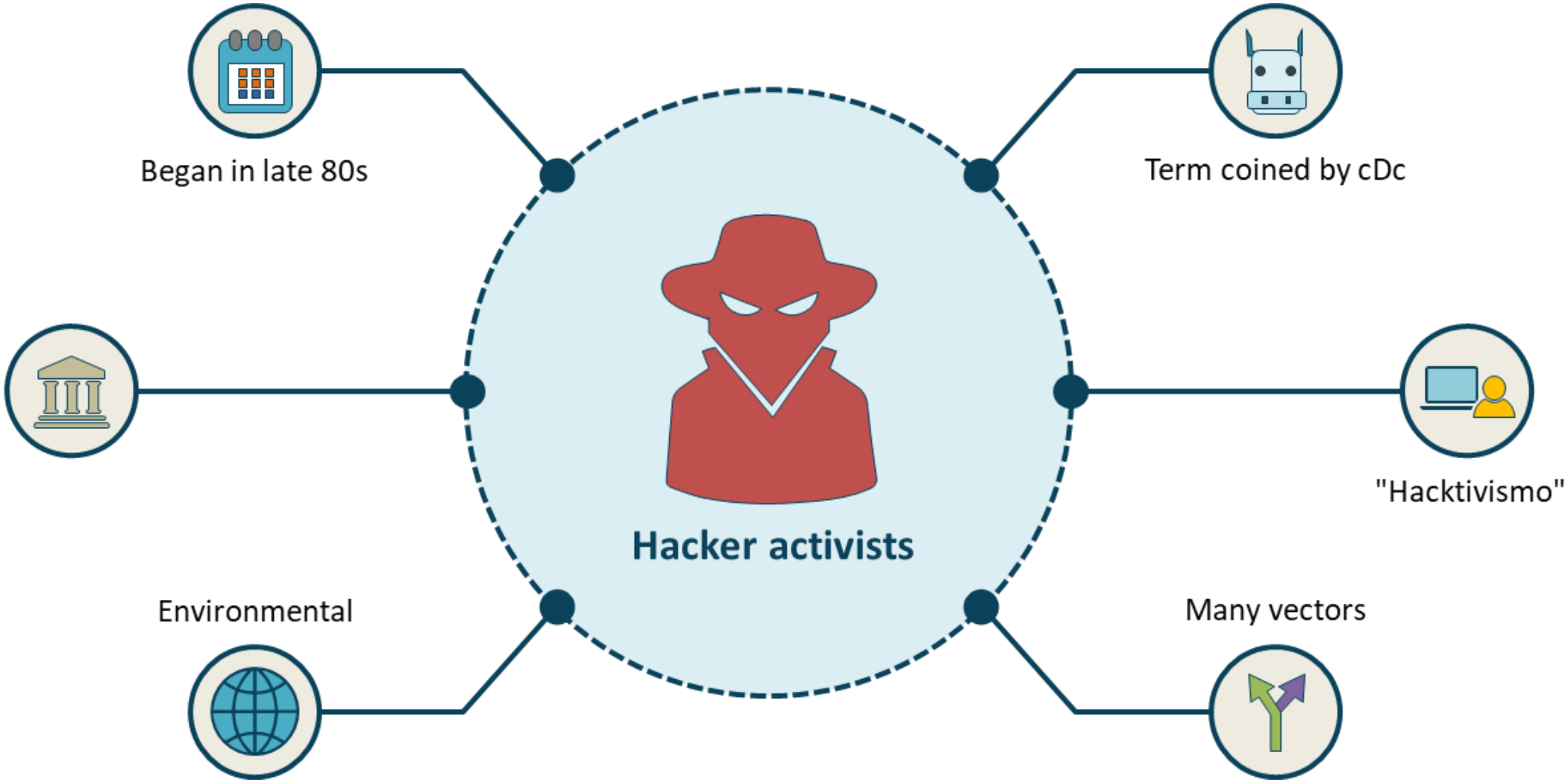


Passeri, Paolo. “Q1 2020 Cyber Attacks Statistics.” HACKMAGEDDON, April 14, 2020. https://www.hackmageddon.com/2020/04/14/q1-2020-cyber-attacks-statistics/.

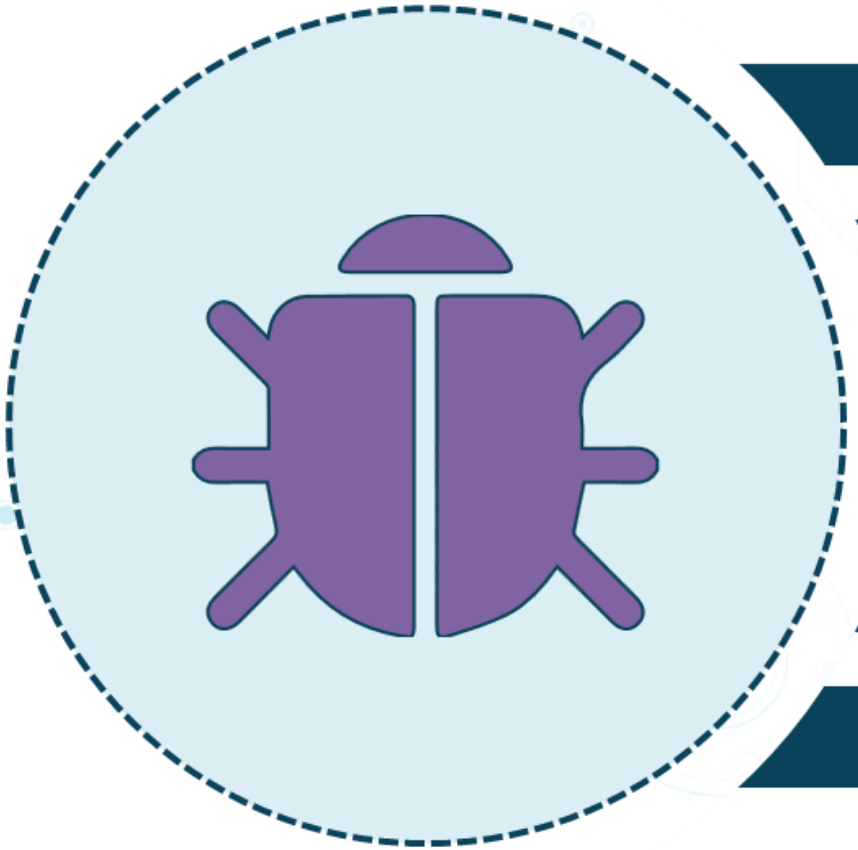
State Actors

- World War C involves many of the same activities as criminal syndicates
- Cyber warfare, espionage, and blackmail
- 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

Hacktivists



Dark Web



- Also called overlay networks or darknets
- Need special software, configs, or authorization
- Deep web not indexed by search engines
- Peer-to-peer networking
- Tor, Freenet, I2P, and Riffle

Dark Web

- Botnets
- Bitcoin services
- Darknet marketplaces like Silk Road
- Hacking groups and MaaS
- Fraud and hoaxing services
- Financing
- Phishing, ransomware, and scam campaigns
- Puzzles and games
- Illegal pornography
- Niche social media
- Terrorism

Advanced Persistent Threats (APTs)

Usually long-term planned malware campaigns

Pre-planned with cost-benefit analysis

Persistent in activity and system state existence

Very often from nation state actors

Sophisticated multi-phased polymorphic attacks

Zero-day Attacks

- "Zero-day" is a term describing a recently discovered exploit or malware for a vulnerability that attackers launch against systems
- "Zero" refers to the number of days since the anti-malware vendor or organization discovered the threat
- Exploits can go unnoticed for years and are often sold on the black market for large sums of money
- Although there are millions of lines of zero-day code waiting to be logic bombed, the Common Vulnerabilities and Exposures (CVE) is a valuable list of recently discovered security vulnerabilities

Indicators of Compromise (IoCs)

These are network or host-based cyber observables

Forensic artifacts of an incursion or disturbance

A measurable event or stateful property in the cyber domain

Registry entries, files on disk and in-memory, etc.

Cloud vs. On-premise Vulnerability

Public cloud

- Threat actors are external in the majority of attacks
- Access keys must be protected
- Many accounts to reduce attack and blast surface
- Managed security service providers (MSSP) and Cloud Access Service Brokers (CASB)

On-premise

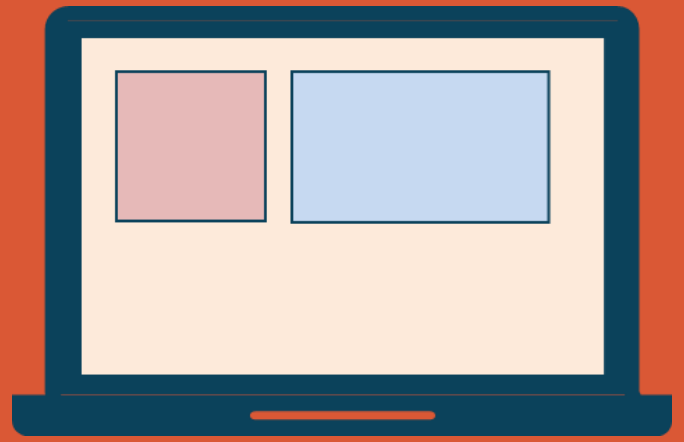
- Biggest threat is privileged insiders
  - C-suite or C-team
  - Database engineers and architects
  - Highly privileged security personnel
  - HR and legal departments
  - Disgruntled present and ex-employees

Weak Configurations

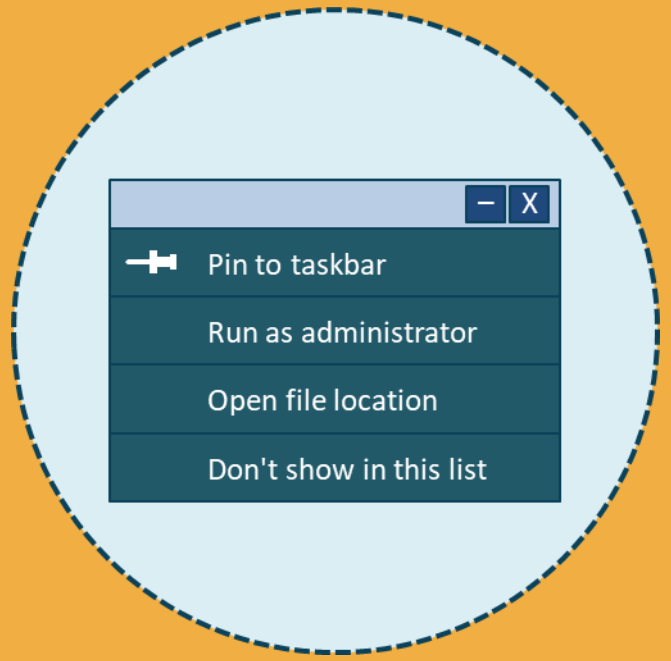
- Open permissions, ports, and services
- Errors sent to logs and SIEM systems
- Weak encryption
- Unsecure protocols
- Default settings and passwords

Weak Configurations

- Human error is the number one vulnerability
- Deploy change, configuration, and patch management systems (automated)
- Peer reviews and dual operator are beneficial
- Test configurations in virtual lab or the private cloud before deployment
- Do not be the first customer to use a new product or upgrade
- Store config files in secure document library such as GitHub or SharePoint with strong access controls



Improperly Configured Accounts

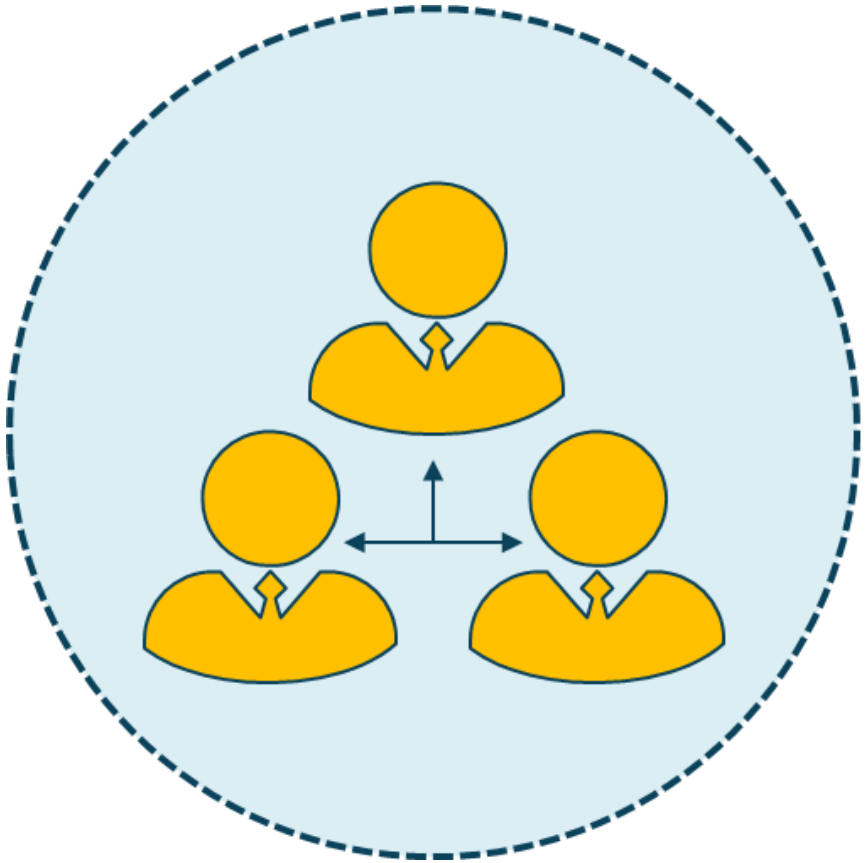


- Biggest issue is overprivileged users
- Logging, auditing, and reporting
- Least privilege principle should be used
- Use separate account for admin tasks (Run as…)
- Proper permission policies
- Use centralized secure systems and directory services
- Vulnerable to privileged insiders

Improperly Configured Accounts

- Local administrative accounts
- Privileged user accounts
- Forest/domain administrators
- Emergency accounts
- Service accounts
- Application accounts
- Shared accounts
- Cloud Service Provider accounts

Third Party Risks



- Vendor management
- System integration
- Lack of vendor support
- Supply chain
- Outsourced code development
- Data storage

Improper Patch Management

One of the top enterprise risks

- Many organizations do not consider or continually improve their patch management plan
- Vulnerability/exposure reviews and gap analysis are not performed or done properly
- A configuration management database (CMDB) of all configuration items (CIs) should be maintained
- Only certain personnel should have the authority to test, apply, and determine the urgency of patching activities
- Agreements with any applicable vendors should also be made to address any potential issues before patch deployment

Impact of using Legacy Systems (IoT, embedded)

- Data loss, breach, and exfiltration
- Identity theft
- Financial loss
- Loss of reputation and goodwill
- Availability loss

Cryptology

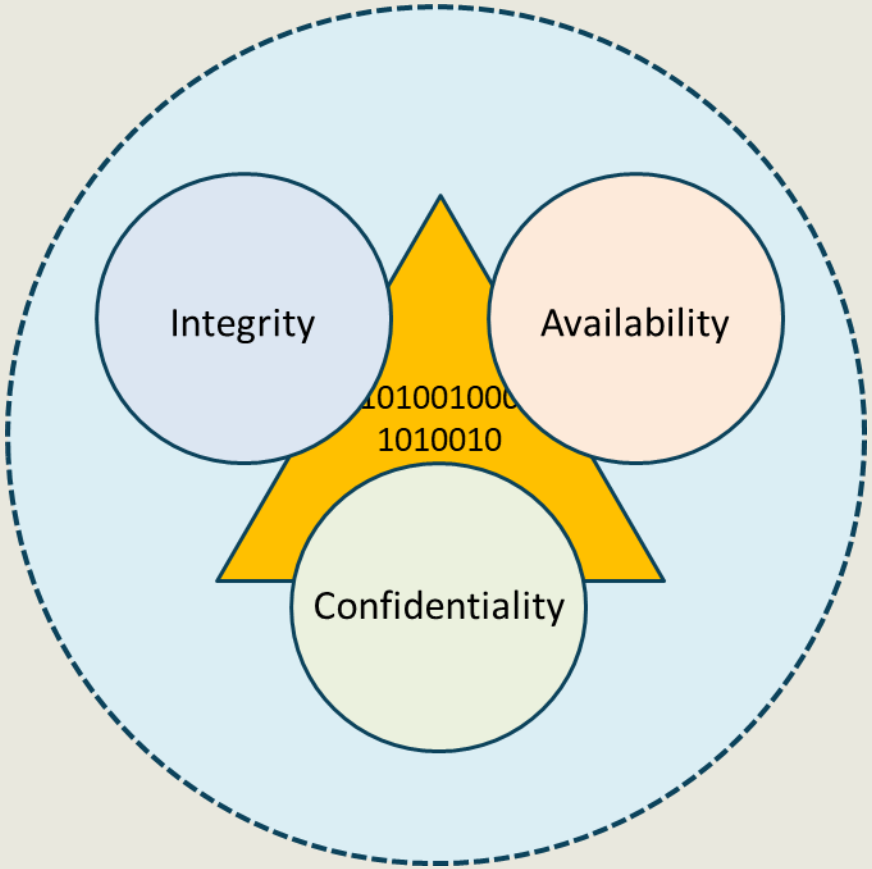
Cryptography

- The study and practice of securing communications
- Encryption, hashing, and signing are most common applications
- Involves creating cryptosystems and testing new variants and modes

Cryptanalysis

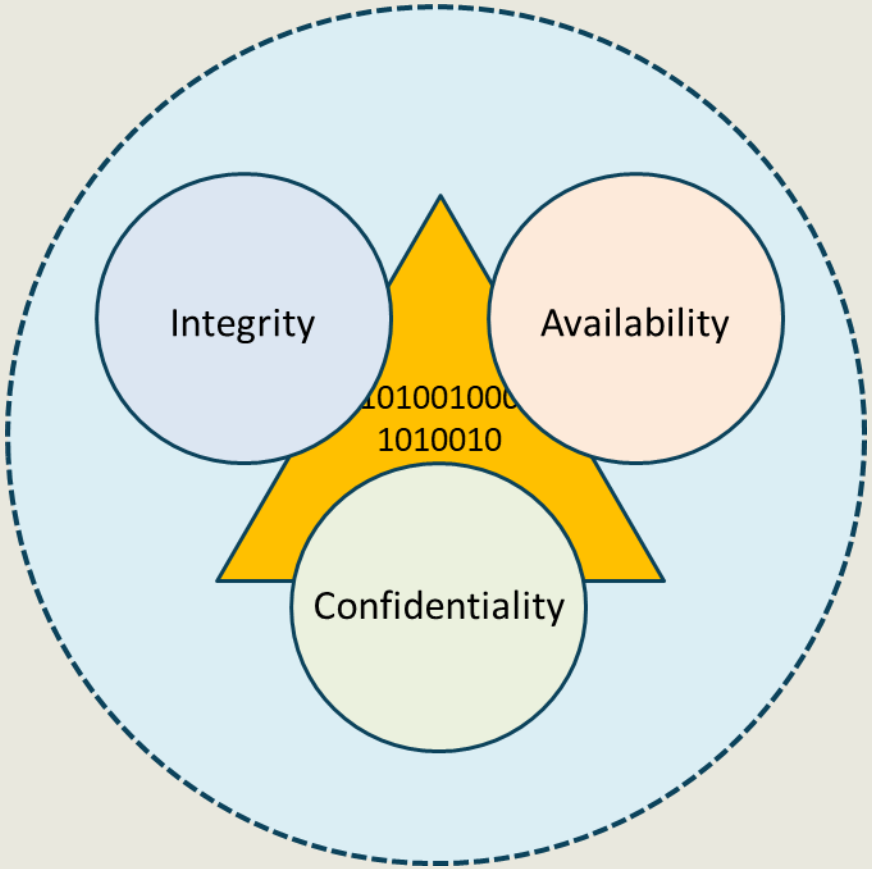
- The study and practice of exploiting weaknesses in communications
- Analysts actively explore
  - Brute force attacks
  - Implementation attacks
  - Side-channel attacks

Cryptographic Services



- **Confidentiality**
  - Hiding the data at rest, in transit, and in use from unauthorized entities
  - Often involves a system that converts plaintext data into ciphertext
- **Integrity**
  - Ensures the data has not been altered while at rest or in transit
  - Often involves attaching a cryptographic hash digest to the data

Cryptographic Services

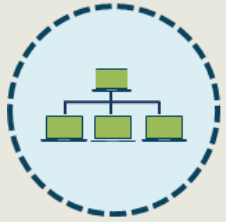


- **Availability**
  - Protecting systems from flooding and denial-of-service techniques
  - Controls that provide redundancy, failover, and backups
- **Non-repudiation**
  - Ensures original sender cannot deny sending data or engaging in a digital transaction
  - Common to use digital signatures

Encryption Occurs at Several Layers

Application layer - example: PGP

Session layer - example: SSL/TLS

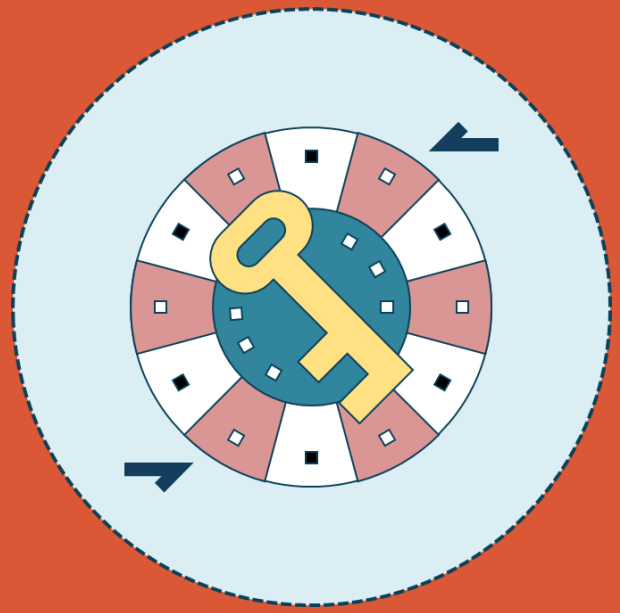


Network layer - example: IPsec

Data link layer - example: MACsec

Ciphers

- A cipher is an algorithm used for encryption and decryption
- It outlines the procedures that are followed and establishes a well-defined series of steps
- The result is often called "ciphertext"
- There are many different types of ciphers - from simple substitution to complex multi-layered modes
- Modern ciphers often involve a combination of transposition, diffusion, and confusion techniques



Symmetric Key Cryptosystems

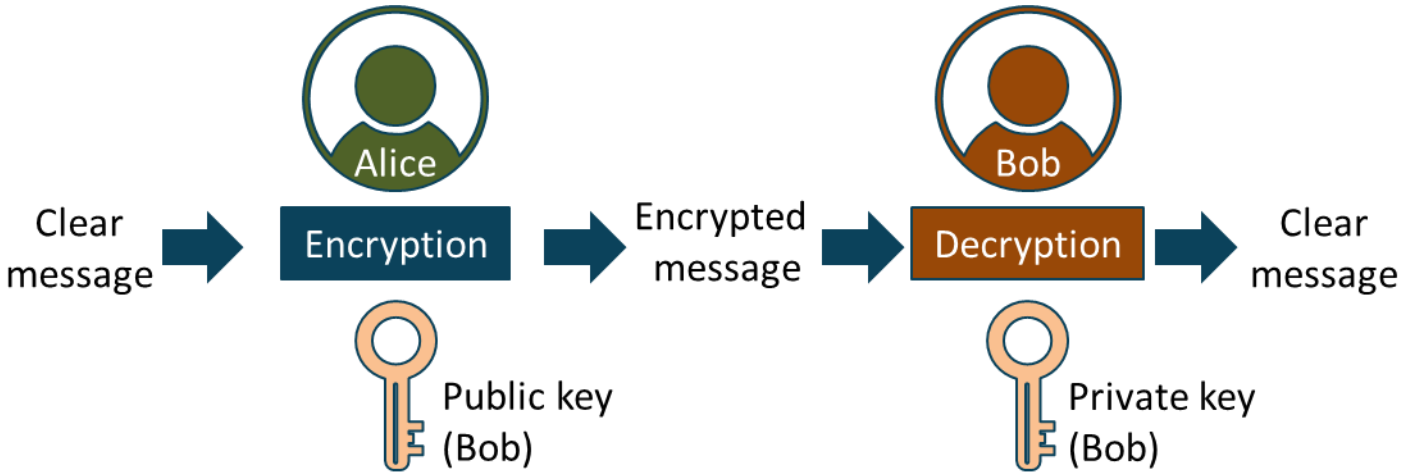
- Uses the same key to encrypt and decrypt
- Efficient, fast, and handles high data rates of throughput
- Computationally inexpensive
- Has shorter key lengths (40 to 512 bits)
- Key management is more complex
- More difficult to secure than other systems
- No origin authentication
- Does not scale well

Asymmetric Key Cryptosystems

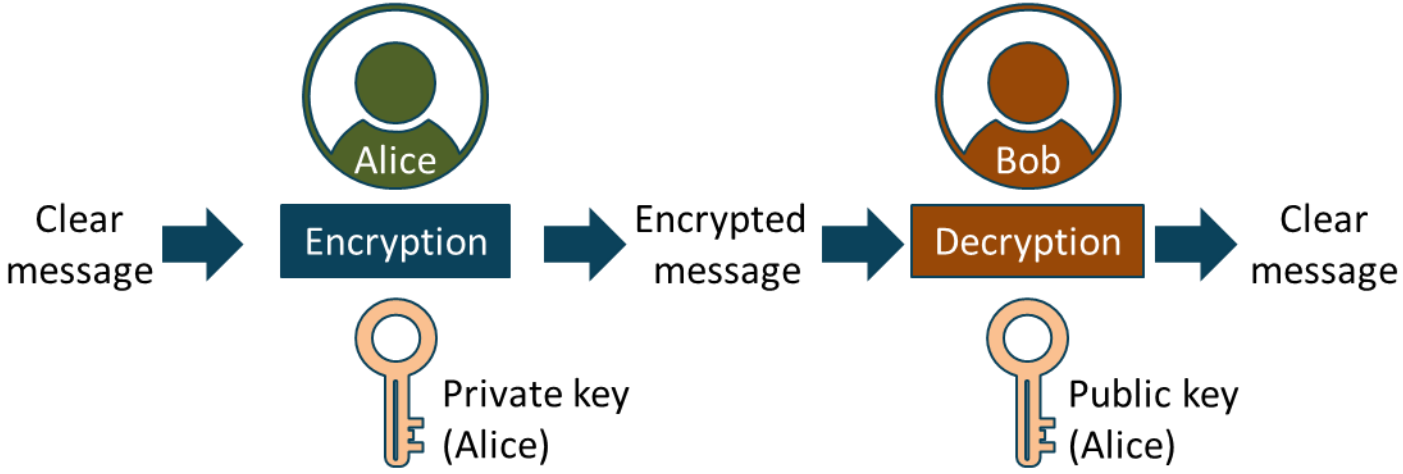
- Uses a mathematically related pair of a public and private key
- If one is used to encrypt - the other is used to decrypt
- Allows for efficient key management
- Great for digital signatures and key exchange
- Highly scalable with a public key infrastructure
- Employs longer key lengths than symmetric
- Slower and more computationally expensive

Asymmetric Key Cryptosystems

- Confidentiality
  - Encrypt with public key
  - Decrypt with private key

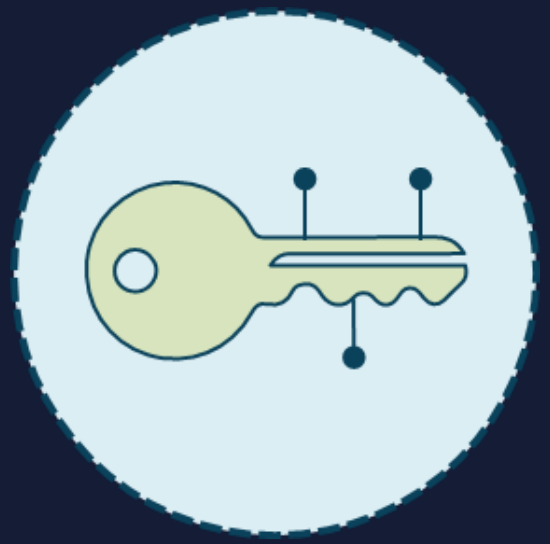


- Origin authentication
  - Encrypt with private key
  - Decrypt with public key



Cryptographic Keys

Sets of alpha-numeric characters used for converting plaintext to cipher text

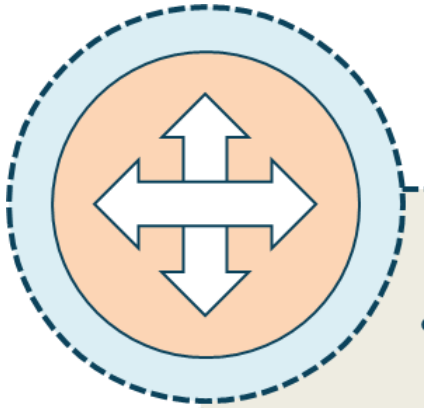


- The only element that must remain secret in a sound cryptosystem is the key as the ciphers, algorithms, and protocols are open source
- The keyspace represents the total number of mathematical possibilities in the set
- Key lengths often vary from 56 to 4096 bits
- Keys enable cryptographic encryption, digital signatures, hash functions, and message authentication codes

Types of Cryptographic Keys

- Static keys
  - Used for a long period of time
  - Used multiple times for key establishment processes
- Session keys
  - A single-use symmetric key used for an entire session
  - Encrypts and decrypts all messages per session
  - Limits the amount of information encrypted with key
  - Makes many cryptanalytic attacks more difficult
- Ephemeral keys
  - Used for a very short time period
  - Used for only one single key establishment processes
  - Never stored in memory or retained

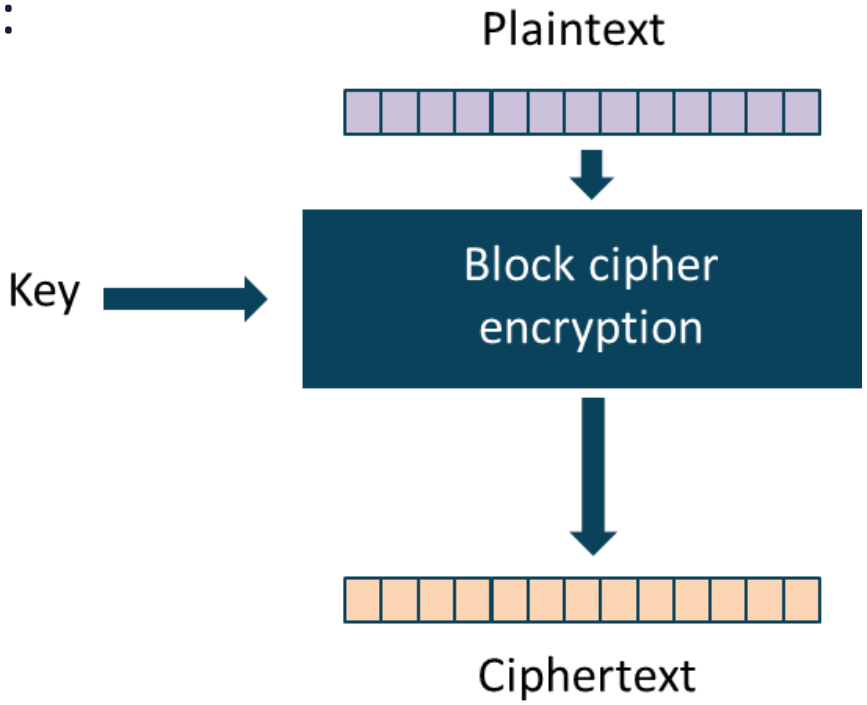
Key Stretching



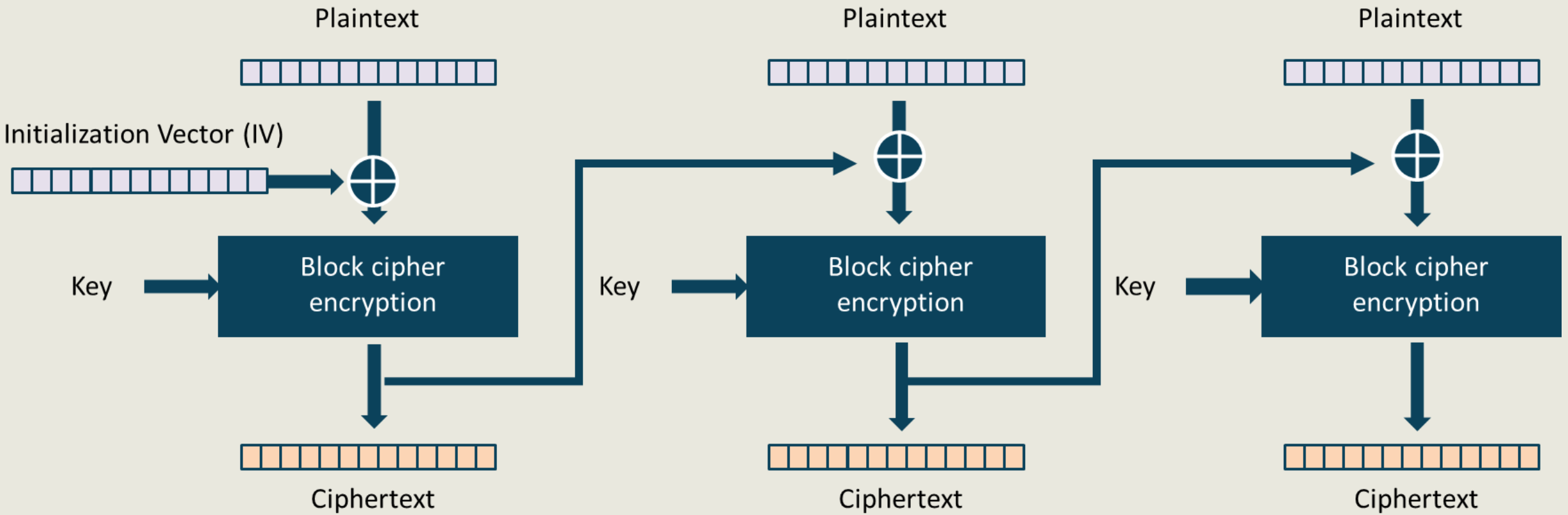
- PBKDF2 and BCRYPT are programs that use pseudorandom functions (password + salt) applied many times to produce longer and stronger cryptographic key for other uses
- Example
  - Password = thisismypassword
  - Salt = ACB3F274509886057D924912E201EED0 (at least 64-bits)
  - Iterations = 1000
  - Key length = 128
- Result
  - xvgFAWdnw035eJxsldD9xrLIhuxpGM1SIiqSZStt4ClTqHk3dluVB5r44yc1ICrfrqsG kvCVmdVF7kuk/e16FCnZsajE6ErwSB3mkx6tZOX0LELU9wutBHxGJKiXGyrTQp99 lAY8ghhIt4ciu71OJvjKTbT8nSskJyZ3pzZI5UM=

Block Ciphers

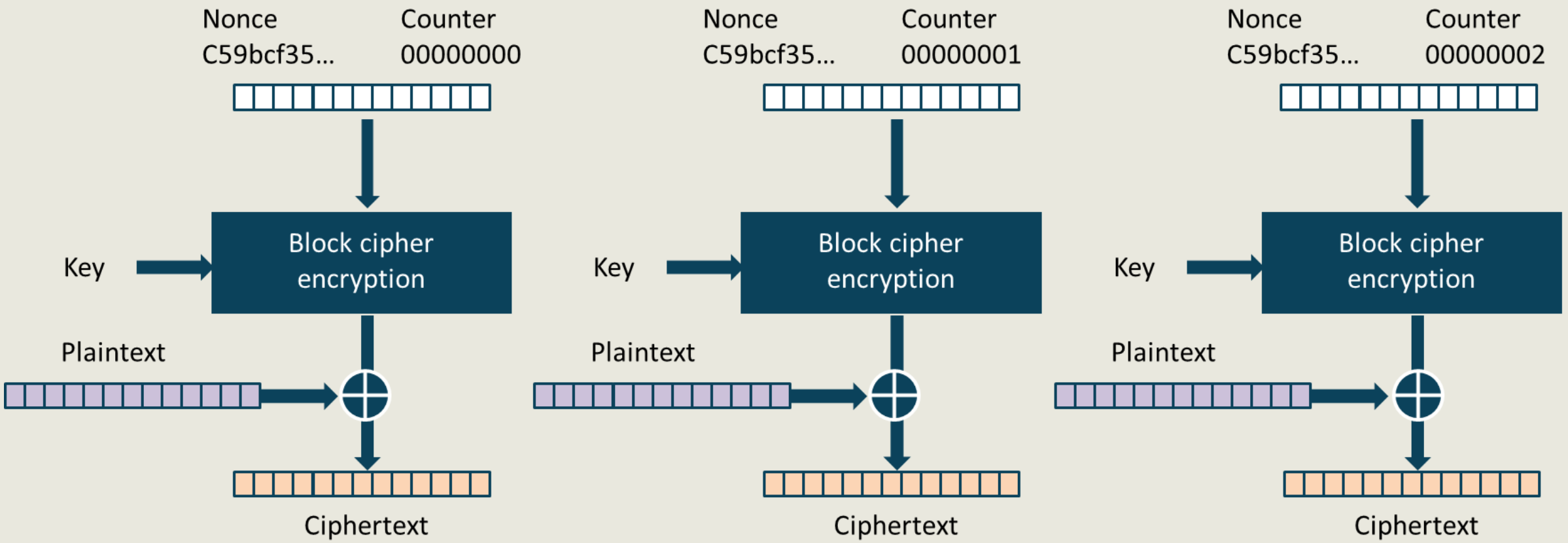
- Operates on fixed blocks of data (bits) based on key size
- 64, 128, and 256-bit keyspaces are common
- Messages bigger than the key size are broken into blocks the size of the key and must include padding
- Common block ciphers:
  - DES
  - 3DES-EDE
  - AES-CBC
  - AES-GCM
  - Blowfish
  - Block



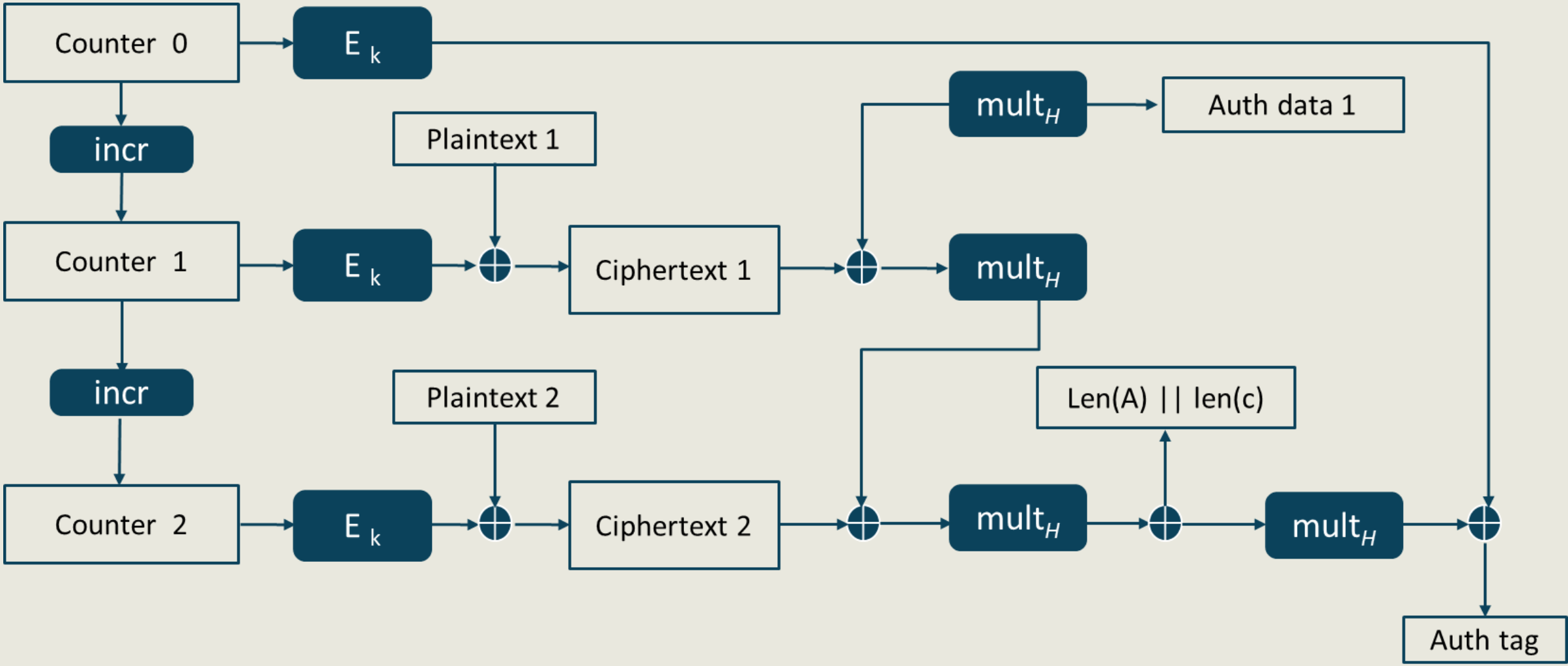
Cipher Block Chaining (CBC)



Counter Mode (CTM)



Galois Counter Mode (GCM) - AEAD



AES is Ubiquitous

- Advanced Encryption Standard (AES) is the replacement for DES using the Rijndael algorithm
- 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
- Most often used with IPsec, SSL/TLS, and CSP data encryption (KMS)

Stream Ciphers

- Operate on a continuous stream of plaintext data by encrypting one bit or byte at a time
- Plaintext bits are typically XORed with keystream bits
- Keystream = random bits, bytes, numbers, characters
- Faster and less complex than block ciphers
- Modern ciphers can work in block or stream mode or both
- Examples of stream ciphers include:
  - FISH
  - CryptMT
  - Scream
  - RC4
  - Cryptographic hashing

Simple Stream Cipher Example

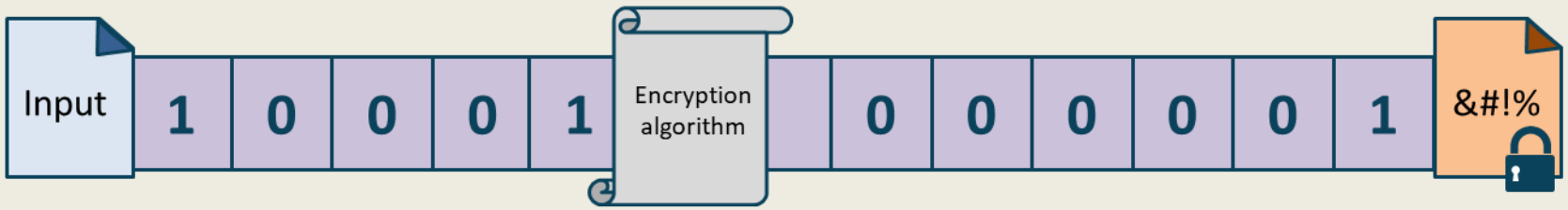
- Alice wants to use a stream cipher to encrypt the letter "A"
- In ASCII, the letter "A" has the value of 65 = 1000001
- The first cipher stream bits are 0101100
- We perform an XOR function (Modulo 2 addition)

  1000001 = A

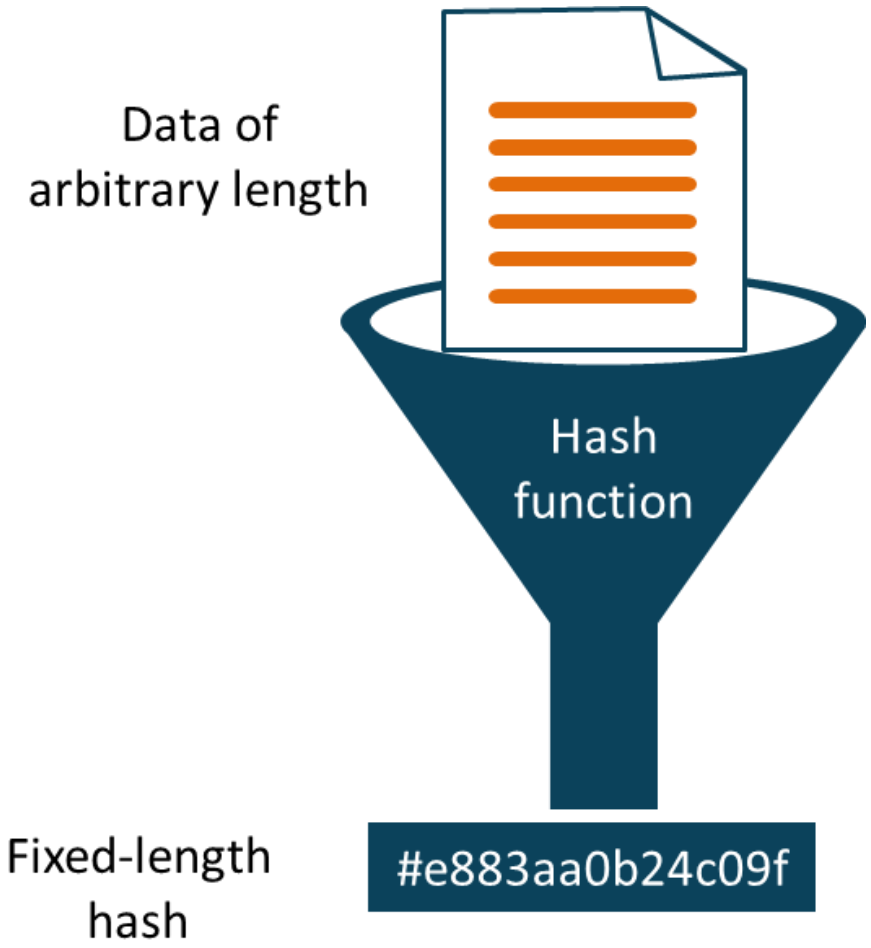
  XOR

  0101100

  1101101 is the result
- The letter "A" becomes ciphertext "m" (ASCII value 109)



Cryptographic Hashing



- Converts data of any input size to a fixed-length string called a hash value, message digest, or fingerprint
- An advanced version of a simple checksum
- A one-way mathematical function that produces a digest of 128 to 512 bit
- Birthday paradox and avalanche effect
- Used in authentication, data integrity, non-repudiation, fingerprinting, and password storage
- Password + salt + hash function = hashed password

Cryptographic Hash Functions

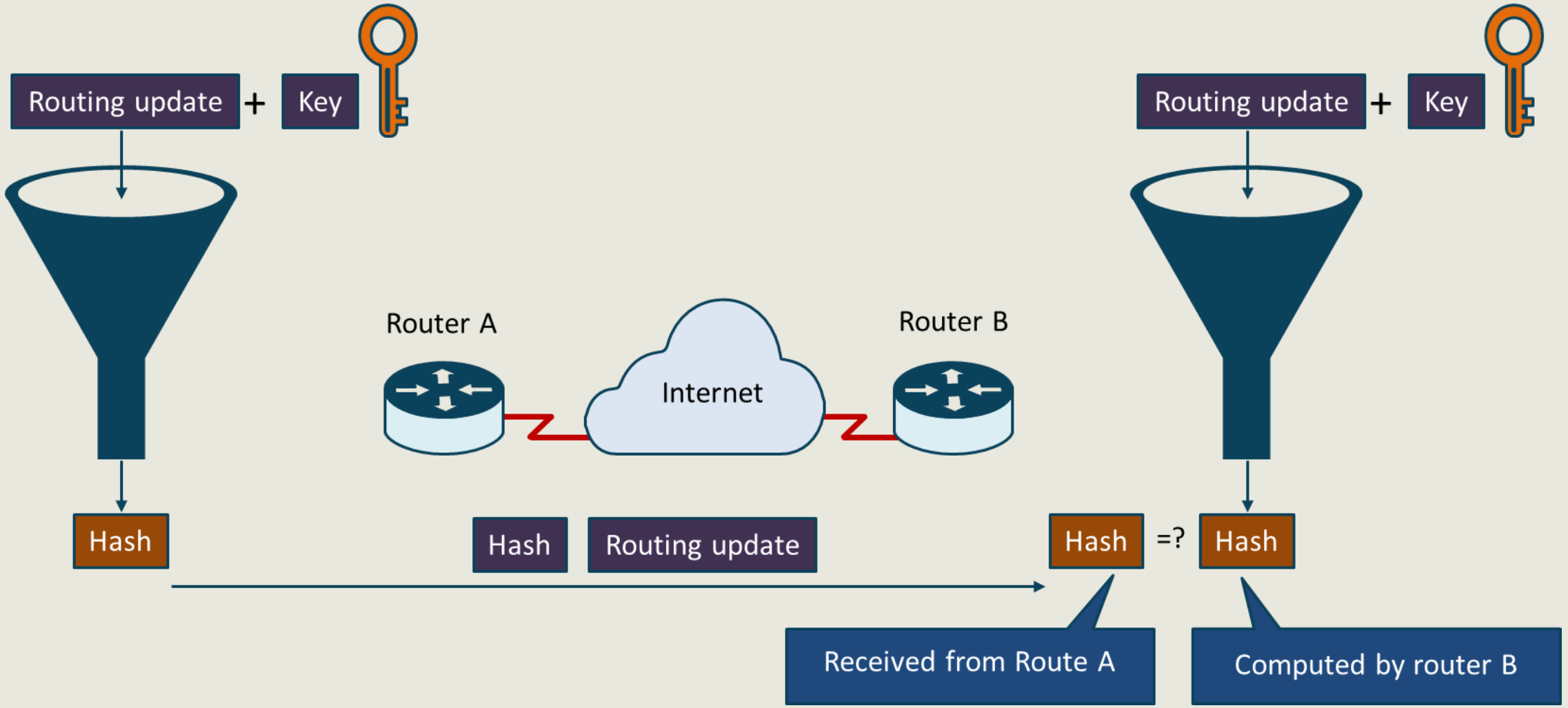
MD5 (128-bit digest is produced)

SHA-1 (160-bit digest is produced)

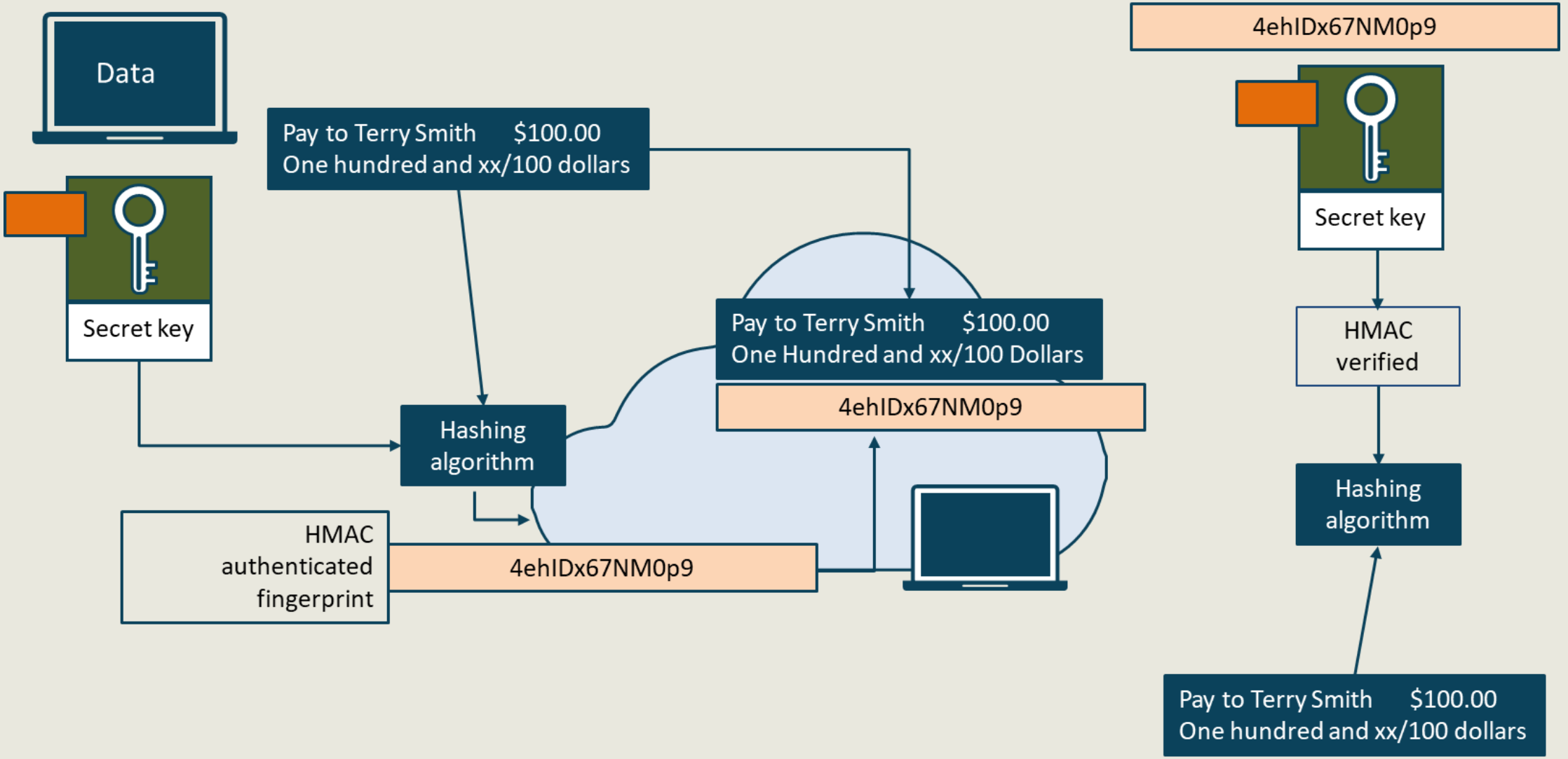
SHA-2 (SHA-256 or SHA-512) and SHA-3 (224 - 512)

RIPEMD (128, 160, 256, 320-bit versions)

HMAC for Origin Authentication and Integrity

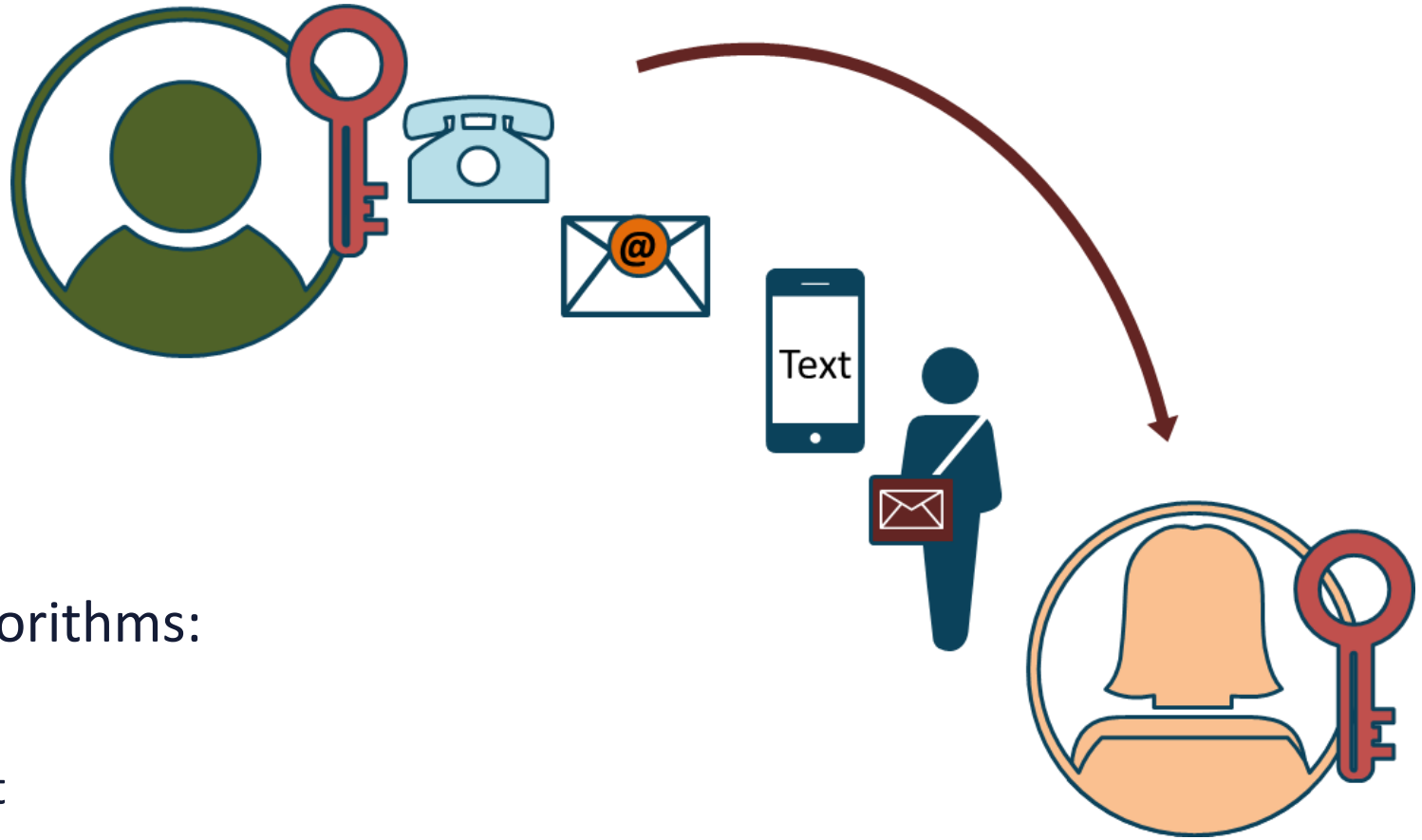


HMAC for Origin Authentication and Integrity



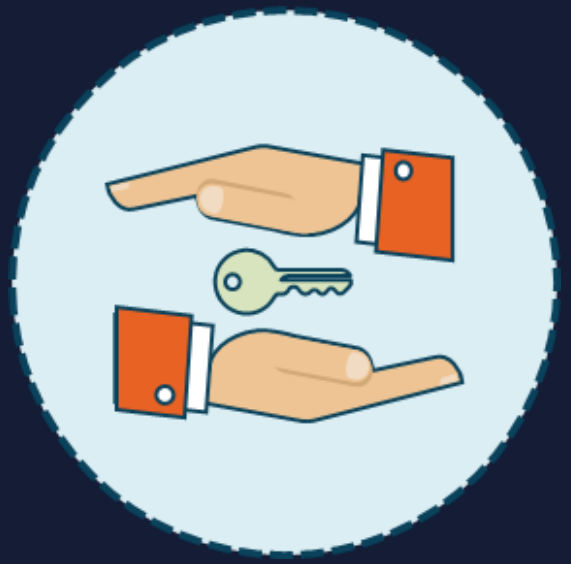
Key Exchange

- Phone
- Email or secured email
- Text
- Couriers
- Diplomatic bags
- Asymmetric key exchange algorithms:
  - RSA - key exchange
  - Diffie-Hellman - key agreement
  - Elliptic Curve Diffie-Hellman



Diffie-Hellman

- Diffie-Hellman Key Exchange (DHKE) and RSA key transport are original protocols created for establishing secret keys between two parties over an unsecure channel
- Diffie-Helman is a widely used asymmetric cryptosystem found in SSH2, TLS, and IPsec
- It represents an impressive application of the discrete logarithm problem

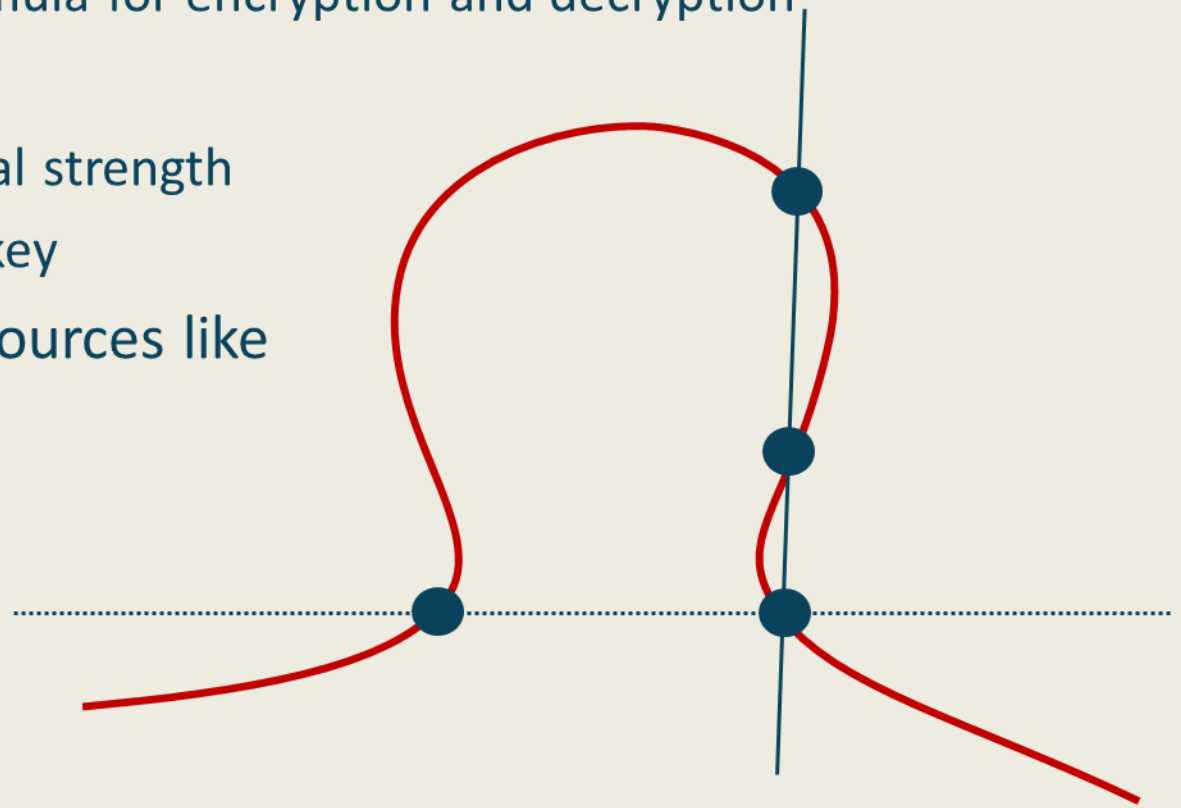


Diffie-Hellman Modes

- 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 (Elliptic-Curve Ephemeral Diffie-Hellman)
  - Uses EC public/private key pair
  - Different shared secret used each time

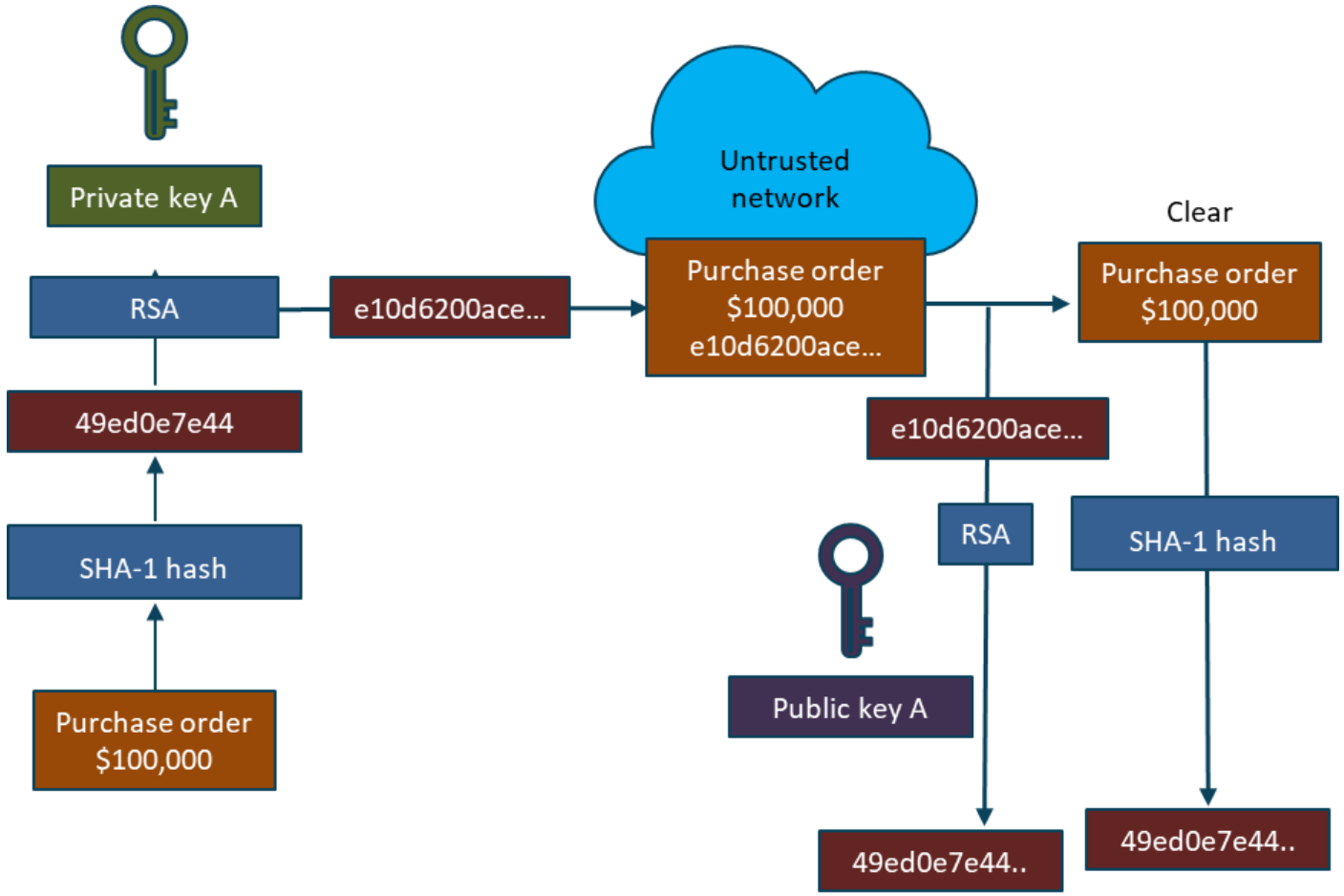
Elliptic-Curve Diffie-Hellman

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



Digital Signatures

- Scalable mechanism for providing authenticity, integrity, and non-repudiation
- Does not offer confidentiality
- Equivalent to a handwritten signature in many countries
- Random private/public key pair
- SHA1/2/3 hash algorithm
- Signing algorithms
  - RSA (Rivest, Shamir, Adelman)
  - DSA (digital signature algorithm)
  - ECDSA



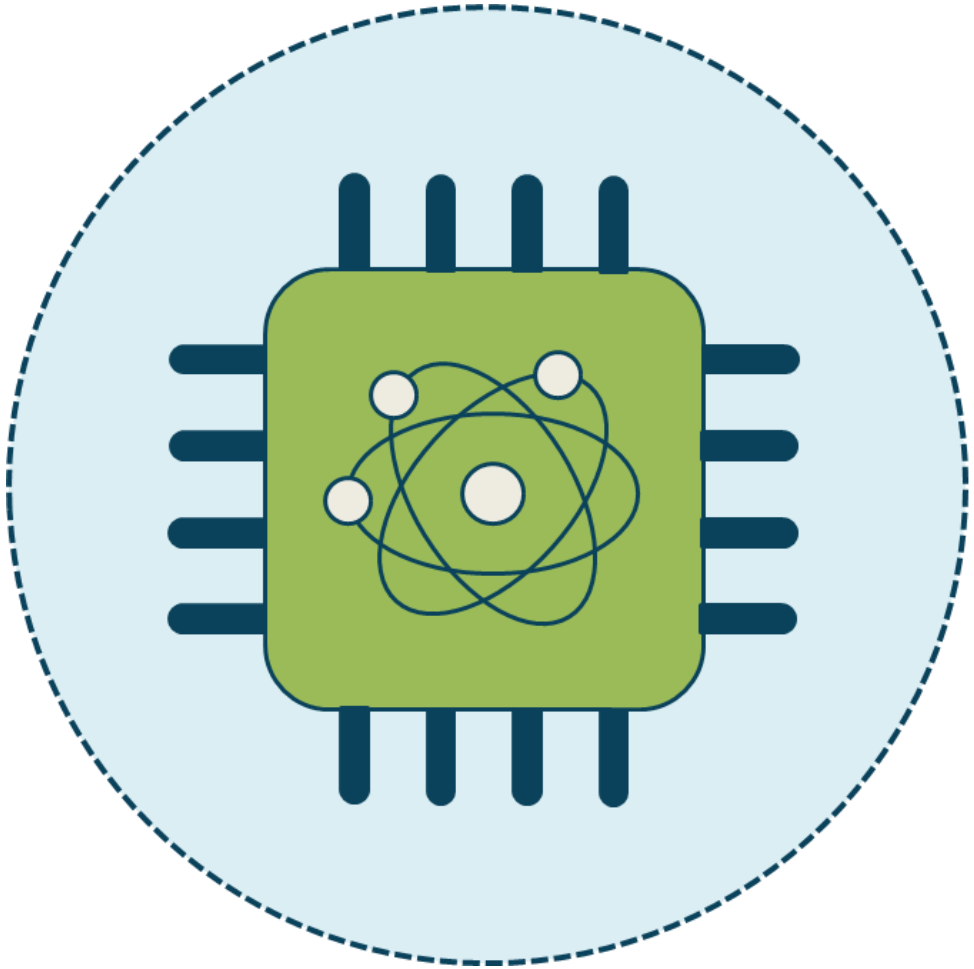
Perfect Forward Secrecy (PFS)

- Also called "forward secrecy"
- A cryptographic protocol has perfect forward secrecy if the compromise of long-term keys does not allow an attacker to obtain past session keys
- 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

Lightweight Cryptography

- Most current cryptographic algorithms were designed for desktop/server environments
- There are several emerging areas such as sensor networks, healthcare, distributed control systems, and IoT, in which highly-constrained devices are interconnected
- They are usually communicating wirelessly and working together to accomplish some task
- NIST held its Lightweight Cryptography Workshop in November 2019 and they are still evaluating protocol submissions

Quantum Computing



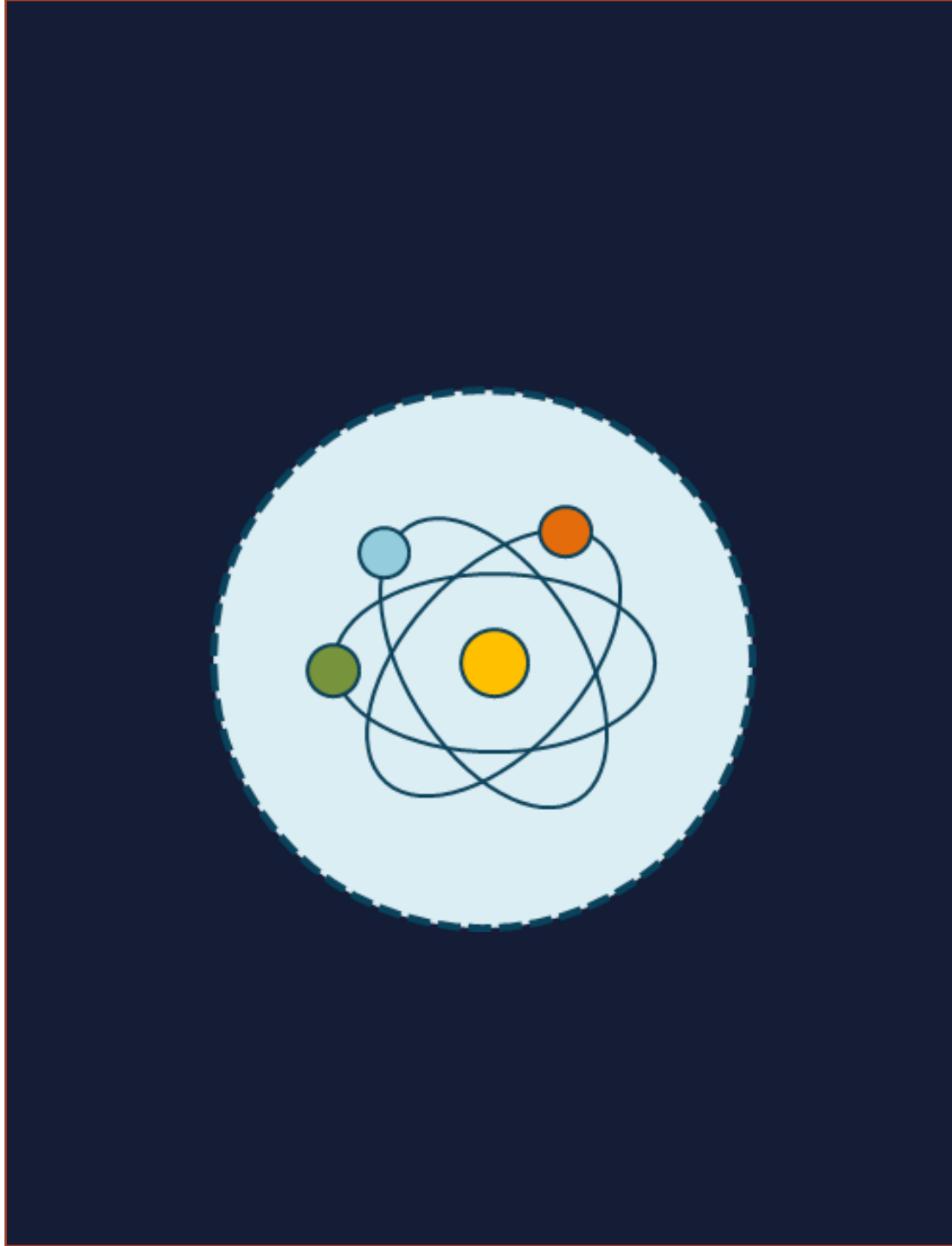
- Personal computers use bits (1s or 0s) whereas quantum computers use qubits
- These are typically subatomic particles like electrons or photons
- Quantum computing derives its power from the fact that qubits can represent numerous possible combinations of 1 and 0 at the same time
- This ability to simultaneously be in multiple states is called superposition

Post-Quantum Computing

- Post-quantum cryptography involves developing new cryptosystems that can be implemented using today's existing computers, but that will be resistant to attacks from tomorrow's quantum computers
  - Increase the size of digital keys
  - Develop more complex trapdoor functions
  - Lattice-based cryptography
  - Supersingular isogeny key exchange

Quantum Communications

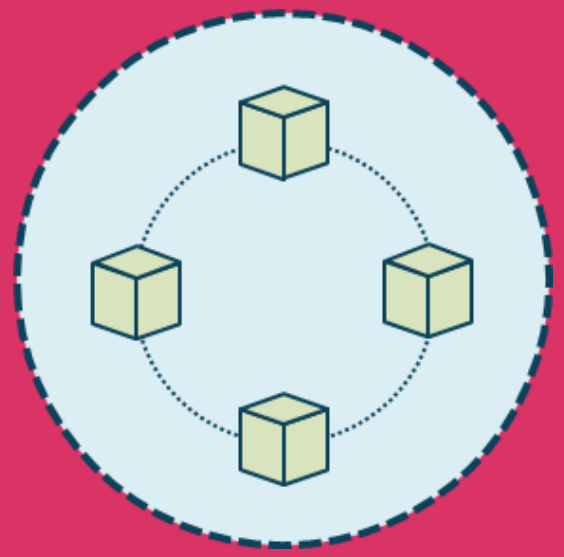
- Quantum communication leverages the laws of quantum physics and quantum computing to protect data
- Some organizations are transmitting highly sensitive data using quantum key distribution (QKD)
- QKD sends encrypted data as normal bits over the network, while the decryption key information is encoded and transmitted in a quantum state using qubits
- These networks are theoretically ultra-secure



Homomorphic Encryption

- Helps to protect data-in-use
- Data remains encrypted while being processed
- CSPs can apply functions on encrypted data
- Commonly uses public/private keypair
- Uses algebraic operations on ciphertext

Blockchain

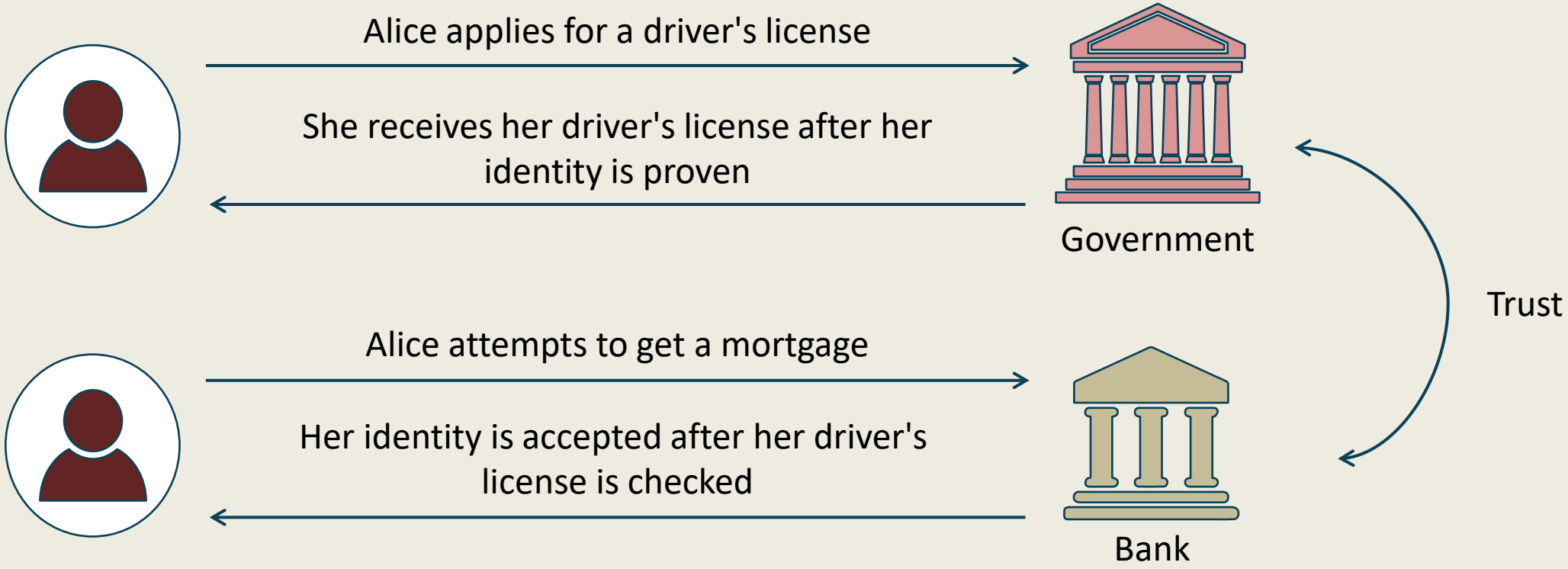


- A public ledger consisting of a digital "chain of blocks" storing information
- Transaction data such as date, time, and amount
- The transaction participants identities are based on digital signatures
- Unique cryptographic hashes that distinguish the blocks from each other
- These things must occur for a block to be added
  - A transaction must take place
  - The transaction must be verified
  - That transaction must be stored in a block and given a hash

Key Management

- Symmetric systems are more vulnerable to poor key management
- Only authorized persons should be involved in the life cycle
- Long-term storage is often done with Gemalto HSM or CloudHSM
- Removing keys from operation:
  - Destruction - removes an instance of a key in one of the permissible key forms at a specific location
  - Deletion – also removes an instance of a key, plus any data from which the key may be reconstructed, from its operational storage/use location
  - Termination - All instances and information of the key are completely removed from all locations, making it impossible to regenerate or reconstruct the key

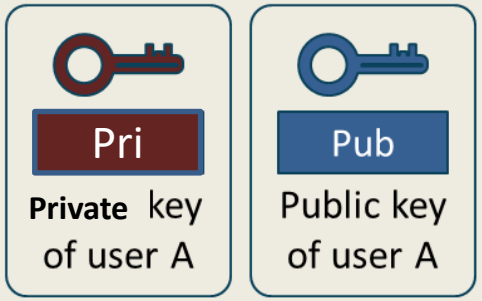
Trusted Third Parties



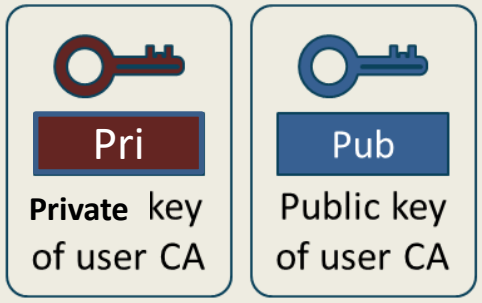
Public Key Infrastructure

- 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

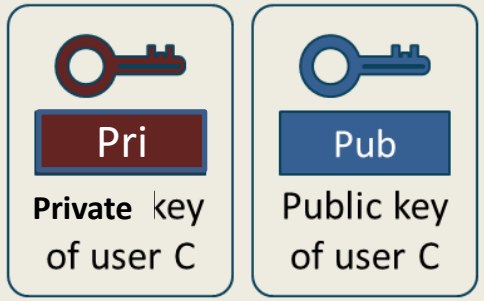
User A



Certificate Authority

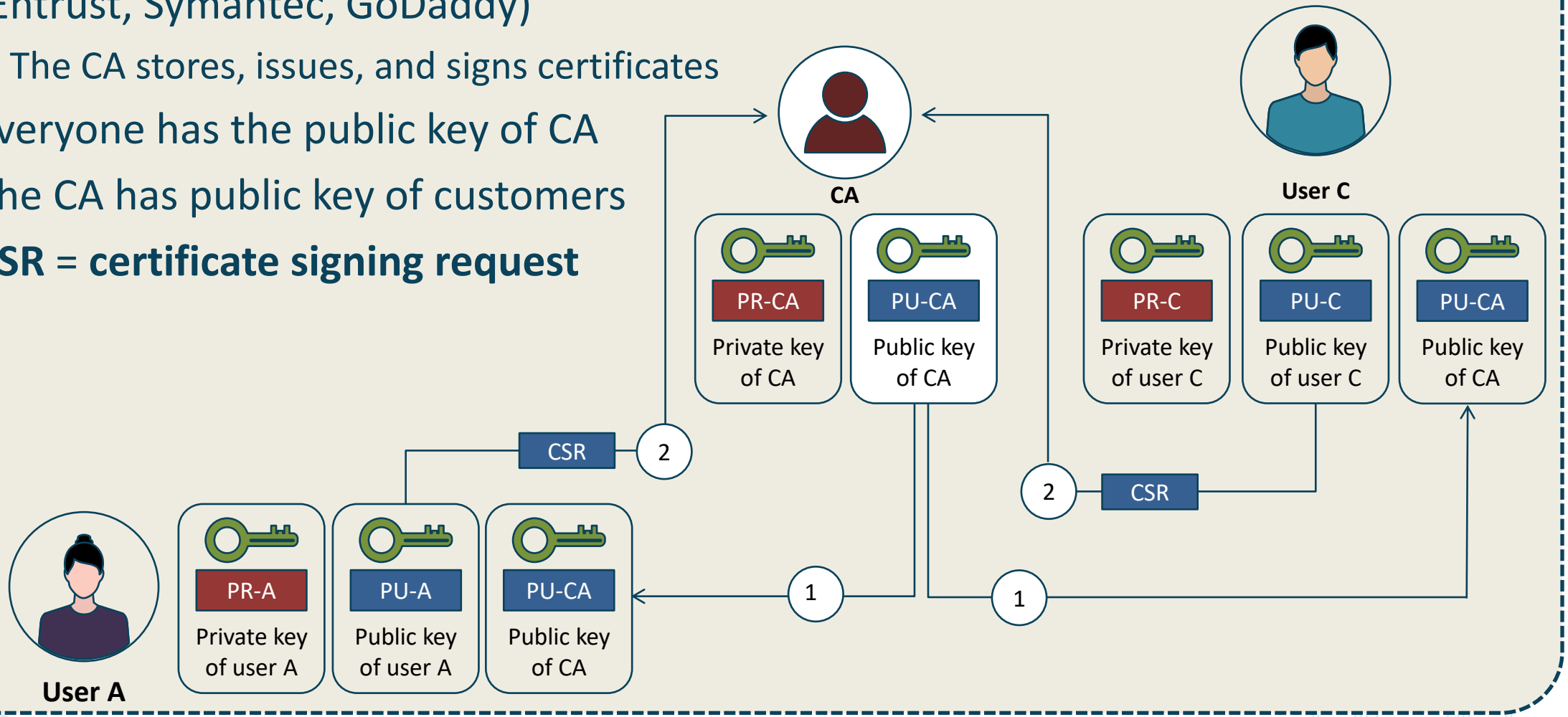


User C



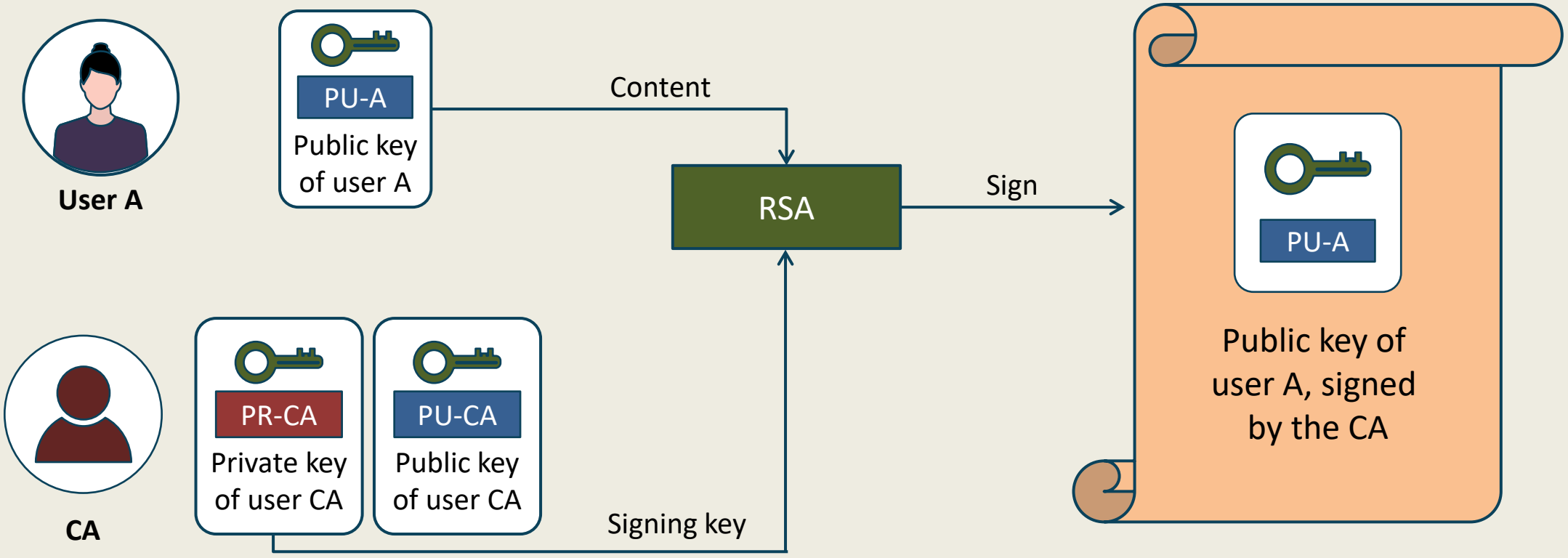
Public Key Infrastructure

- CA is the central trusted introducer (Entrust, Symantec, GoDaddy)
  - The CA stores, issues, and signs certificates
- Everyone has the public key of CA
- The CA has public key of customers
- **CSR = certificate signing request**



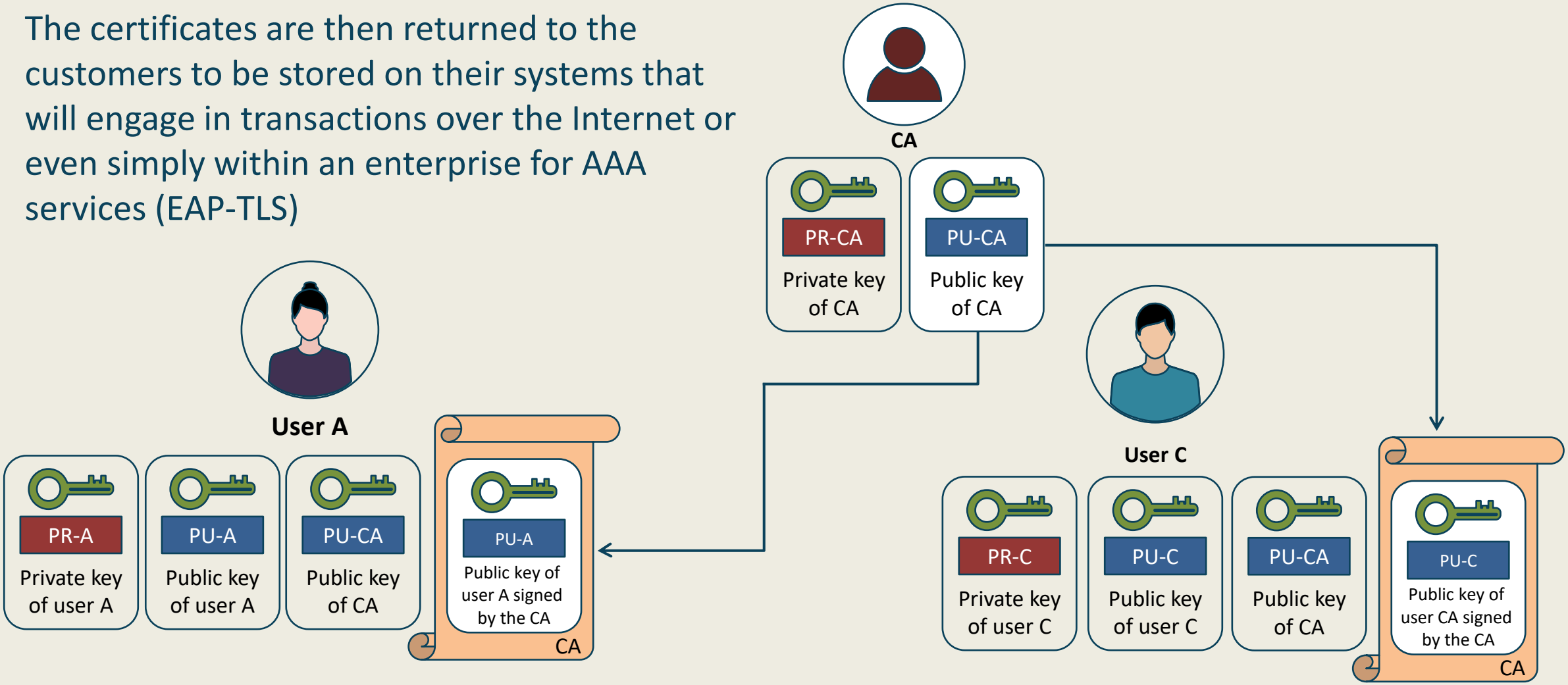
Public Key Infrastructure

The CA signs the public key of customers using its private key. It is in the form of a Digital Certificate



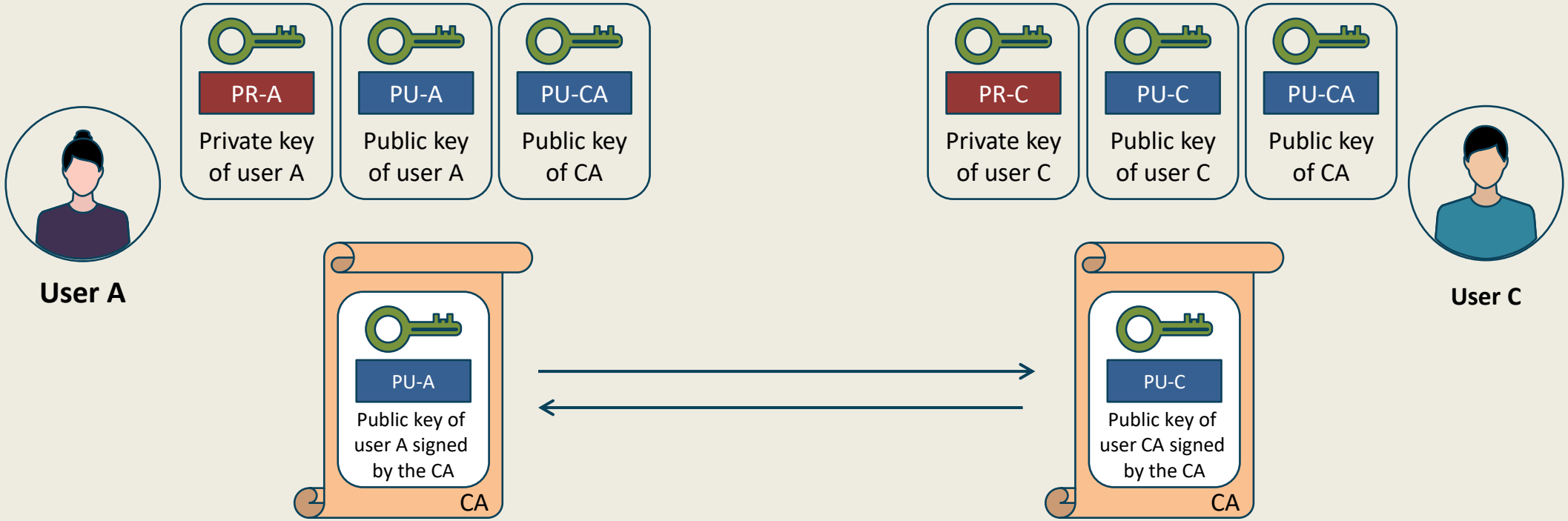
Public Key Infrastructure

The certificates are then returned to the customers to be stored on their systems that will engage in transactions over the Internet or even simply within an enterprise for AAA services (EAP-TLS)

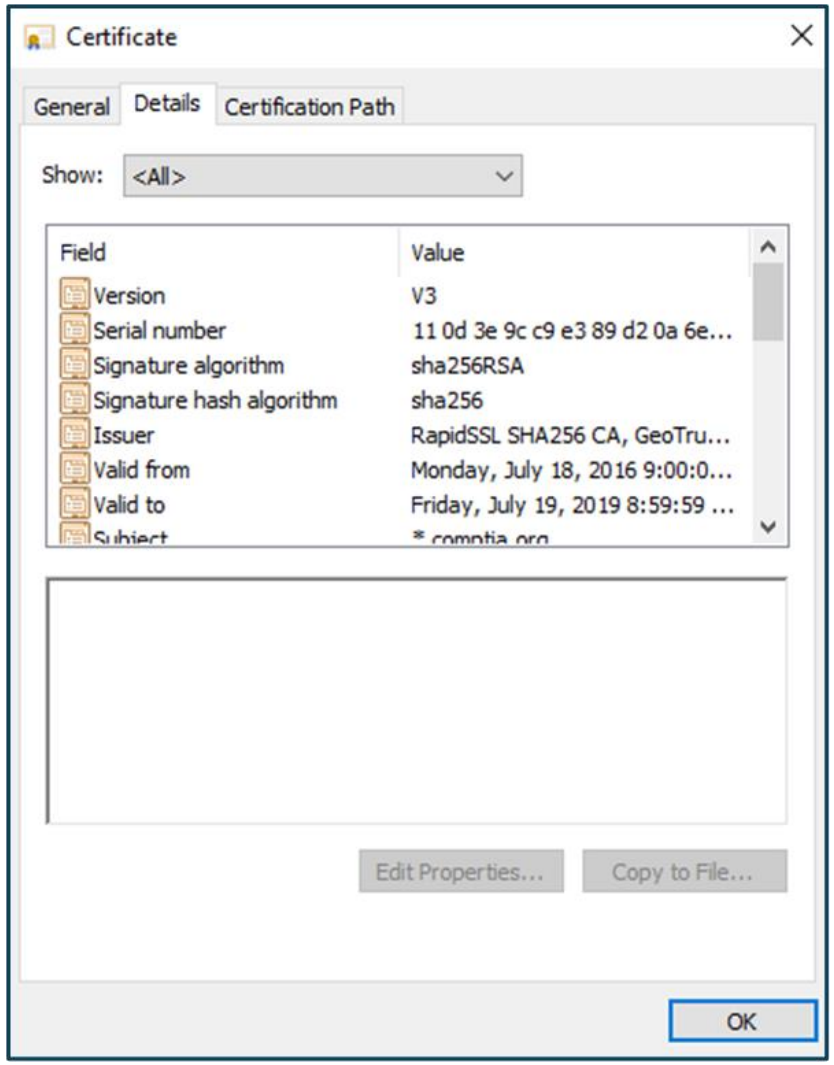


Public Key Infrastructure

Certificates can now be exchanged over untrusted network. Certificates/public keys of entities are now verified with public key of CA or another entity that is part of the Certificate Authorities web of trust



X.509v3 Certificate Format



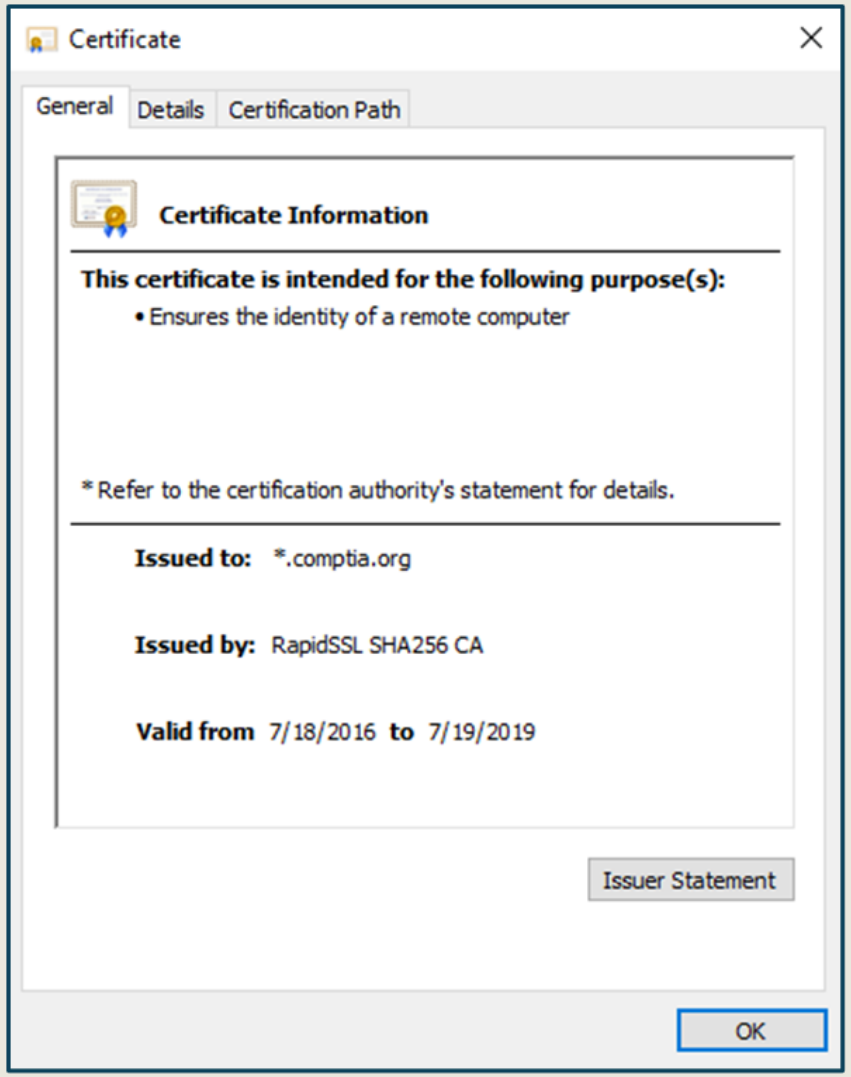
- Version number
- Serial number
- Signature algorithm ID
- Issuer name
- Validity period
  - Not before
  - Not after
- Subject name*
- Subject Alternative Name (SAN)
- Subject public key info
  - Public key algorithm
  - Subject public key
- Issuer unique identifier
- Subject unique identifier
- Extensions
- Certificate signature algorithm
- Certificate signature

Certificate File Extensions

Not to be confused with certificate extension fields

- DER
  - A form of binary encoding using definitive lengths
- CER
  - A form of binary encoding using indefinite lengths
- **PEM (Privacy-enhanced Electronic Mail)**
  - **A Base64 encoded DER certificate (most common)**
- PFX
  - A predecessor of PKCS#12
- P12 (PKCS#12)
  - A standard used for exchanging public and private objects such as keys
- P7B (PKCS#7)
  - A standard used for signing and encrypting data

Certificate Types



- Wildcard - used with multiple subdomains (*.)
- Code signing - authenticates the source and integrity of drivers, apps, macros, configuration files, and more
- Self-signed - signed by the entity it certifies
- Root - unsigned or self-signed that identifies the root CA – serves as a trust anchor for digital certificates in the chain of trust
- E-mail (S/MIME) - sign and encrypt e-mail messages
- Machine/computer and User - an individual entity authenticated to a network directory

Certificate Validation

Domain Validation (DV)

Provides proof over the control of a domain using an email or domain registry check (WHOIS)

Organization Validated (OV)

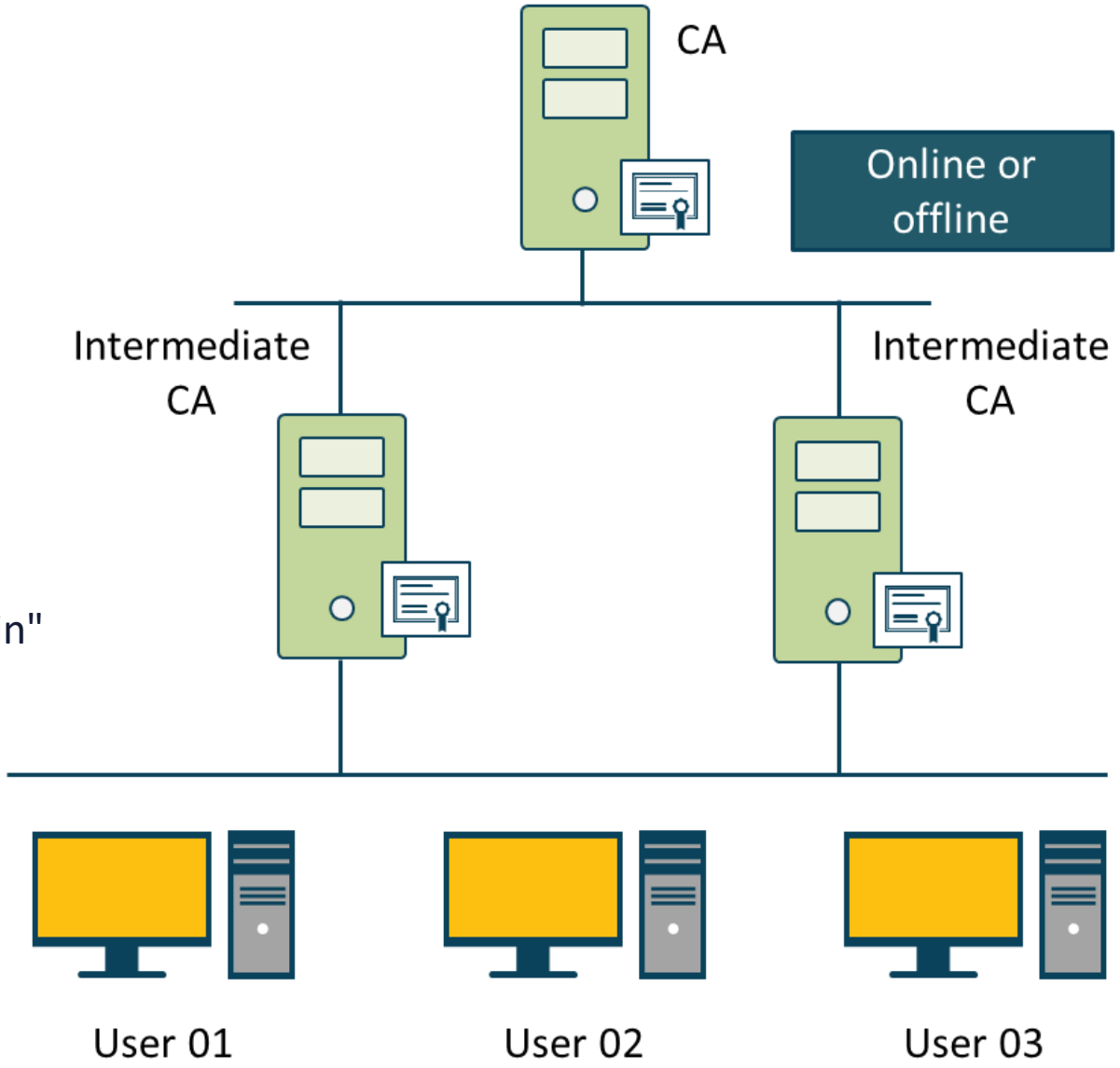
Certificates require more validation than DV certificates, but provide more trust

Extended Validation (EV)

Certificates provide the maximum amount of trust to visitors with green padlock

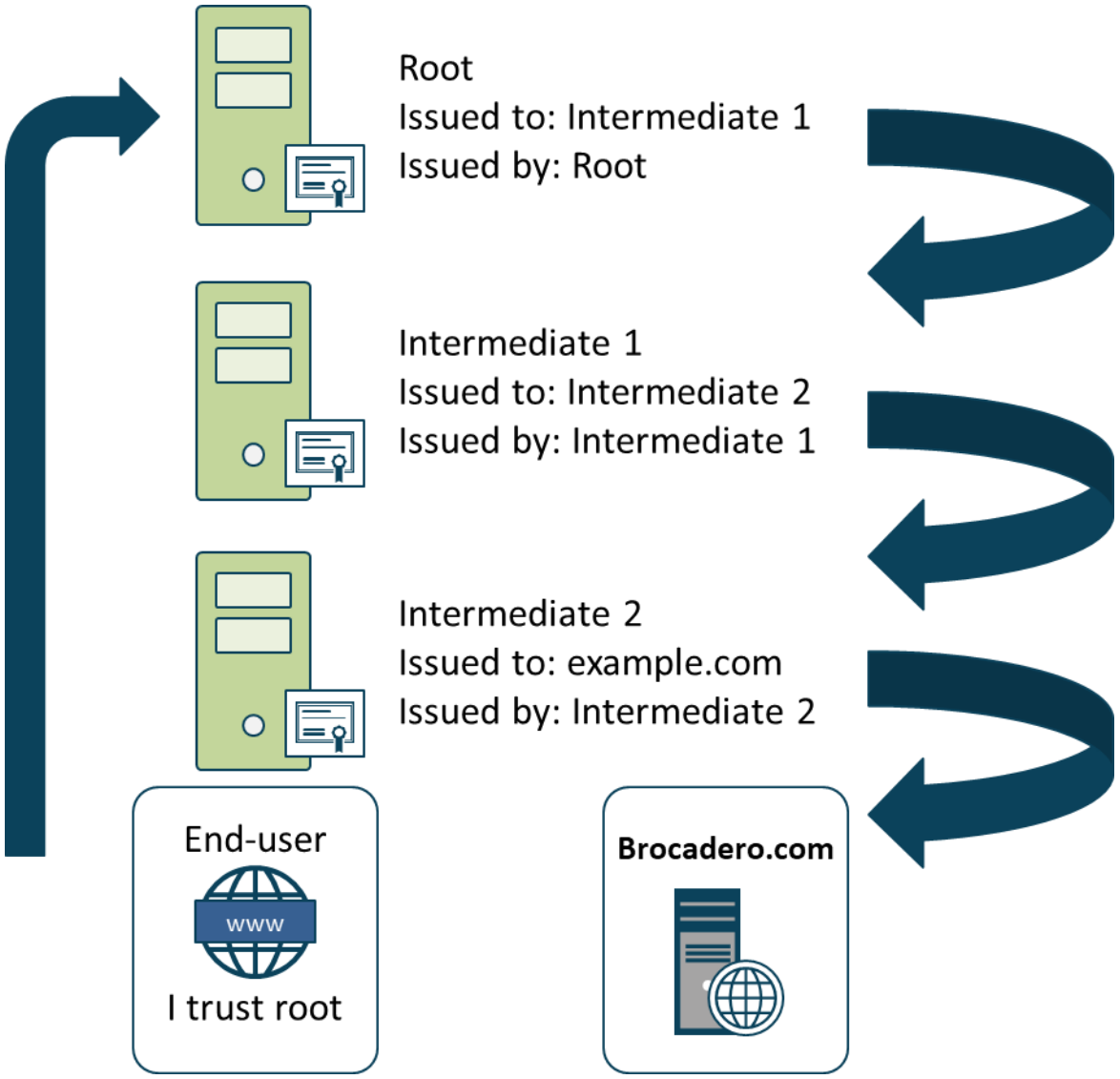
CA Trust Models

- **Single CA**
  - Responsible for directly providing certificates to everyone (enterprise PKI)
  - Must always be online
- **Hierarchical**
  - Combination of root CA and 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 and issues certificates over the network
    - Offline - not connected to network and issues certificates on removable media



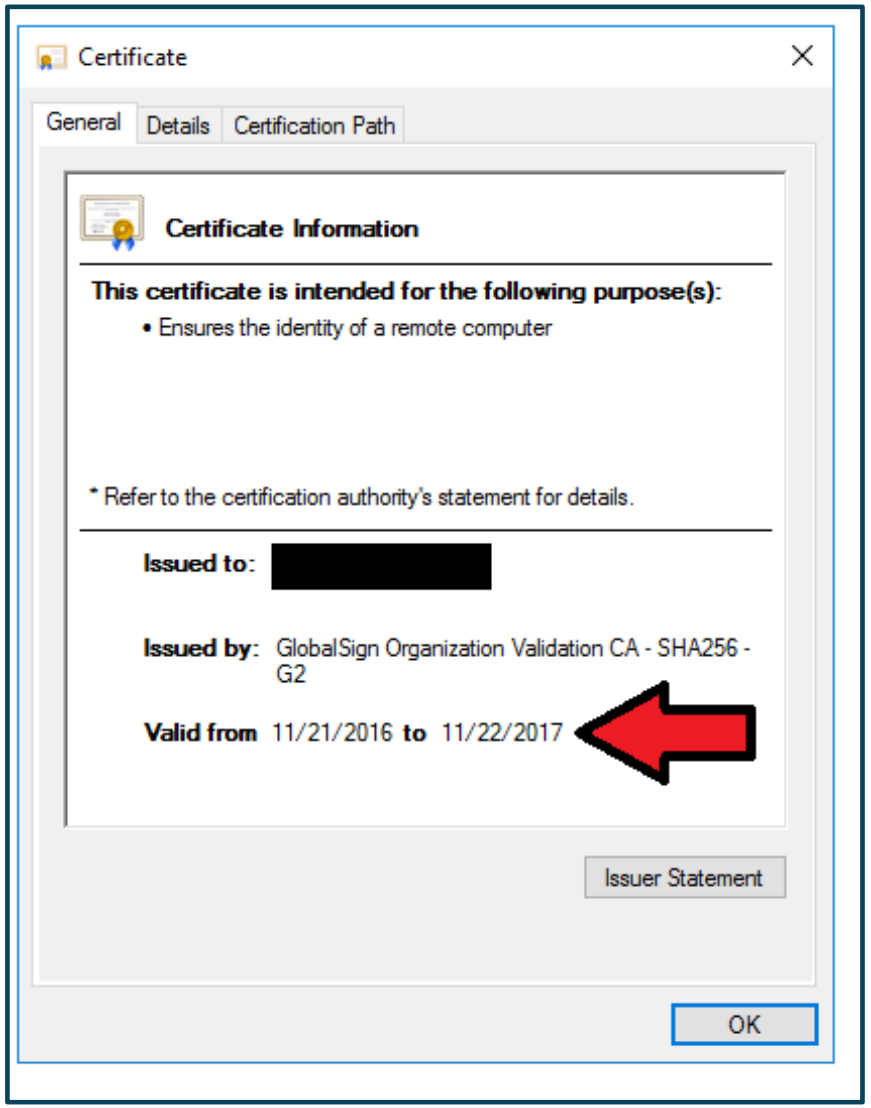
CA Certificate Chaining

- How do I trust a certificate?
  - The CA must be in trusted store
- It is not possible to include all CAs
- A chain of trust is used
  - "Issued to" field
  - "Issued by" field



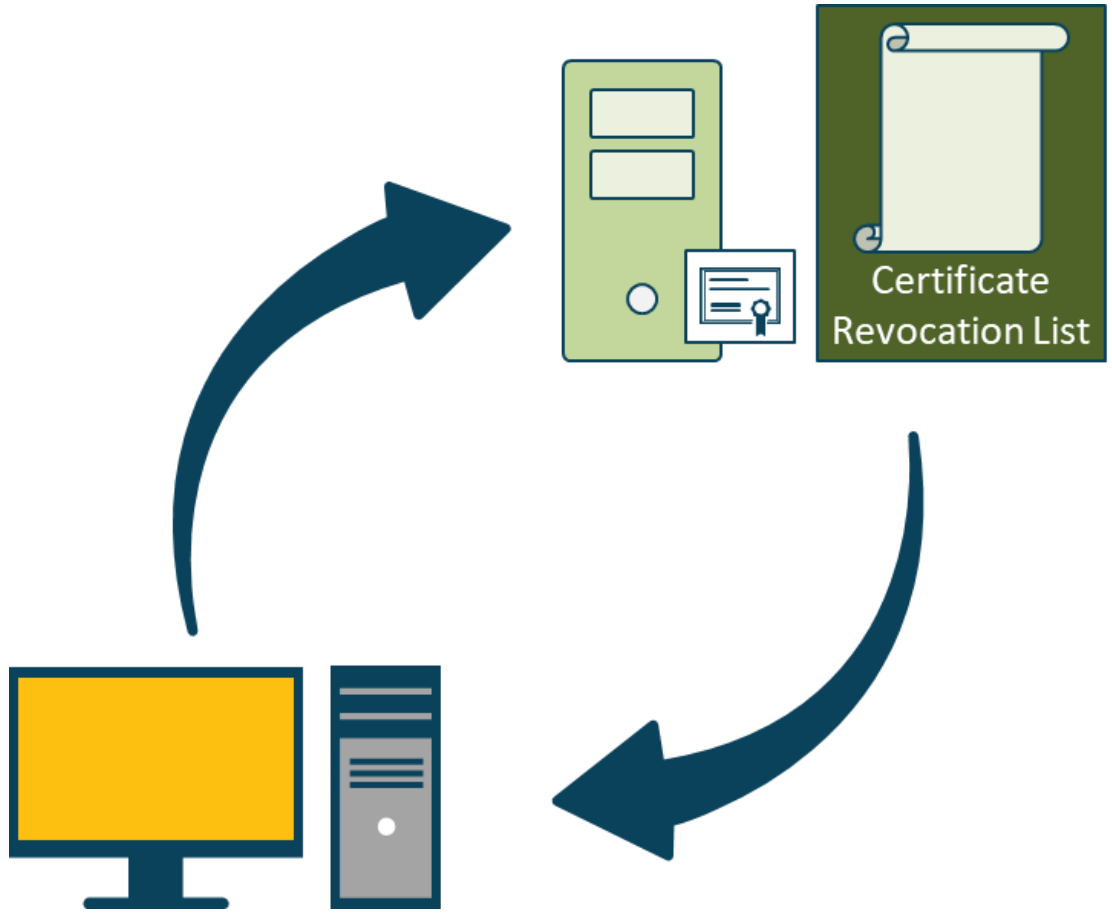
Certificate Revocation and Suspension

- 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



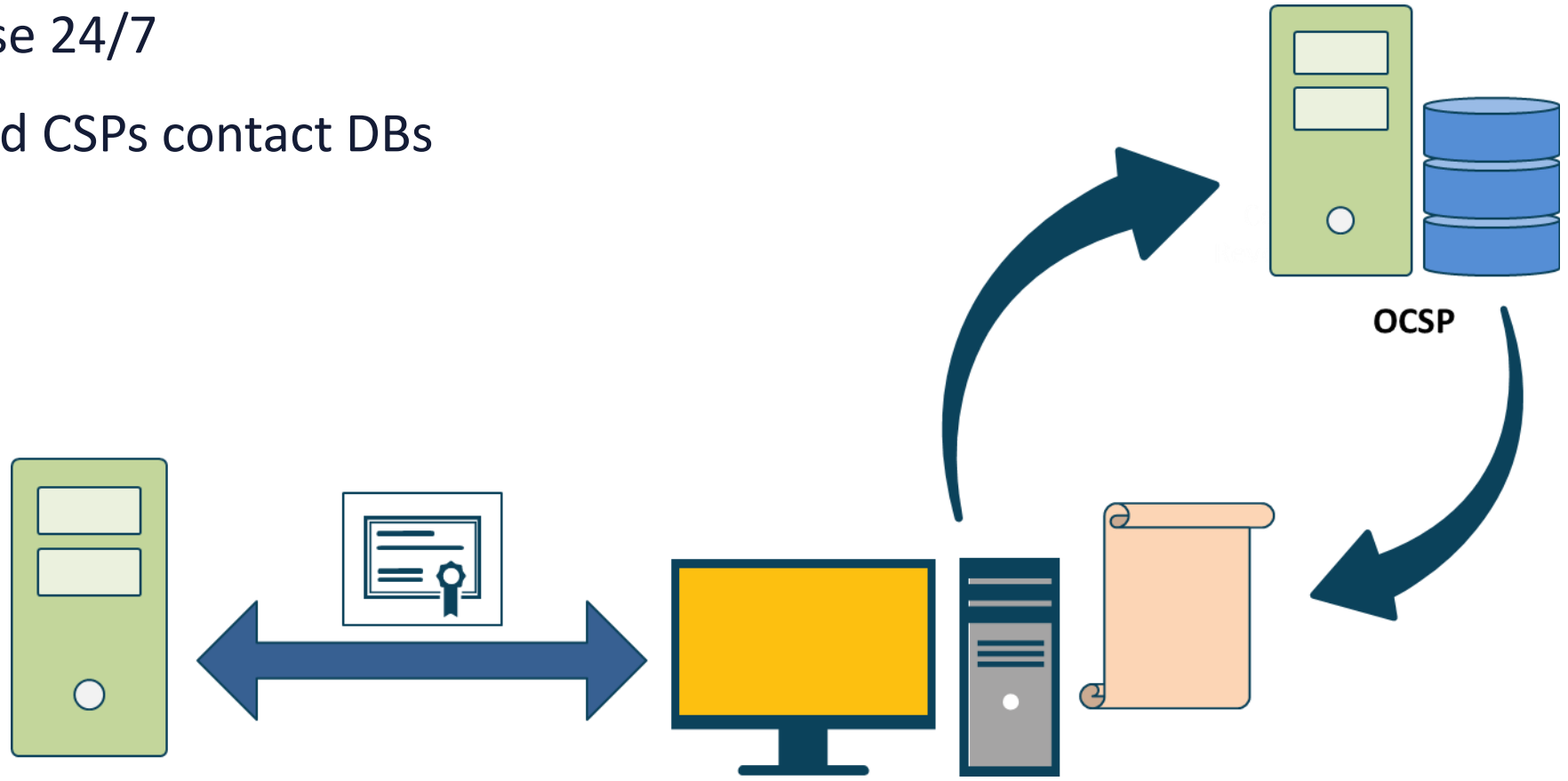
Certificate Revocation List (CRL)

- A list of certificate serial numbers that are no longer valid or have been revoked
- Issued by CA who issued certificate
- Generated and published periodically
  - Defined intervals or immediately (not real-time)
  - Downloaded by client regularly (not real-time)



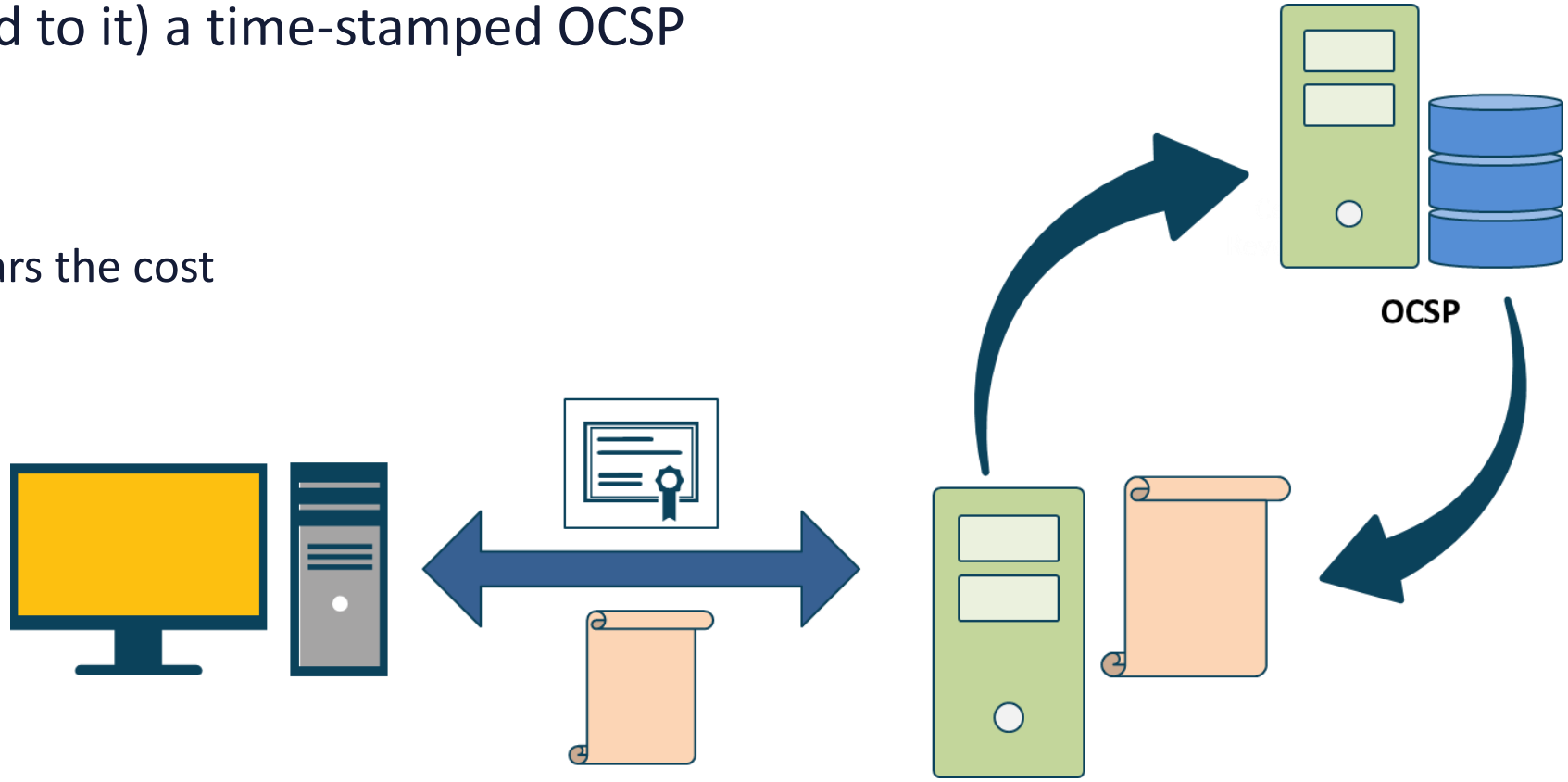
Online Certificate Status Protocol (OCSP)

- Generated and published immediately
- Online database
- Clients query database 24/7
- Web servers, ISPs, and CSPs contact DBs



Certificate Stapling

- Alternate approach of checking the revocation status of certificate (OCSP stapling/TLS certificate status request)
- 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 cost



Certificate Pinning

- A 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)
- Pin when you need to be 100% sure of remote host's identity and/or when you are in a hostile environment
- Certificate pinning - easiest but not flexible
- Public key pinning – difficult but more flexible