Welcome to the SSCP Bootcamp

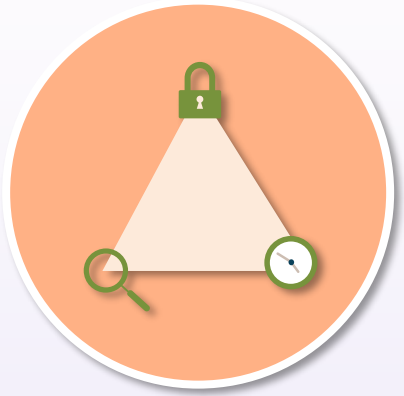
Your instructor:

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)**

Systems Security Certified Practitioner (SSCP) Bootcamp



Session 1

Systems Security Certified Practitioner (SSCP)

Basic Security Concepts

(ISC)² Code of Professional Ethics

"All information security professionals who are certified by (ISC)² recognize that such certification is a privilege that must be both earned and maintained. In support of this principle, all (ISC)² members are required to commit to fully support this Code of Ethics (the "Code").

(ISC)² members who intentionally or knowingly violate any provision of the Code will be subject to action by a peer review panel, which may result in the revocation of certification.

(ISC)² members are obligated to follow the ethics complaint procedure upon observing any action by an (ISC)² member that breach the Code. Failure to do so may be considered a breach of the Code pursuant to Canon IV."

"Code of Ethics: Complaint Procedures: Committee Members," Code of Ethics | Complaint Procedures | Committee Members ((ISC)², Inc, 1996), https://www.isc2.org/Ethics.

Code of Ethics Preamble

- "The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior
- Therefore, strict adherence to this Code is a condition of certification"

"Code of Ethics: Complaint Procedures: Committee Members," Code of Ethics | Complaint Procedures | Committee Members ((ISC)², Inc, 1996), https://www.isc2.org/Ethics.

Code of Ethics Canons

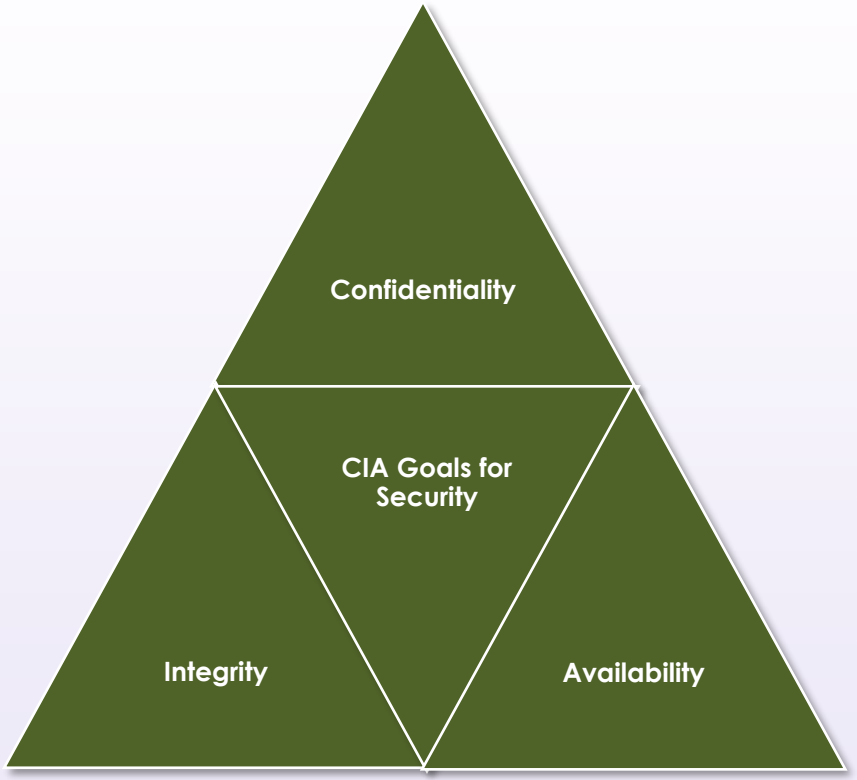
1. Protect society, the common good, necessary public trust and confidence, and the infrastructure

2. Act honorably, honestly, justly, responsibly, and legally

3. Provide diligent and competent service to principals

4. Advance and protect the profession

CIA Triad


Confidentiality
CIA Goals for Security
Integrity
Availability

Confidentiality

- Confidentiality measures the attacker's ability to get unauthorized data or access to information from an application or system
- Involves using techniques, such as cryptography, tokenization, and compartmentalization, to allow only approved users the ability to view or access sensitive information
- Confidential information can include passwords, cryptographic keys, personally identifiable information (PII), personal health information (PHI), intellectual property (IP), or other secret or top-secret information

Confidentiality According to NIST

- The security objective that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads
- Confidentiality covers data in storage, during processing, and while in transit
- In a general information security context, it preserves authorized restrictions on information access and disclosure, including means for preserving personal privacy and proprietary information

High-level Confidentiality

- Uses hybrid encryption involving combinations of symmetric and asymmetric cryptosystems
- Employs advanced post-quantum and homomorphic cryptosystems
- Combines secure compartmentalization with the most recent modes of encryption available

Integrity

- Integrity measures an attacker's ability to manipulate, change, or remove data at rest and data in transit
- Involves implementing controls that make certain only authorized subjects can change sensitive information
- Might also include affirming the identity of a communication peer (origin authentication)
- Examples would be injection or hijacking attacks on data in transit, modifying files, changing access control lists, and DNS or ARP cache poisoning

Integrity According to NIST

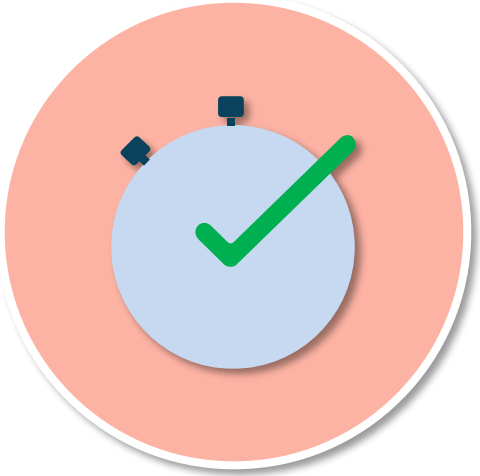
- Protection against unauthorized modification or destruction of information
- A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination
- It guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity

High-level Integrity

- The advanced goals of the Clark-Wilson model:
  - Prevent unauthorized users from making modifications
  - Ensure separation of duties prevents authorized users from making improper modifications
  - Ensure well-formed transactions; maintain internal and external consistency

Availability

An aspect of resiliency



- Resilience is the ability of a system to continue to
  - operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and
  - recover to an effective operational posture in a time frame consistent with mission needs
- Availability measures an attacker's ability to disrupt or prevent access to services or data
- Controls will protect systems and services from spoofing, flooding, denial-of-service (DDoS), poisoning, and other attacks that negatively affect the ability to deliver data, content, or services

High-level Availability

- Vulnerabilities that impact availability can affect hardware, software, and network resources, such as flooding network bandwidth, consuming large amounts of memory, CPU cycles, or unnecessary power consumption
- Availability zones of cloud service providers
  - Multiple datacenters in one
  - Zones are tens of miles apart
  - Connected with high-speed fiber (MANs)
  - Placed in regions all over the world
  - Can distribute through CDN services into metro areas

D.A.D

You can also describe the CIA goals of the security triad by looking at the opposite – D.A.D

- Disclosure is the unauthorized revealing of data and information
- Alteration is the unauthorized change or modification of data or systems
- Destruction involves rendering an entity inaccessible – can also add the element of lack of durability in some scenarios

Accountability

- The principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information
- This security goal creates the requirement for actions of an entity to be traced uniquely to that entity
- This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action

Accountability

From a practical standpoint, accountability will involve first deploying the proper administrative, technical, and physical controls to offer automated and enhanced visibility into all activities of your highest privileged users on the mission critical systems and applications

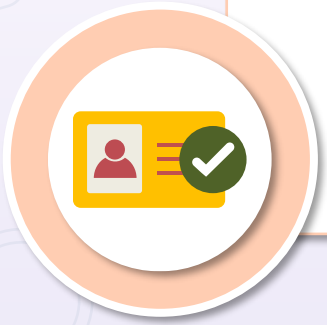
Accountability

Authentication

Authorization

Accounting

High-level Authenticity



- Origin authentication is a basic form of authentication, as it only provides a degree of confidence that the correct password, passphrase, or private/secret key was used
- Additional levels of authentication rely on trusted third parties and certificates, digital signatures, and multi-factors, like biometrics
- A new trend is knowledge-based authentication (KBA)

Privacy According to NIST

Related to confidentiality

- The freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual
- Assurance that the **confidentiality** of, and access to, certain information about an entity is protected
- The right of a party to maintain control over and confidentiality of information about itself

Privacy by Design

- Individuals do not always understand the possible consequences for their privacy when they interact with applications, systems, products, and services
- Failure to design for privacy can have direct negative effects at both the individual and societal levels affecting
  - an organization's brands
  - the financial bottom line, and
  - future prospects for growth

Privacy by Design

Taking privacy into account as you design and deploy systems, products, and services that affect individuals

Realizing that privacy issues can be different when dealing with other countries and jurisdictions (General Data Protection Regulation, or GDPR)

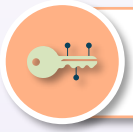
Communicating about your organizational privacy practices with all stakeholders

Encouraging cross-organizational workforce collaboration by developing profiles, selection of tiers, and achievement of outcomes

Non-repudiation

The inability to refuse participation in a digital transaction, contract, or communication (S/MIME)

With cryptosystems, a public/private key pair is used



The owner/creator of the private key must protect the key

The owner/creator of the private key must notify a trusted third party when the key is lost, stolen, or compromised

Is usually accomplished with digitally signed certificates

Non-repudiation According to NIST

- Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data
- Technical non-repudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key
- Legal non-repudiation refers to how well possession or control of the private signature key can be established

Least Privilege

- An aspect of AAA and IAM where the subject has just the proper level (or amount) of permissions and rights to perform the job role or responsibility and nothing more
- Should be built into all access control architectures
- Any deviation (escalation or elevation), if allowed, should go through an established change control IT service or service desk implementation
- Also referred to as "need to know" or staying within one's "pay grade" or classification level

NIST SP 800-53 Least Privilege

Authorize access to all security functions

Use non-privileged accounts or roles when accessing non-security functions

Prevent non-privileged users from executing privileged functions

Audit the execution of secure functions

ISO/IEC 27001 Least Privilege

Access to networks and network services

Management of privileged access rights

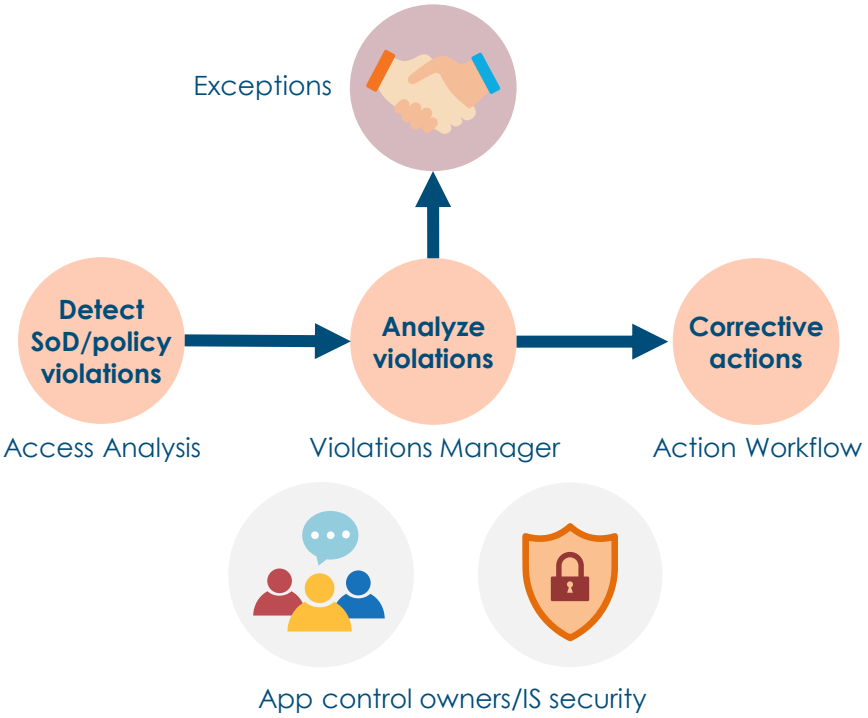
Use of privileged utility programs

Access control to program source code

Segregation of Duties

- Also referred to as "separation of duties"
- A principle where more than one entity is required to complete a particular task, such as a separate Backup Operators group and a Data Restoration group
- SoD policies are often automated and strictly enforced in areas with highly sensitive data, applications, and systems

Segregation of Duties Example



Segregation of Duties

- Example: two signatures or cryptographic keys are required for certain actions
- Rotation of duties is also a related principle where the roles of two subjects switch at scheduled or arbitrary times
  - Example: mandatory time-off or forced vacations

Systems Security Certified Practitioner (SSCP)

Security controls

Administrative Controls

Administrative (or managerial) controls define policies, procedures, best practices, and guidelines

Should be published or printed definition of policies

- Risk assessment and management
- Best practices and guidelines
- Password policies
- Screening, hiring, and termination procedures
- Mandatory vacations
- Training and awareness

AUP Administrative Controls

No piggybacking or tailgating

Clean desk policy

Mandatory vacations

Rotation of duties

Segregation of duties

Technical Controls

- Technical controls are security mechanisms that the specific systems run – either manually or more often automated and orchestrated
- These controls deliver confidentiality, integrity, authenticity, and availability protections
- They defend against unauthorized access or misuse
- They also facilitate detection of security violations and support security requirements for applications and data

Technical Controls

Infrastructure security and device hardening

Identity and access management

Cryptographic key management and HSM

Web application firewalls and threat modeling tools

Next-generation endpoint detection and response

Physical Controls

- Physical controls are introduced to protect the campus, facility, environment, and people
  - Various physical barriers
  - Guards and security teams
  - Cameras and surveillance equipment
  - Different types of sensors and alarms
  - Locking mechanisms
  - Secure safes, cabinets, cages, and areas
  - Mantraps and faraday cages
  - Fire detection and suppression systems
  - Environmental controls

Security Control Categories

Administrative	Technical	Physical
Effective hiring practices	Controlled user interfaces	Guards
Effective termination practices	Passwords, tokens, OTPs	Fences
Classification of data based on levels of sensitivity	Firewalls	Motion detectors
Supervision of employees	Routers that filter traffic	Locks
Tracking of employee activity	Antivirus software	Cable conduits
Separation of duties	Access control lists	Swipe cards
Rotation of duties	Intrusion detection/prevention systems	Badges
Dual operator	Smart cards	Dogs
Clean desk policy	Biometrics	Cameras
No tailgating or piggybacking	Hardware security modules (HSM)	Alarms

Deterrent Controls

- Deterrent controls discourage the attacker from performing an attack
- They do not prevent someone from performing the unauthorized action, but rather encourage them to choose not to do something
- Policies and regulations are forms of deterrent where the violation of a policy could result in the employee being disciplined or fired

Deterrent Controls

- Violation of a regulation or law could result in criminal or civil prosecution
- Examples include signs in public places that indicate that video monitoring is being used and yard, fence, and window signs and stickers with alarm company logos
- The signs themselves do nothing to avert people from doing something undesirable, but they should indicate that there may be consequences for doing so

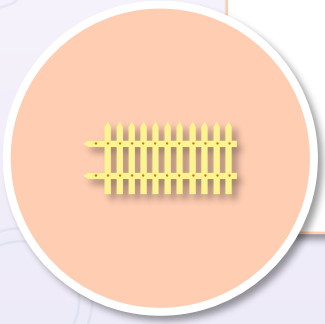
More Deterrent Controls

- Locks (may be preventative on the exam)
- Signage and bollards
- Security badges and security guards
- Mantraps
- Security cameras and lighting (also detective)
- Trespass or intrusion alarms
- Separation of duties
- Auditing and accounting

Preventative Controls

- Preventive controls stop the attacker from performing the exploit
- Preventative controls describe any security measure that is designed to stop unwanted or unauthorized activity from occurring
- Examples include physical controls, such as fences, locks (also a deterrent), and gates
- Technical controls, such as updated antivirus software, restrictive firewalls, and IPS sensors
- Administrative are rarely a strict preventative control due to their logical and voluntary nature

More Preventative Controls



- Locks (may be deterrent on the exam)
- Fences and gates
- Security badges and security guards
- Mantraps
- Security cameras and lighting (also detective)
- Trespass or intrusion alarms
- Auditing and accounting

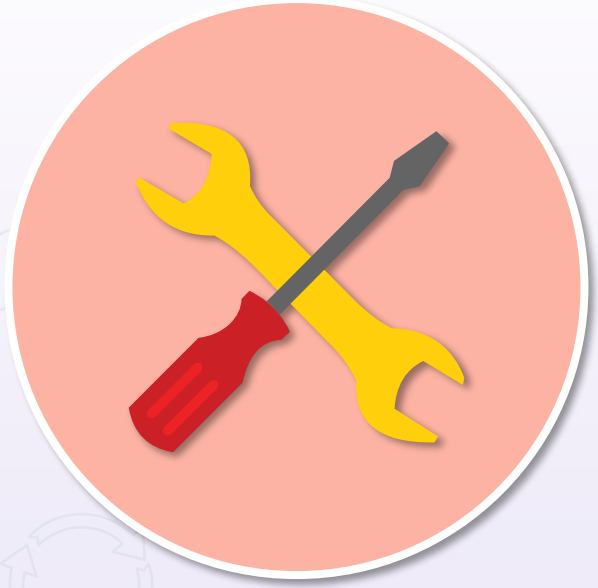
Detective Controls

- Detective controls identify that an attack is happening
- Any security measure taken or solution that is implemented to detect and alert to unwanted or unauthorized activity in progress or after it has occurred
- Detective controls can be proactive or reactive
- They can be manual or automated

Detective Controls

- **Examples of detective controls include the following:**
- Alarms, logs, and alerts sent from SNMP agents
- NetFlow records
- CCTV and security webcams
- Notifications from physical sensors (door alarms, fire alarms) that alert guards, police, or system administrators
- Honeypots, honeynets, and honeytokens
- IDS and IPS sensors
- SIEM and SOAR systems

Corrective Controls



- Corrective controls include any measures taken to repair damage or restore resources and capabilities to their prior state following an unauthorized or unwanted activity
- Examples of technical corrective controls include patching a system, quarantining a virus, terminating a process, or rebooting a system
- Putting an incident response plan into action is an example of an administrative corrective control

Compensating Controls

- In the simplest terms, mitigating controls (preventative or corrective) are meant to reduce the chances of a threat occurring, while compensating controls are put into place when certain requirements for compliance cannot be met with existing controls
- The former is permanent; the latter is temporary
- Compensating controls often aid or augment controls that are already in place until more permanent solutions can be deployed

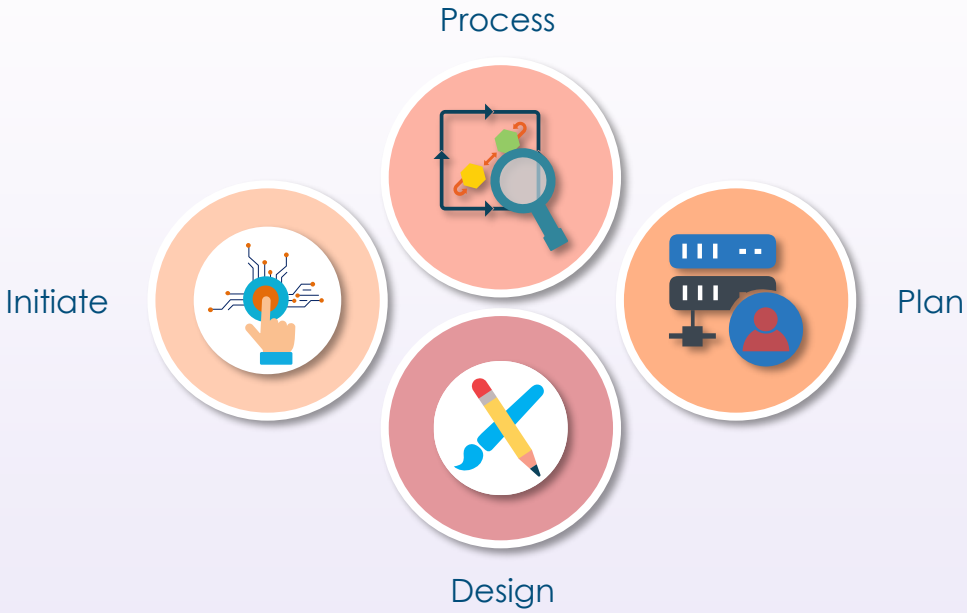
Compensating Controls

- Compensating controls are often the result of an audit, vulnerability assessment, or penetration test
- It is a temporary improvement or upgrade to an existing control to reduce residual risk while increasing difficulty or resistance to a threat agent
- Introducing a dual operator or segregation of duties initiative can be considered improving the existing access control architecture

Systems Security Certified Practitioner (SSCP)

Asset and Change Management Lifecycles

Process, Planning, Design, and Initiation



Process, Planning, Design, and Initiation

- Before you can successfully analyze risk, you must have a good understanding of your organization's assets, both physical and logical
- You also must determine all roles and responsibilities, as they pertain to assets such as data
- There are several types of asset roles, including processors, owners, custodians, stewards, and officers

Data and Asset Ownership

- Are often the creators in a discretionary access control (DAC) model
- Determine the classification level
- Decide on handling and tagging (labels)

Data and Asset Ownership

- Manage assets from a business perspective
- Often deal directly with customers (internal and external)
- Ensure compliance (standards and controls) and data quality

Data and Asset Ownership

Maintain the assets from a technical perspective

Often deal directly with stakeholders and management

Ensure confidentiality, integrity, authenticity, and availability of data and assets

Data and Asset Ownership

- Chief information officer (CIO)
- Chief privacy officer (CPO)
- Chief information security officers (CISOs)

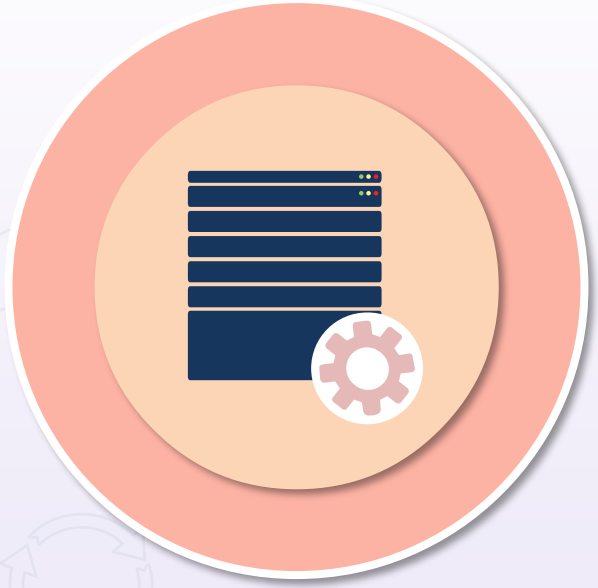
Data and Asset Classification

You may be using a model that has sensitivity levels and classification

You must have a well-established tagging and labeling schema that maps to a configuration management database (CMDB), such as ServiceNow

- Facilities, equipment, physical assets
- Data and information assets
- Human resources (people assets)
- Intangible assets and intellectual property
- Can be on-premises, in the cloud, or used as disaster recovery sites

Information and Asset Handling Requirements



- Labeling concerns the classification and prioritization of data, systems, and assets to determine the level of protection and how the asset should be handled
- Handling controls who has access to assets and what actions they can take
- Handling is based on labeling and how it has been classified

Choose a Classification Level

- Value – the most common criteria – if it is valuable, it should be protected
- Age – the value of data lowers over time – i.e., automatic de-classification
- Useful life – if the information is made obsolete it can often be de-classified
- Personal association – if the data involves personally identifiable or health information
- Architecture – the subjects and objects are assigned a sensitivity level in a mandatory access control model

Classification of Assets

Government/military:

Top Secret

Secret

Confidential

Sensitive But Unclassified (SBU)

Unclassified

Commercial/private sector:

Confidential

Private

Sensitive

Public

Development or Acquisition

- Development or acquisition is also referred to as **"build or buy"**
- This decision can mean developing a software solution in-house or purchasing from a third-party vendor
- With hardware, the deciding factor is often a public or hybrid cloud solution instead of using or expanding the data center facility
- When developing an asset management initiative, the software solution should be done securely

Development or Acquisition

Data

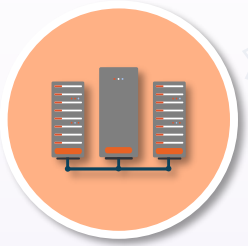
Data is either generated from scratch, inputted, or modified into another format either locally or remotely

The security practitioner must consider the privacy, confidentiality, integrity, availability, and durability of data in ALL states

Applications

Security best practices must be considered in commercial off-the-shelf (COTS) or open-source software solutions

Secure coding, version control, handling, APIs, and the overall lifecycle must be considered

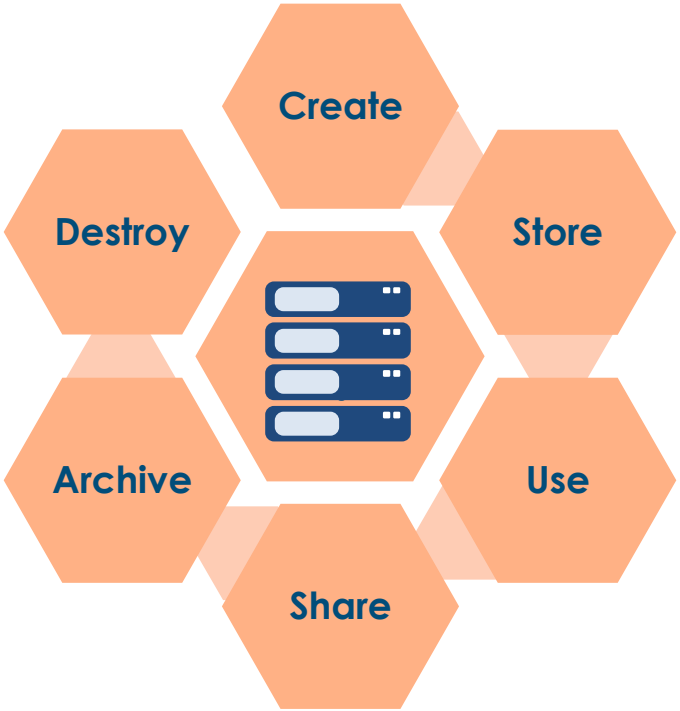


Hardware

Physical security controls must be implemented along with

- least privilege
- defense-in-depth
- separation-of-duties, and
- dual-operator

Secure Data Lifecycle



Asset Management

- Tracking all physical and logical assets for location, modification, and disposition leads to improved risk management and asset recovery for business continuity
- Whether an asset is real estate or software, the asset manager's main task is to supervise all the activities related to asset management
- Digital asset manager is a growing enterprise role
- Automation and orchestration systems are vital for medium to large organizations

Asset Inventory Control

Just-in-time (JIT) is prevalent

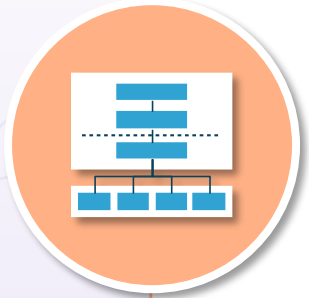
- Managing inventory helps you keep corporate budgets in line and allows for better security and more efficient management of operating capital
  - Assess the type of inventory you keep
  - Determine the quantity of goods you need to keep on hand
  - Track market trends of competitors
  - Identify minimum stock level
- Just-in-time (JIT) is an inventory strategy used to increase efficiency and decrease waste by acquiring goods only as needed in the production process

Asset Inventory Control

Just-in-time (JIT) is prevalent

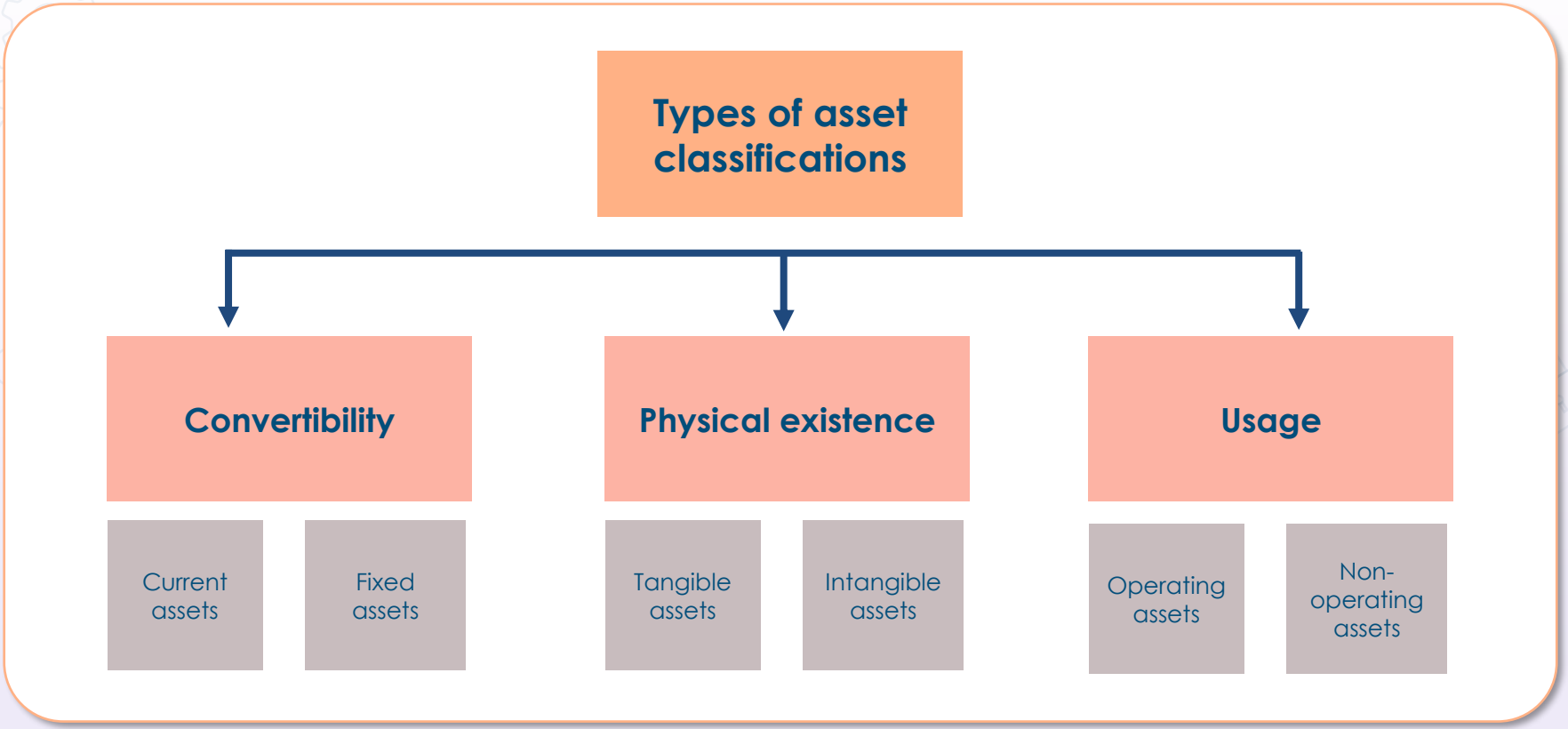
- Managing inventory helps you keep corporate budgets in line and allows for better security and more efficient management of operating capital
  - Assess the type of inventory you keep
  - Determine the quantity of goods you need to keep on hand
  - Track market trends of competitors
  - Identify minimum stock level
- Just-in-time (JIT) is an inventory strategy used to increase efficiency and decrease waste by acquiring goods only as needed in the production process

Asset Inventory Control



- Best practices for fixed asset inventory software:
  - Realize the scope of your project
  - Assign responsibility for your asset management
  - Learn basic fixed asset procedures
  - Rely on automated software in the future
  - Look for emerging technological trends
  - Clear out ghost assets (ghost IT)
  - **Have a comprehensive software licensing system with a dedicated officer(s), database, and DRP storage**
    - The more automated and orchestrated the better

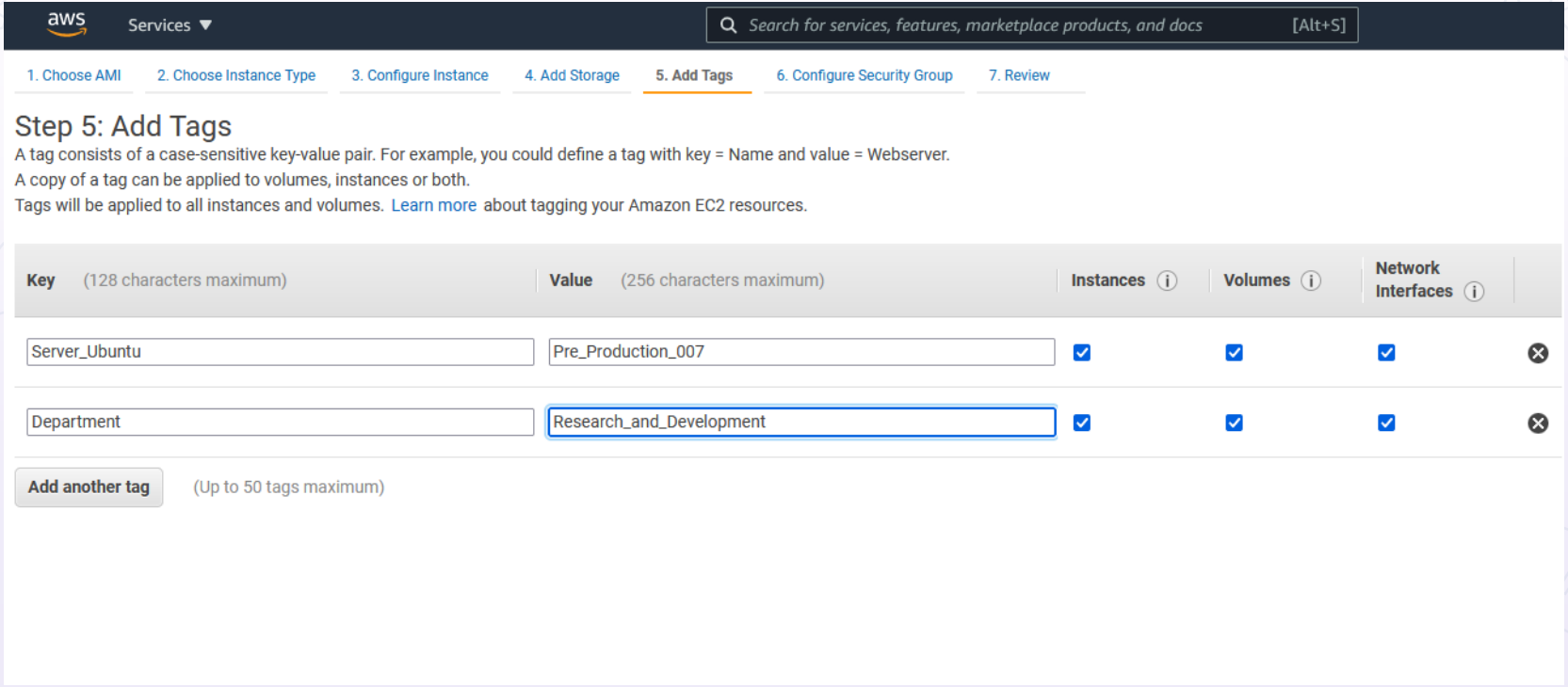
Asset Tagging Methodology



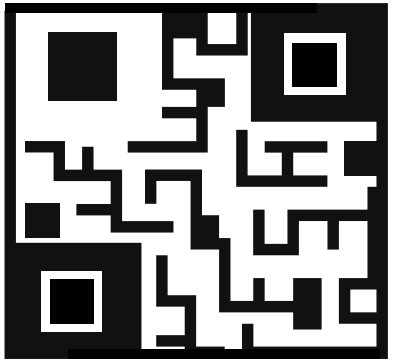
Asset Tagging Process

1. Recognize the asset type and category
2. Assign a unique identification number
3. Decide on the form of asset label required
4. Input the asset and all related metadata into the inventory tracking system
5. Affix (associate) asset or logical tag to the configuration item
6. Employ solid data verification processes

Tagging Cloud Resources



Tagging Physical Resources



PROPERTY OF

SONICAL ELECTRONICS

ADDITIONAL LINE

0001

Implementation and Assessment Policy

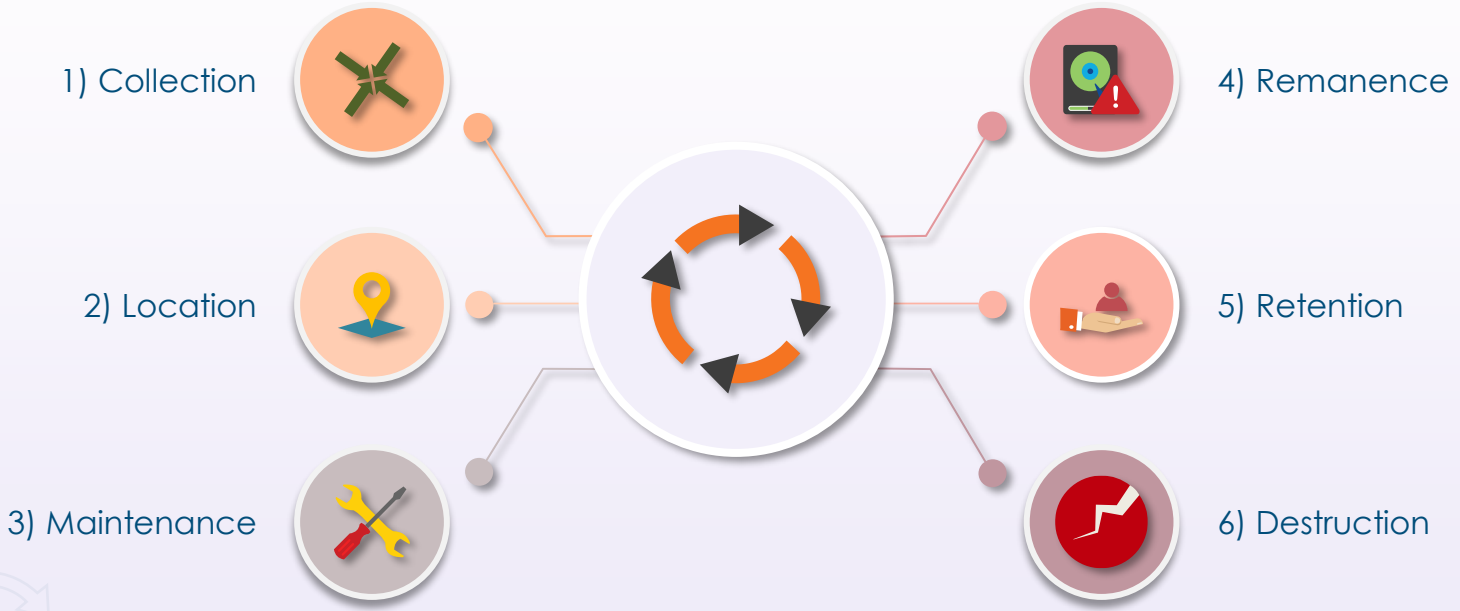
- Policies, specifically security policies, establish a general framework within which to work and a guiding direction to take in the future
- The function of a policy is to classify guiding principles, direct behavior, and offer stakeholder guidance and a security control implementation roadmap
- An information security policy is a directive that outlines how an enterprise plans on protecting its data, applications, and systems
- It helps ensure compliance with legal and regulatory requirements and preserve an environment that sustains security principles
- Policy documents are high-level overview publications that guide the way in which various controls and initiatives are implemented

Policies That Change Based on New Technologies

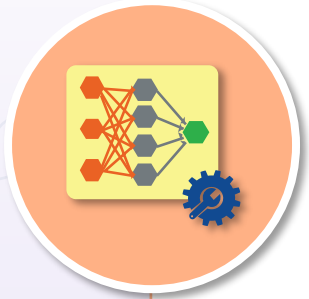
- IoT hardware authentication policies
- User Behavioral Analytics (UBA) policies
- AI and machine/deep learning policies
- Cloud provider interaction policies
- Enterprise mobility management policies

Developing an Information Security Policy

Asset Lifecycle Management



Data Collection



- This is also called "data capture," and there are three key methods through which data can be captured:
  - Data acquisition – the consumption of readily obtainable data that has been produced by an entity outside the organization
  - Data entry – the generation of new data values for the organization by human operators or devices that produce data for the enterprise
  - Data reception – the capture of data generated by devices
    - Examples: SIEM systems, NetFlow collection, logs, industrial control systems, SCADA, and information systems linked to the Internet of Things (IoT)

Data Collection

- Unless data is collected, it cannot be analyzed, matched for patterns, or used for data-driven business decisions
- Only data necessary for organizational or business needs should be collected
- Article 25 of the General Data Protection Regulation (GDPR) mandates that many companies protect data by design and by default
- Enterprises should integrate data protection principles into business activities in the beginning and throughout the data lifecycle

Data Location: Object vs. Block Storage

	OBJECT STORAGE	BLOCK STORAGE
PERFORMANCE	Performs best for big content and high stream throughput	Strong performance with database and transactional data
GEOGRAPHY	Data can be stored across multiple regions	The greater the distance between storage and application, the higher the latency
SCALABILITY	Can scale infinitely to petabyte and beyond	Addressing requirements limit scalability
ANALYTICS	Customizable metadata allows data to be easily organized and retrieved	No metadata

Data Location: Databases

Database type	Use cases
Relational	Traditional applications, ERP, CRM, e-commerce
Key-value	High-traffic web apps, e-commerce systems, gaming applications
In-memory	Caching, session management, gaming leaderboards, geospatial applications
Document	Content management, catalogs, user profiles
Wide column	High-scale industrial apps for equipment, fleet management, and route optimization
Graph	Fraud detection, social networking, recommendation engines
Time series	IoT applications, DevOps, industrial telemetry
Ledger	Systems of record, supply chain, registrations, banking transactions

Data Maintenance

- Maintenance is initiated once the data has been collected
- It involves offering data to points where usage and synthesis happen
- Some models have this as the transition from raw data to information
- Data maintenance is about processing the data without yet deriving any value from it for the enterprise (that is where information becomes knowledge and ultimately wisdom)
- Involves processes such as movement, integration, cleansing, augmentation, and the familiar extract-transform-load (ETL) functions
- Maintenance is the goal of a far-reaching array of data management activities, and because of this, data governance faces many challenges in this area

Data Remanence

- Data remanence is the data, metadata, and artifacts that are leftover after a software deletion process
- This is a known residual risk when handling data during the lifecycle
- To counter the risk of malicious data recovery, physical destruction is always the best choice, however, there are other methods
- There are fundamentally three categories of ways to handle data remanence:
  - Clearing – involves wiping or overwriting the data with zeroes or ones; data may be recoverable under this method
  - Purging – a stronger enduring form that can include methods such as sanitizing or degaussing; data is not considered recoverable by any known methods
  - Destruction – the strongest technique, which includes shredding, pulverizing, burning, and encryption

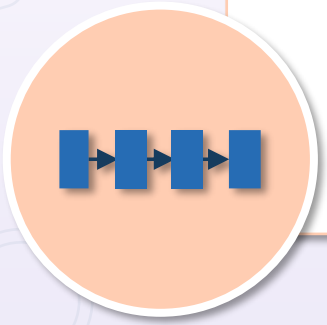
Data Retention

- In some organizations, how long a particular document or record is stored can be just as important as what is being stored
- A data retention policy helps to define what is stored, how it is stored, how long it is stored, and how it is disposed of when the time arrives
- Periodic audits help to ensure that data records or documents are removed when they are no longer needed
- You should implement an automated disk or object storage lifecycle on-premises or in the cloud

Asset Disposal

- In the asset disposal process/phase, plans are developed for discarding system information, hardware, and software and making the transition to a new system
- The information, hardware, and software may be moved to another system, archived, discarded, or destroyed
- If performed improperly, the disposal phase can result in the unauthorized disclosure of sensitive data
- When archiving information, organizations should consider the need and methods for future retrieval

Asset Disposal

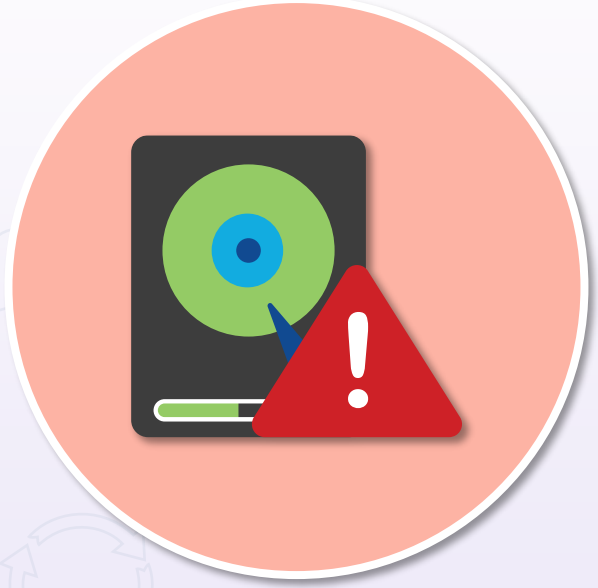


- The disposal activities ensure the orderly termination of the system and preserve vital information about the system so that some or all of it can be reactivated in the future, if necessary
- Emphasis is given to proper preservation of the data processed by the system so that data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access
- The removal of information from a storage medium, such as a hard disk or tape, should be done in accordance with the organization's security requirements

Destruction and Sanitization

- Burning, shredding, pulping, and pulverizing for paper records
- Pulverizing for microfilm or microfiche, laser discs, and document imaging applications
- Magnetic degaussing for computerized data
- Shredding or cutting for DVDs
- Demagnetizing magnetic tapes

Destruction and Sanitization



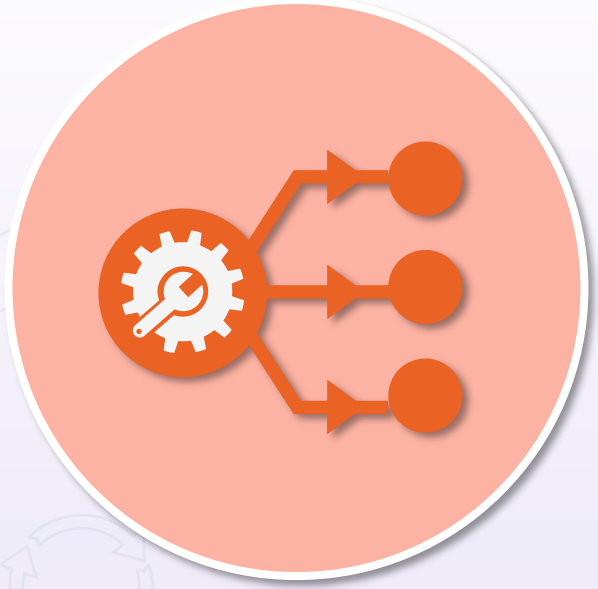
- Degaussing – removing the magnetic field
- Purging – clearing everything off the media
- Wiping – overwriting every sector of drive
  - The DoD 5220.22-M sanitization method is one of the most common sanitization methods used in data destruction software, and in general, is still perceived as an industry standard in the U.S.
- Encryption – encrypting all files before deleting or disposing of media
  - **The only realistic method when storing at a cloud service provider**

Destruction and Sanitization

Example: medical offices should maintain documentation of the destruction of health records, including the following:

- date of destruction
- method of destruction
- description of the disposed records
- inclusive dates
- a statement that the records were destroyed in the normal course of business, and
- the signatures of the individuals supervising and witnessing the destruction

Configuration Management



- The goal of configuration management is to ensure that accurate and meaningful information is readily available regarding the configuration of applications and services along with the configuration items (CI) that support them
- Includes all relationships and dependencies between the CIs
- Objects include hardware, software, networks, sites, vendors, suppliers, and people

Configuration Management

- CM is a governance and systems lifecycle process for ensuring consistency among all assets (configuration items, or CIs) in an operational environment
  - Classifies and tracks individual CIs
  - Documents functional capabilities and interdependencies
  - Verifies the effect a change to one configuration item has on other systems

Configuration Management Practices

- Configuration management practices offer the required data about assets and their configurations, including their interactions with other assets, which assists administrators and managers with
  - problem resolution
  - incident response
  - network component deployment
  - strategy formulation
  - budgetary forecasting, and
  - overall decision-making

Configuration Management Tools

- Directory service utilities and tools
- Diagrams and topologies
- Inventory baselines
- Naming and tagging schemas

Configuration Management System (CMS)

- A configuration management system (CMS) is a set of data, tools, utilities, and processes used to support configuration management
- All information should be tagged and labeled with a common unified schema, preferably using key-value pairs
- This data will populate a database system known as a CMDB
  - Relational databases have been used historically
  - NoSQL/document databases are emerging as a common solution
  - Could leverage a CSP service, such as AWS DynamoDB

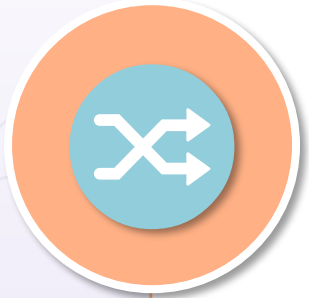
Configuration Management Database (CMDB)

- A configuration management database is not a typical data warehouse
- It plays a critical role in several IT management initiatives, like IT service management (ITSM) and IT asset management (ITAM)
- Helps various IT services to better align with business needs by providing current and accurate data to
  - change and patch management
  - incident and problem management
  - availability management, and
  - release and deployment management

Sample CMDB Schema

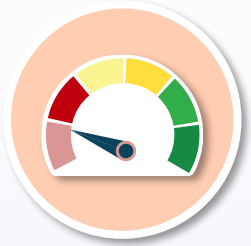
Field (Key)	Value
Collector (_collector)	The name of the collector
Source (_source)	The name of the Source entered when the Source was generated
Source Category (_sourceCategory)	A tag determined by your entry to the Category field when you configure a Source (e.g., sensor, syslog, NetFlow)
Source Host (_sourceHost)	A fixed value determined by the hostname you enter in the Hostname field
Message Count (messageCount)	A unique sequence number (per Source) added by the Collector when the message was received

Change Management



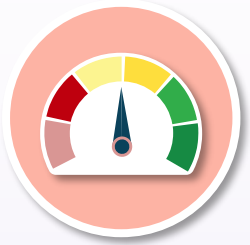
- Change management is also called the "change control practice"
- The goal is to maximize the amount of successful service and product changes
- Should make certain that risks have been adequately assessed, authorized, and managed with a change schedule
- Operates with the configuration database to track all possible dependencies and repercussions of changes
- Involves a change log or change database

Types of Changes



Standard

- Low-risk changes
- Pre-authorized and well-documented
- Can be automated
- Service requests that don't need additional authorization
- Example: changing directory password



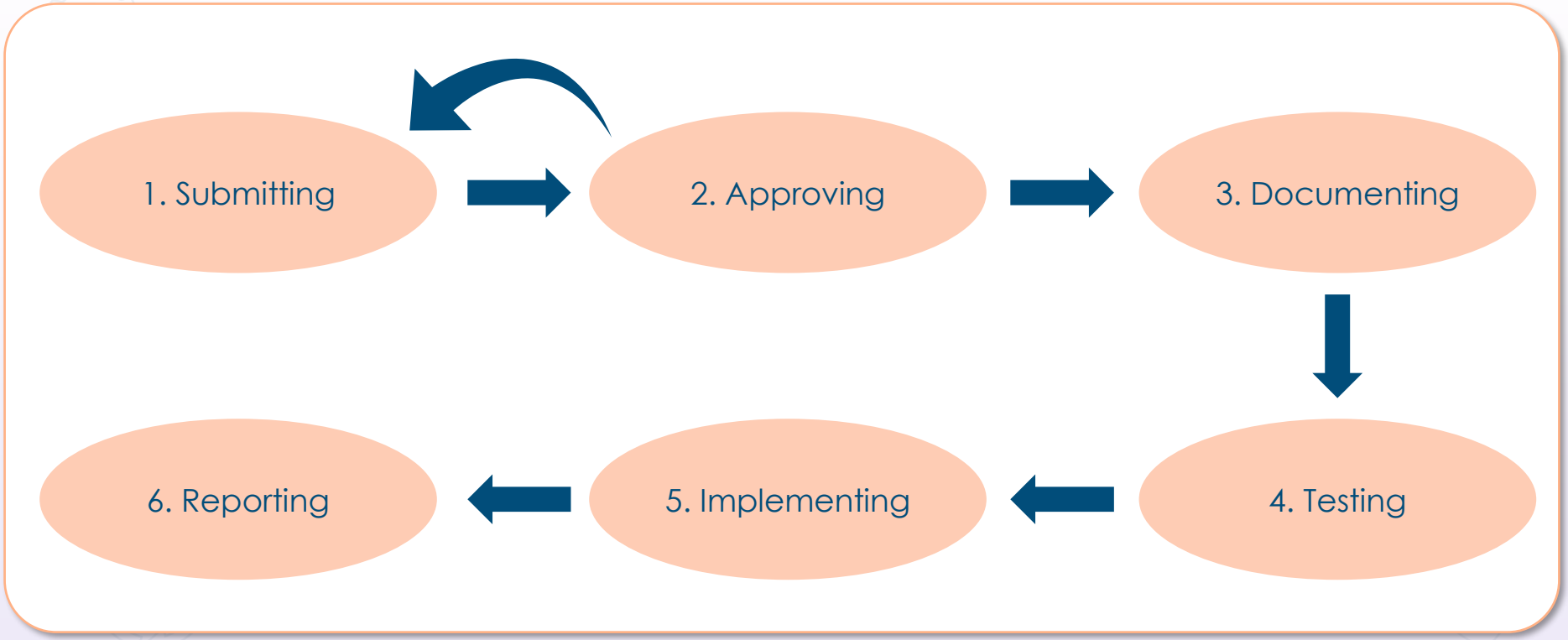
Normal

- Changes follow a specific process for scheduling, assessment, and authorization
- They are lower risk, but they do go through an approval process
- Example: onboarding a new phone or laptop; installing an application

Emergency

- Changes that must be implemented immediately
- Often a result of problem management or after-action reporting
- May involve escalation or an emergency advisory board if the number of resources or disruptions is significant

Change Management Lifecycle



1. Submitting

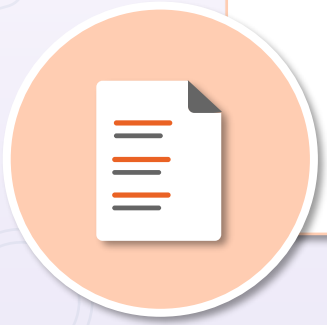
The proposed change is analyzed and validated. If necessary, the submitter may be required to provide more information before it is approved or escalate the change to a higher authority

2. Approving

The proposed change request should first be delivered to the individual or group responsible for change management in the organization

3. Documenting

After approval, the change needs to be inputted into a changelog or configuration management database (CMDB). This log or database must be updated regularly as each change progresses through the various phases

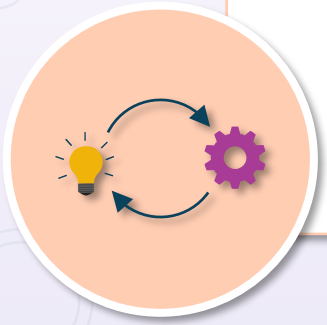


4. Testing

Before implementing the change, there may need to be a formal testing and verification process. This allows for modifications to be made if any issues arise. The testing group can also determine if any other processes are affected by the change

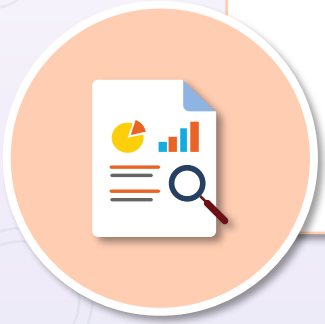
5. Implementing

After the change is tested and approved, it can be deployed based on a schedule that has been determined. The schedule needs to document the projected phases of the change and define the milestones for the change process

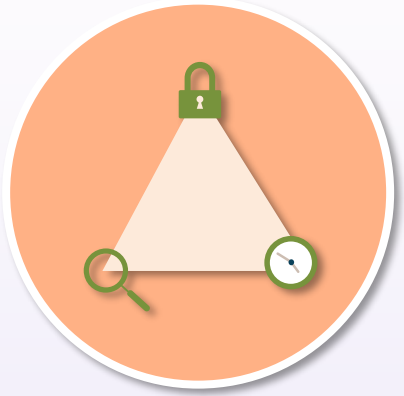


6. Reporting

After the change has been implemented, a full report should be submitted to management. If there are any negative consequences to implementing the change, this should trigger an iterative move to an earlier phase of the lifecycle



Systems Security Certified Practitioner (SSCP) Bootcamp



Session 2

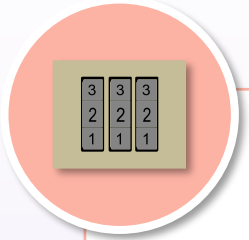
Systems Security Certified Practitioner (SSCP)

Understanding and Applying Cryptography

Overview of Cryptology

Cryptography

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



Cryptanalysis

- The study and the practice of exploiting weaknesses in cryptographically protected systems
- Analysts actively explore
  - brute force attacks
  - implementation attacks, and
  - side-channel attacks

Cryptographic Services

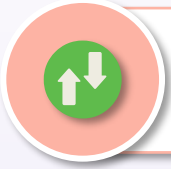
- Confidentiality
  - Hiding the data at rest, in transit, and in use from unauthorized entities
  - Often involves a system that converts plaintext data into ciphertext
- Integrity
  - Ensures the data has not been altered while at rest or in transit
  - Often involves attaching a cryptographic hash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

Cryptographic Services

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

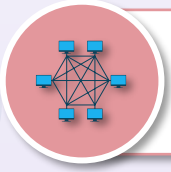
Encryption Occurs at Different Levels

Application layer – example: PGP, GnuPG (GPG)



Session layer – example: SSL/TLS

Network layer – example: IPsec for IPv4 and IPv6



Data link layer – example: L2TP, MACsec

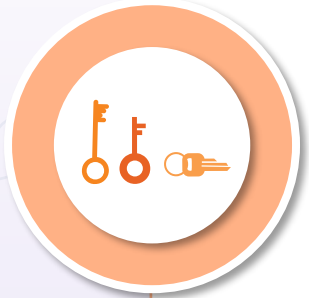
Ciphers

- A cipher is an algorithm used for encryption and decryption that outlines the procedure to follow 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

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 4,096 bits
- Keys enable cryptographic encryption, digital signatures, hash functions, and message authentication codes

Common Key Types



- 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 process
  - Never stored in memory or retained

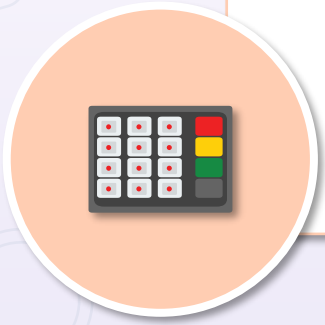
Key Management

- 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

Reasons and Requirements for Cryptography

- Cryptography is used to protect data sensitivity
  - Data in transit, in use, and at rest
- Algorithms are used to protect data in block and object storage
- Databases use cryptosystems to protect data, clusters, and tables
- It is commonly used to protect personally identifiable information (PII), intellectual property (IP), and protected health information (PHI)
  - Confidentiality (privacy), integrity, and origin authentication

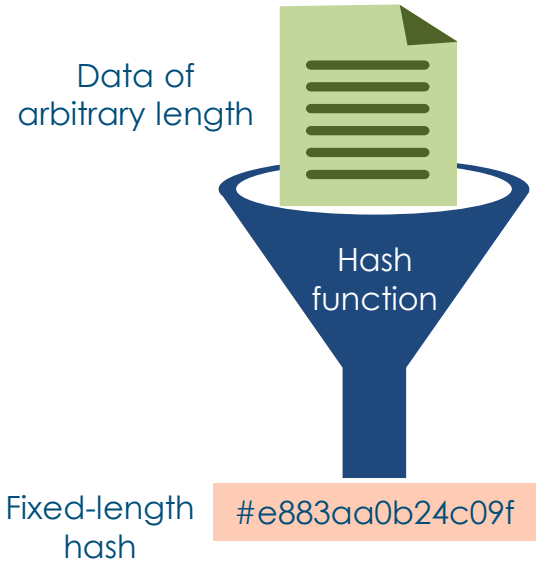
Reasons and Requirements for Cryptography



- Cryptosystems are also put in place to obtain accreditation or certification to an audit for regulatory and industry best practices
  - Payment Card Industry Data Security Standards (PCI-DSS), HIPAA, Sarbanes-Oxley, GDPR
- International Organization for Standardization (ISO) and DoD are other potential mandates

Cryptographic Hashing

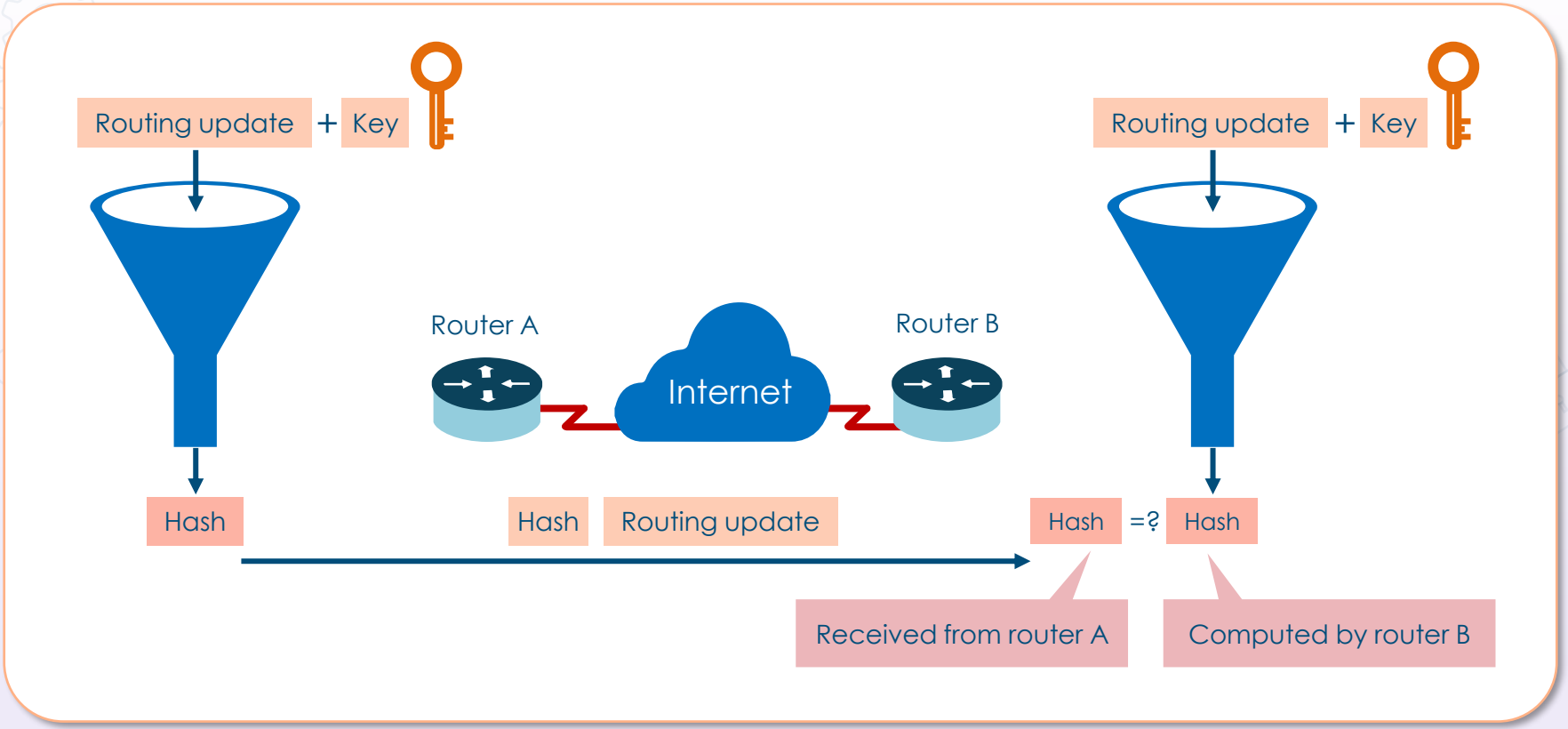
- Converts data of any input size to a fixed-length string called a hash value, message digest, or fingerprint
- An advanced version of a simple checksum
- A one-way mathematical function that produces a digest of 128 to 512 bit
- Birthday paradox and avalanche effect
- Used in authentication, data integrity,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



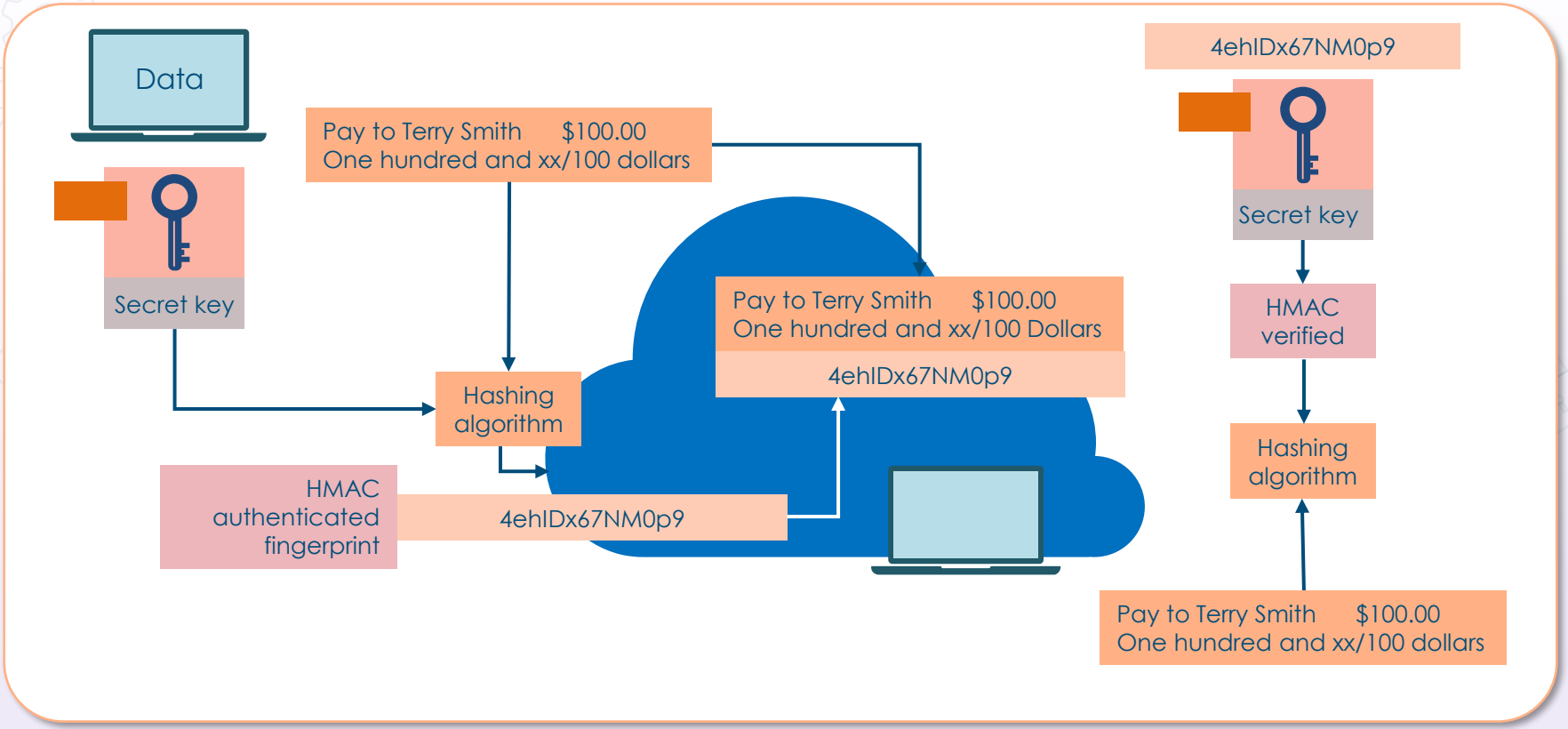
Cryptographic Hash Functions

- MD5 (128-bit digest is produced)
- SHA-1 (160-bit digest is produced)
- SHA-2 (SHA256 or SHA512) and SHA-3 (224-512)
- RIPEMD (128, 160, 256, and 320-bit versions)

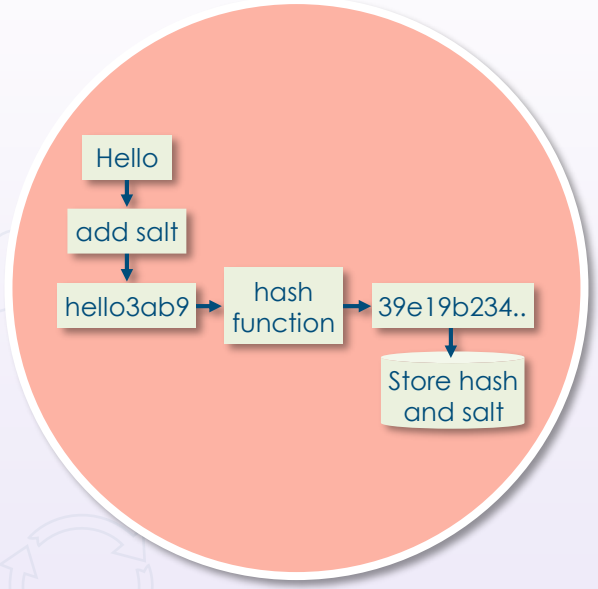
HMAC for Origin Authentication and Integrity



HMAC for Origin Authentication and Integrity



Salting



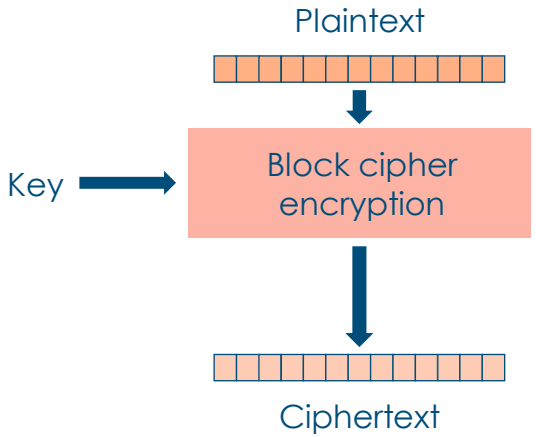
- Salting is an additional pseudo-random value added to the end of the password to create a stronger hash value
- A salt is added to the hashing process to force their uniqueness, increase their complexity without increasing user requirements, and mitigate password attacks, like hash tables
- This adds a layer of protection against brute force attacks and rainbow tables
- The additional value is referred to as a "salt"

Symmetric Key Cryptosystems

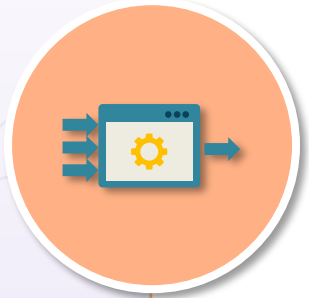
- Uses the same key to encrypt and decrypt
- Efficient, fast, and handles high data rates of throughput
- Computationally inexpensive
- Has shorter key lengths (40 to 512 bits)
- Key management is more complex
- More difficult to secure than other systems
- No origin authentication
- Does not scale well

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



Stream Ciphers



- Operate on a continuous stream of 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
  - cryptographic hashing
  - FISH
  - CryptMT, and
  - RC4

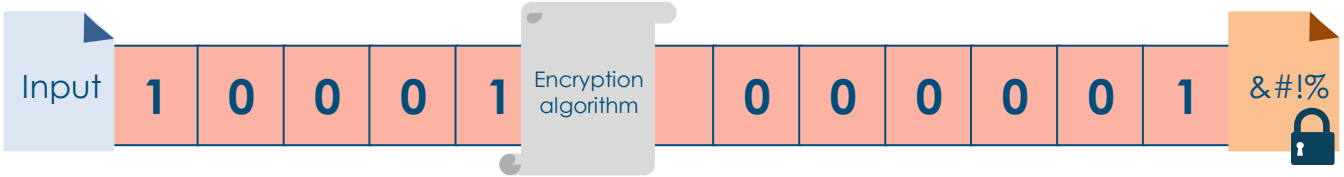
Stream Cipher Example

- 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)

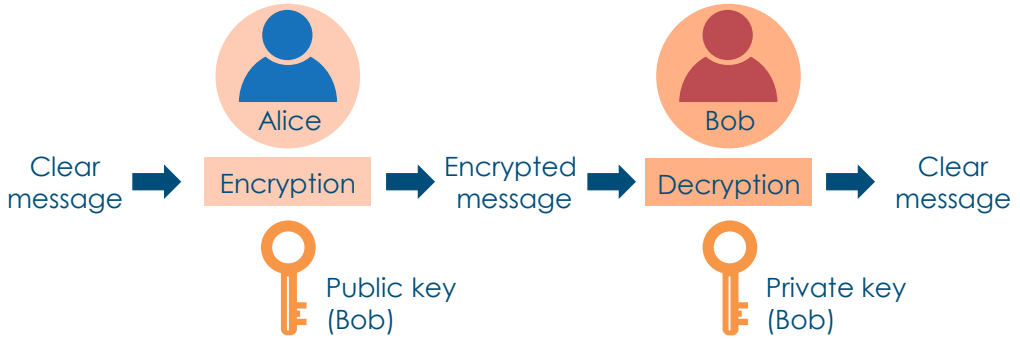


Asymmetric Key Cryptosystems

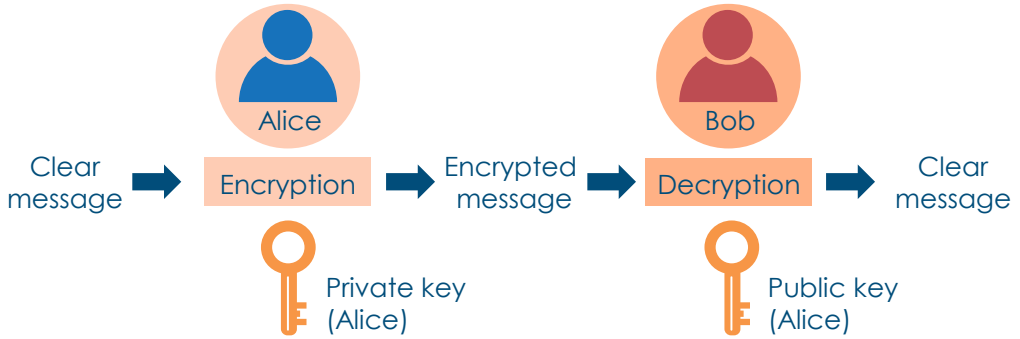
- Uses a mathematically related pair of a public and private key
- If one is used to encrypt, the other is used to decrypt
- Allows for efficient key management
- Great for digital signatures and key exchange
- Highly scalable with a public key infrastructure
- Employs longer key lengths than symmetric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

Asymmetric Key Use Cases

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

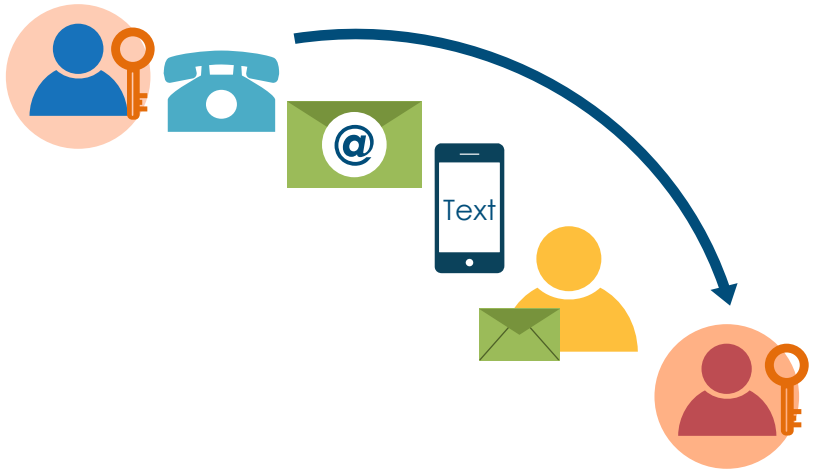


- Origin authentication
  - Encrypt with private key
  - Decrypt with public key

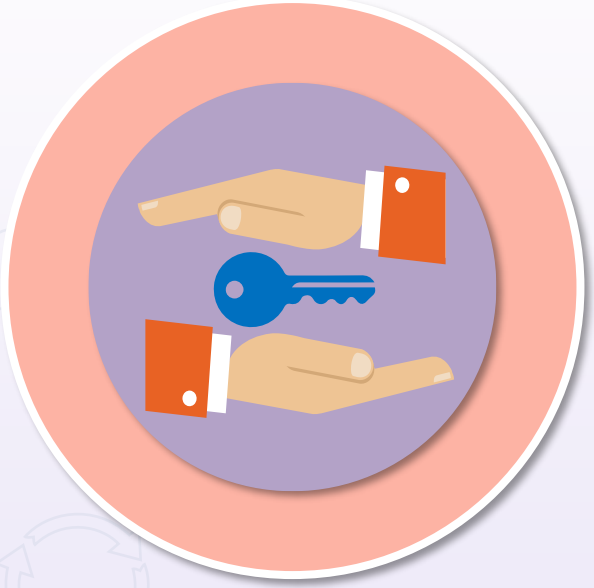


Key Exchange

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

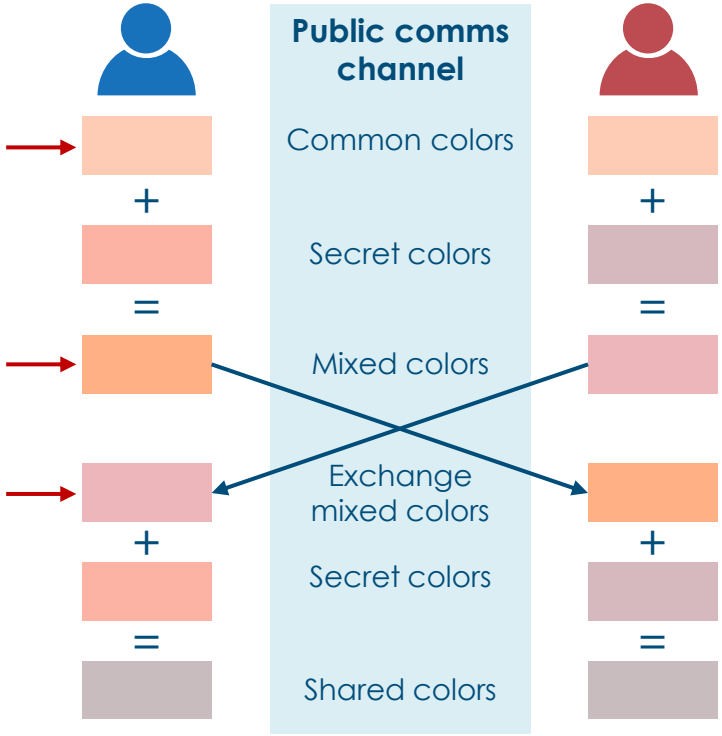


Diffie-Hellman Key Exchange



- 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
- **The RSA algorithm can sign public-key certificates, whereas the Diffie-Hellman key exchange cannot**

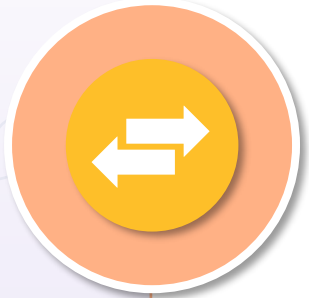
Diffie-Hellman Exchange



Note: attacker only sees these colors, and thus cannot arrive at the shared secret

Note: assume colors are hard to unmix, which means the secret colors are secure

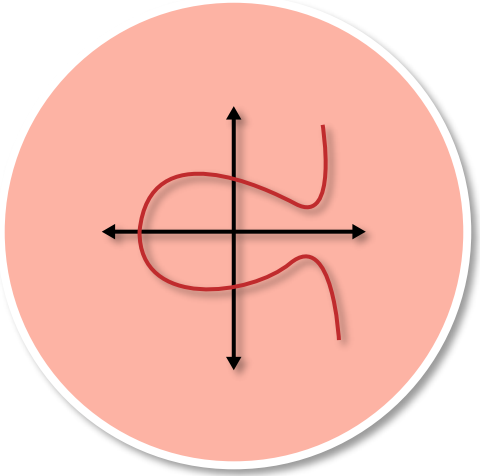
Diffie-Hellman Modes



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

Elliptic-Curve Diffie–Hellman

Recommended

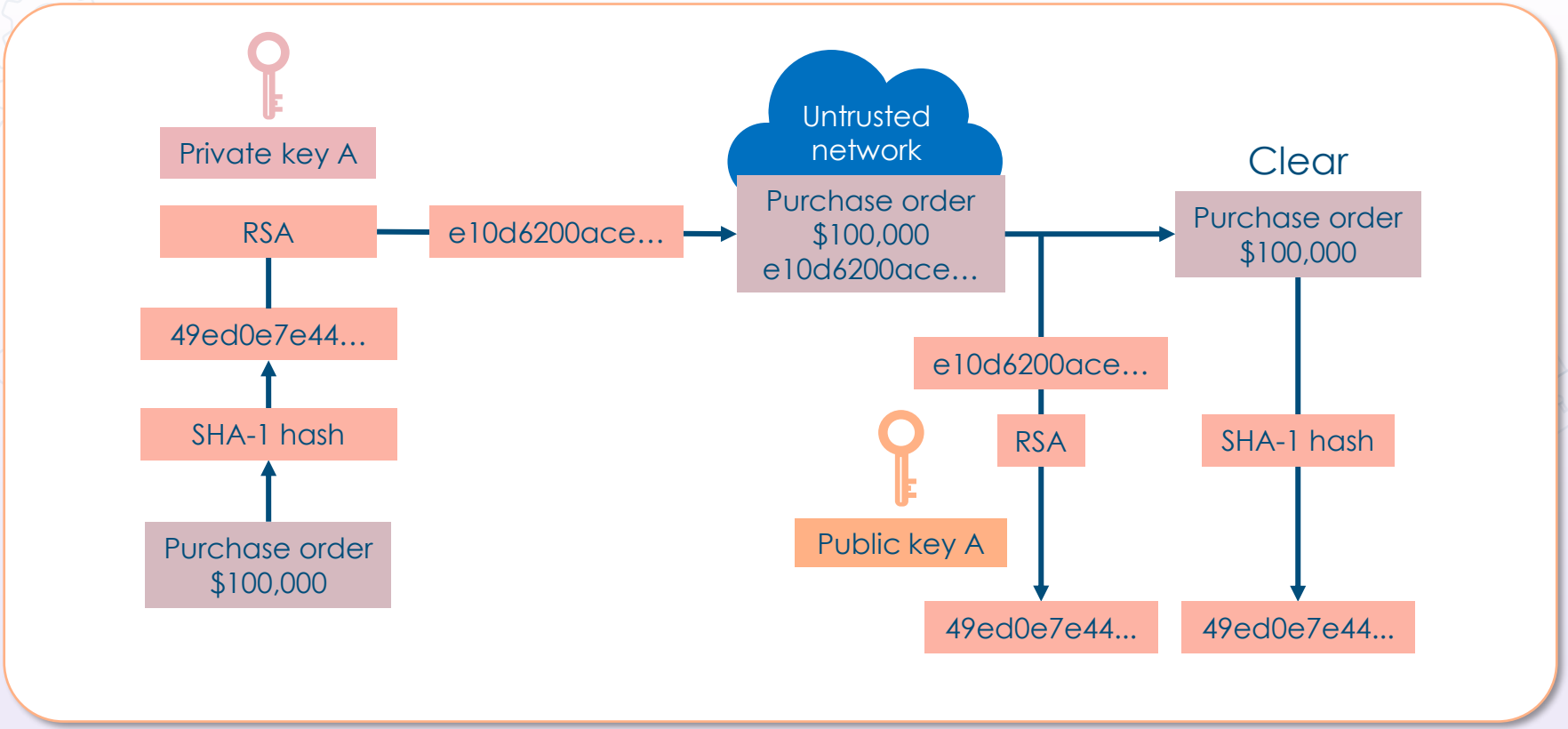


- Based on rich math functions of values plotted on an elliptic curve
- Uses smaller keyspaces while offering superior strength
- 256-bit elliptic key = 3072-bit standard key
- Excellent for mobile devices and IoT with limited memory and processing power
    - Common use cases:
        - digital signatures
        - key exchange, and
        - IPsec and TLS

Digital Signatures

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

Digital Signatures



Digital Certificates

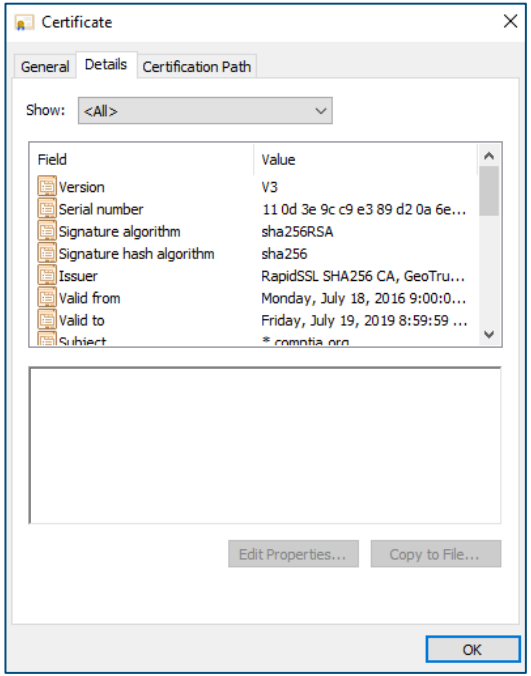
- A digital certificate is a form of file used to bind cryptographic key pairs to entities such as individuals, web sites, or organizations
- If public trust is needed, then a trusted Certificate Authority (CA) will assume the role of a third party to validate, identify, and associate them with cryptographic pairs using the digital certificates

Digital Certificates

- The key pair consists of a public key and a private key
- The public key is included in the certificate, while the private key is stored in a secure fashion
- The owner of the private key can then use it to sign documents, and the public key can be used to verify the validity of those signatures
- A common format for digital certificates is based on the X.509 standard, which consists of the following:
  - a public key
  - a digital signature
  - other metadata about the entity linked to the certificate, such as a serial number and the subject (alternative) name, and
  - information about the issuing CA

X.509v3 Digital Certificates

- 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 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 a green padlock

Cryptanalysis

- Cryptanalysis is the study and practice of exploiting weaknesses in communication protocols and cryptosystems
- Most known methods, like brute force, are ineffective on most modern cryptographic algorithms due to
  - lack of time
  - lack of computing power, and
  - good key management and life cycles
- Most weaknesses are found in the implementation and key management as opposed to the algorithm itself

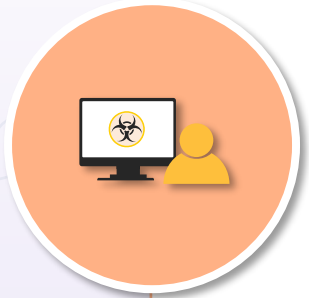
Classical Cryptanalysis

- Classical cryptanalysis typically involves 2 disciplines:
  - mathematical analysis that involves analytical attacks that exploit the internal structure of the encryption methods, and
  - brute-force analysis, which treats the algorithm as a black box and tries all possible keys in the keyspace

Side-channel Attacks

- A common side-channel attack measures the electrical power consumption of a processor operating on a secret key
- The power trace is used to determine "0s" and "1s" and ultimately give information about plaintext or keys
- Typically needs physical access, such as smart card

Attacking RSA



- Protocol attacks – exploit weaknesses in the way RSA is used
  - Padding and proper implementation mitigate these
- Mathematical attacks
  - Best example is factoring the modulus
  - Although 1024-bit RSA is adequate, a modulus of 2048-4096 bits is highly recommended today
- Side-channel attacks
  - Information about the private key is leaked via physical channels, such as power consumption (SPA) and timing behavior

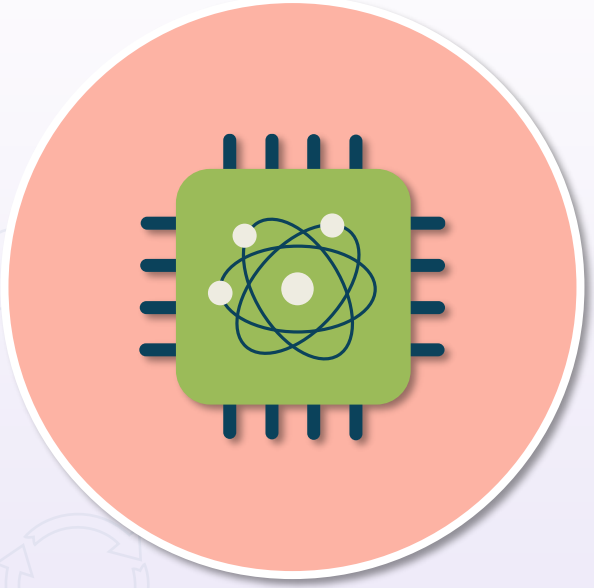
Perfect Forward Secrecy (PFS)

- 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
- Using keys generated from the original access key as opposed to the original at a CSP is forward secrecy

Lightweight Cryptography

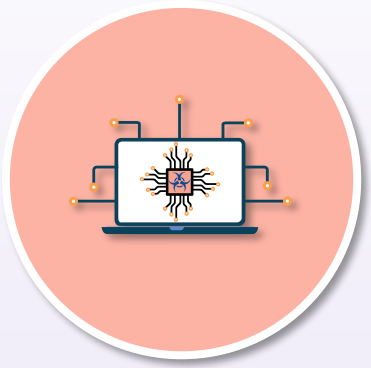
- Most current cryptographic algorithms were designed for desktop/server environments
- There are several emerging areas, such as sensor networks, healthcare, distributed control systems, and IoT, in which highly-constrained devices are interconnected
- They are usually communicating wirelessly and working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

Quantum Computing



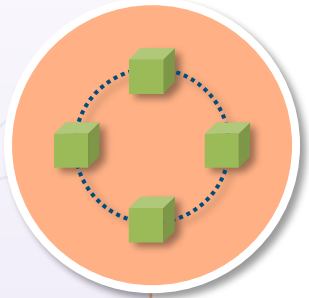
- Personal computers use bits (1s and 0s)
- Quantum computing machines use qubits
- Qubits are typically subatomic particles, like protons or electrons
- Derives its power from the fact that qubits can represent numerous combinations of 1 and 0 at the same time
- The ability to be in multiple states simultaneously is called superposition
- Cryptographers are working on post-quantum computing schemes to counter quantum computing in the future

Homomorphic Encryption



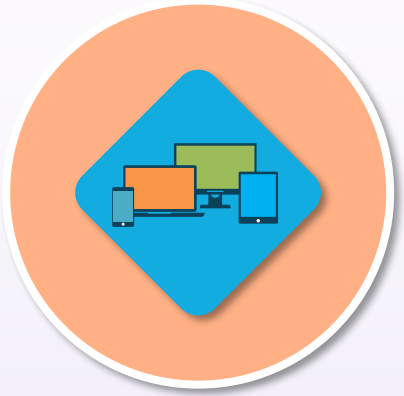
- Can protect data-in-use
- Data remains encrypted while processed
- Commonly uses a public/private key pair
- Uses algebraic operations on the ciphertext
- Future use case is with cloud service providers

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, and
  - that transaction must be stored in a block and given a hash

Systems Security Certified Practitioner (SSCP)



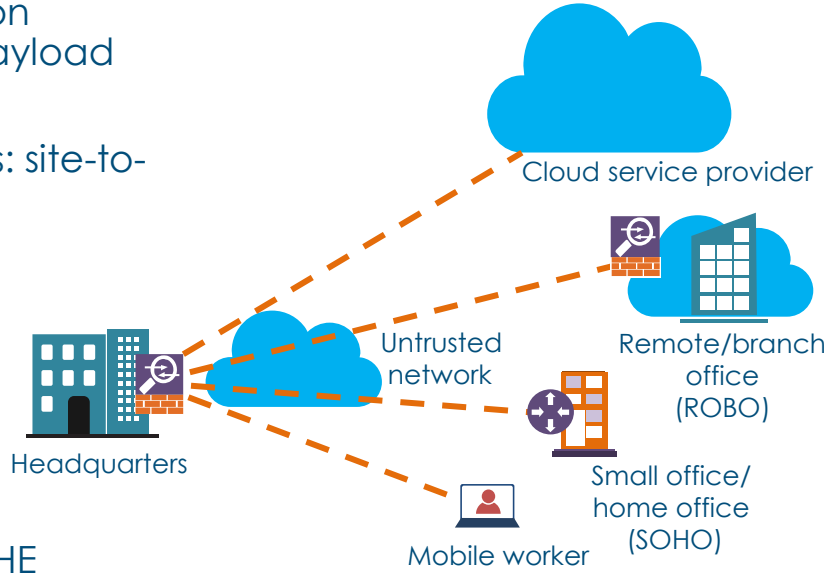
Secure Protocols and Public Key Infrastructure (PKI)

Overview of IPsec

- IP Security (IPsec) offers security services to traffic crossing untrusted networks, like the Internet, between two or more trusted devices or networks
- IPsec VPNs can also be used to protect management traffic as it crosses an organization's intranet and between front-end and back-end services
- IPsec is also popular when connecting to cloud service providers
- IPsec is optional with IPv4 and native to IPv6 using extension headers (AH and ESP)

IPsec

- IPsec is a cryptography-based VPN solution involving two main protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP)
- There are two basic VPN deployment types: site-to-site (S2S) and remote-access VPNs
- IPsec security features are
  - confidentiality (3DES, AES-128/256)
  - data integrity (SHA1, SHA2/3)
  - origin authentication with pre-shared keys or RSA and ECDSA signatures, and
  - anti-replay protection
- Key management with IKEv1/2, DHKE, ECDHE
- Operates in tunnel or transport modes



IPsec Security Profiles (Policies)

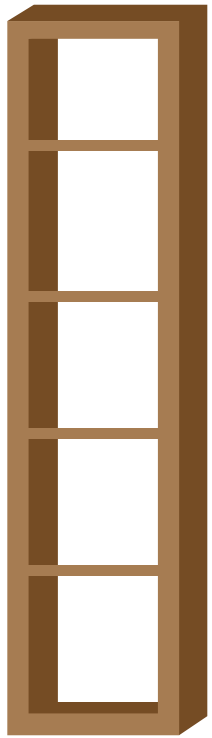
IPsec protocol

Confidentiality

Data integrity

Origin authentication

Key management



ESP | ESP +AH | AH

DES | 3DES | AES

MD5 | SHA-1 | SHA-2

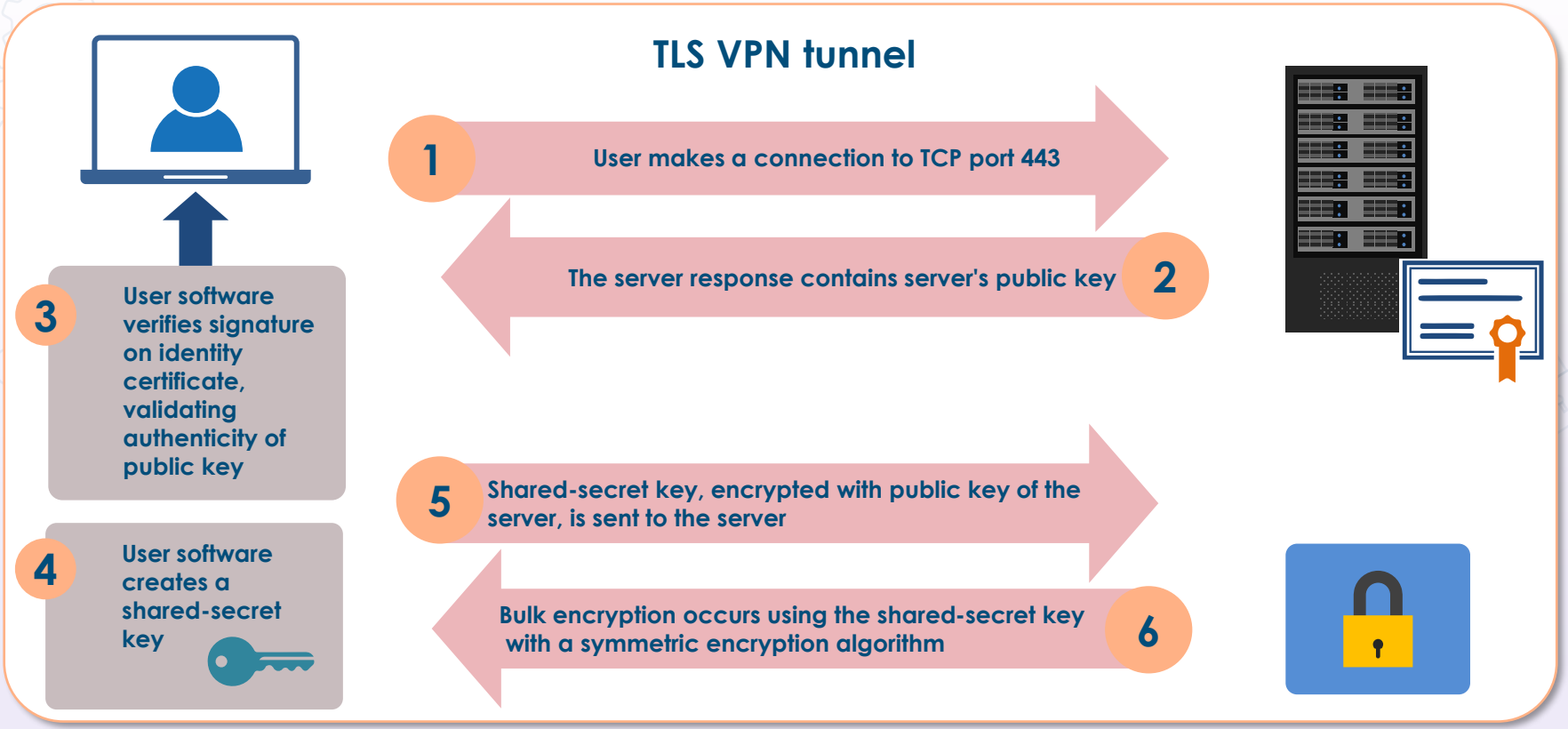
PSK | RSA | ECDSA

DH | ECDH | IKE | IKEv2

Overview of Transport Layer Security

- SSL/TLS is the most ubiquitous certificate-based peer authentication in use on the Internet (HTTPS)
- Transport Layer Security (TLS) is standardized by IETF
- TLS 1.3 is the most recent published version
- It is also used with SMTP, LDAP, and POP3
- The only mandatory cipher suite includes RSA for authentication, AES for confidentiality, and SHA for integrity and digital signatures
- The handshake protocol is a highly extensible mechanism for providing additional security features

Transport Layer Security



HTTPS

- It is basically HTTP over SSL/TLS
- The most widely used protocol on the Internet for any secure commercial transaction, financial service, contract, agreement, file transfer protection, and voice or video service
- Mozilla is deprecating non-HTTPS secured search results in order to hasten the global adoption of HTTPS
- A cryptographic key exchange happens when you first connect to a secure web site and all ensuing activities on the web site are encrypted

S/MIME

Secure/Multipurpose Internet Mail Extensions

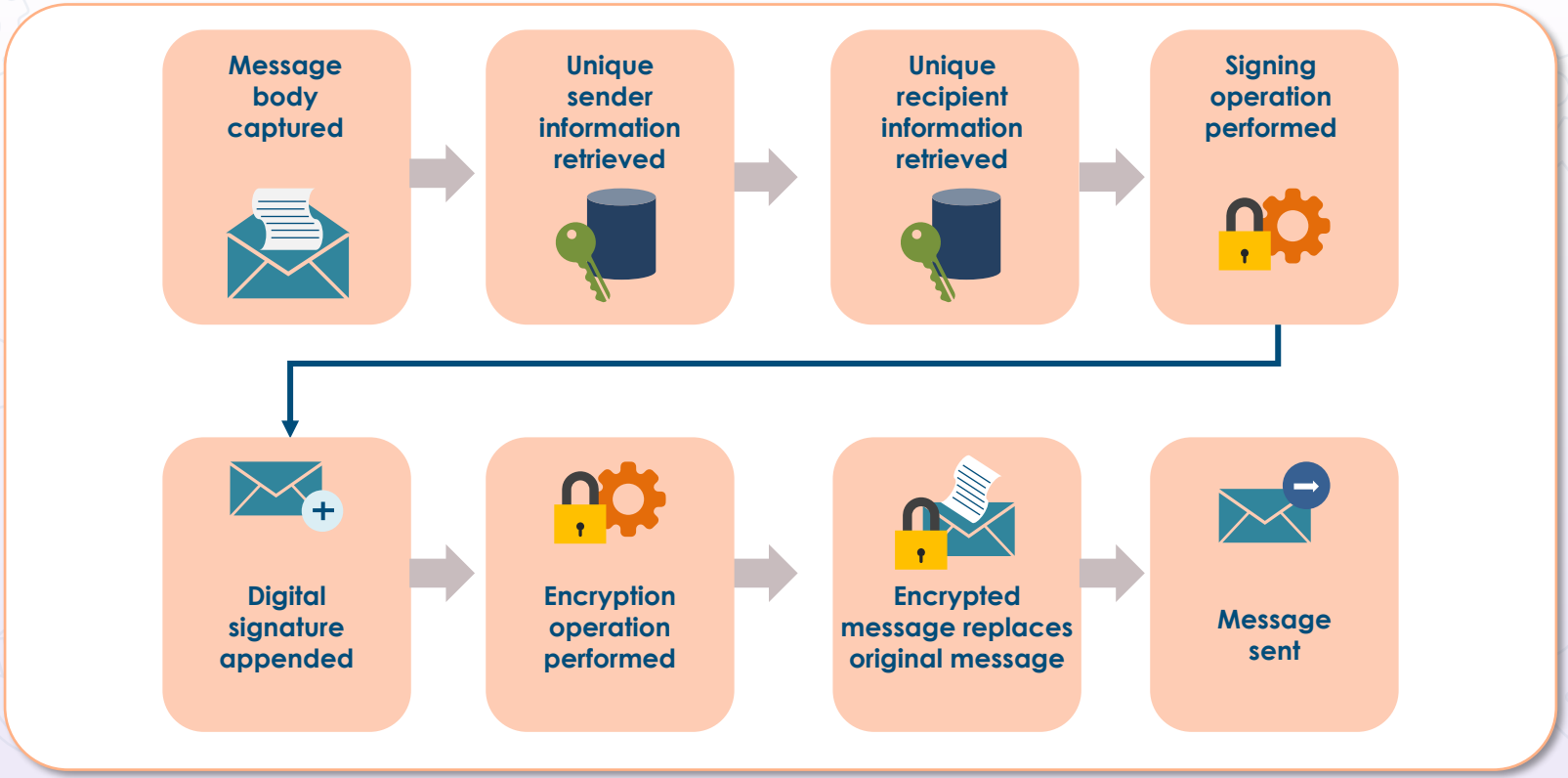
SMTP is not natively secure

S/MIME v3 has become the standard for email message security

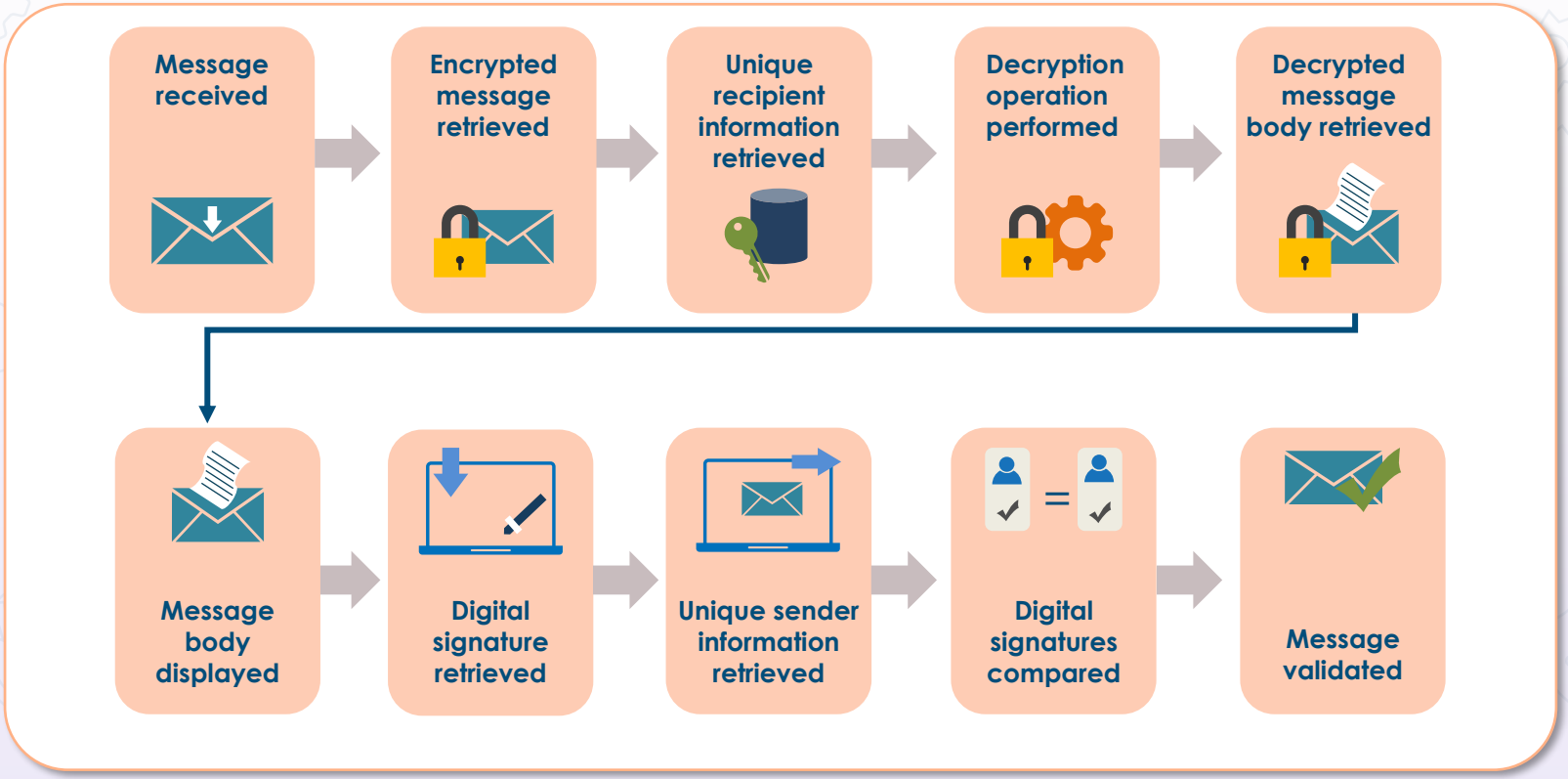
Provides digital signatures and email message encryption

Digital signatures are the most common S/MIME service

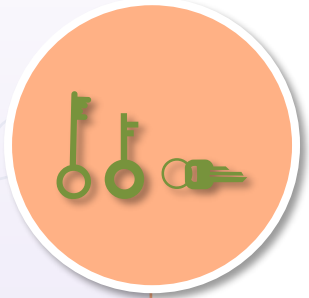
Sending an S/MIME Email



Receiving an S/MIME Email



DomainKeys Identified Mail (DKIM)



- DKIM empowers an organization to take responsibility for email messages in transit by being the handler of the message, either as its originator or as an intermediary
- Their reputation is the basis for evaluating whether to trust the message for further handling, such as delivery
- DKIM technically provides a method for validating a domain name identity that is associated with a message through cryptographic authentication
- DKIM attaches a new independent domain name identifier to a message and uses cryptographic techniques to validate authorization for its presence

Key Management Concepts

- Only authorized persons should be involved in the key management life cycle
- Symmetric systems are more vulnerable to poor key management as rotation is often done manually
- Long-term storage is often done with hardware security modules (HSM), like Thales SafeNet Luna
- Key rotation schemes should be automated or managed with HSM, cloud-based HSM, or key management services (KMSs)
- Keys can be composed with password managers, pseudo-random key generation tools, or HSM modules

Key Exchange Methods

- Phone
- Email or secured email
- Text
- Couriers
- Diplomatic bags
- Asymmetric key exchange algorithms
- RSA – key exchange
- Diffie-Hellman key exchange (DHKE)
- Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)

Key Revocation and Escrow

- Asymmetric key revocation is easier with public or enterprise PKI using certificate revocation lists (CRL) and Online Certificate Status Protocol (OCSP)
- Symmetric keys need an HSM or Cloud KMS
- Key escrow is an arrangement with an authorized third-party where keys needed to decrypt encrypted data are held and only provided under certain pre-defined circumstances

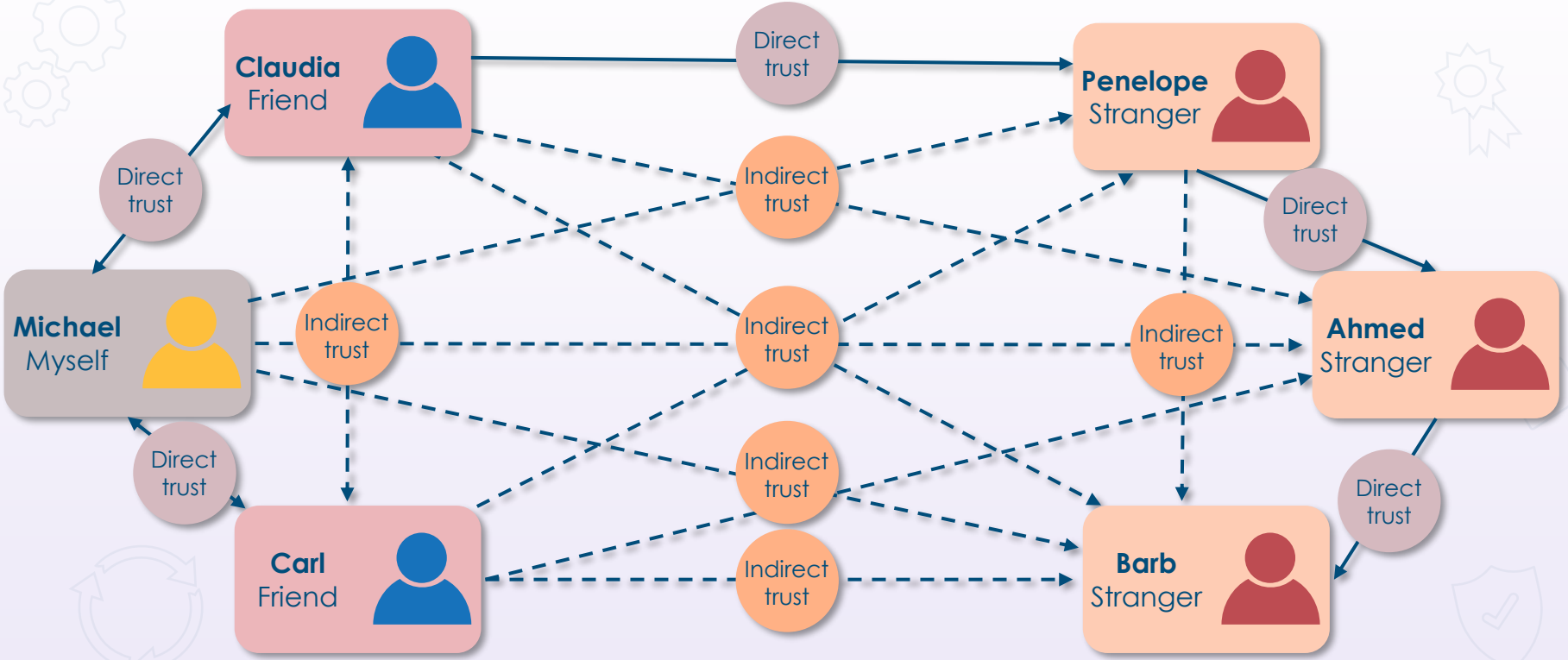
Key Disposition

- Key destruction removes an instance of a key in one of the allowable key forms at an explicit location
  - Information may still exist at the location, from which the key may be feasibly reconstructed for subsequent use
- Key deletion removes an instance of a key and any information from which the key may be reconstructed from its operational storage/use location
  - Instances of this key may continue to exist at other locations (e.g., for archival purposes)
- Key termination completely removes all instances, and information of the key are completely removed from all locations
  - It is impossible to regenerate or reconstruct the key (other than through a restore from a backup image)

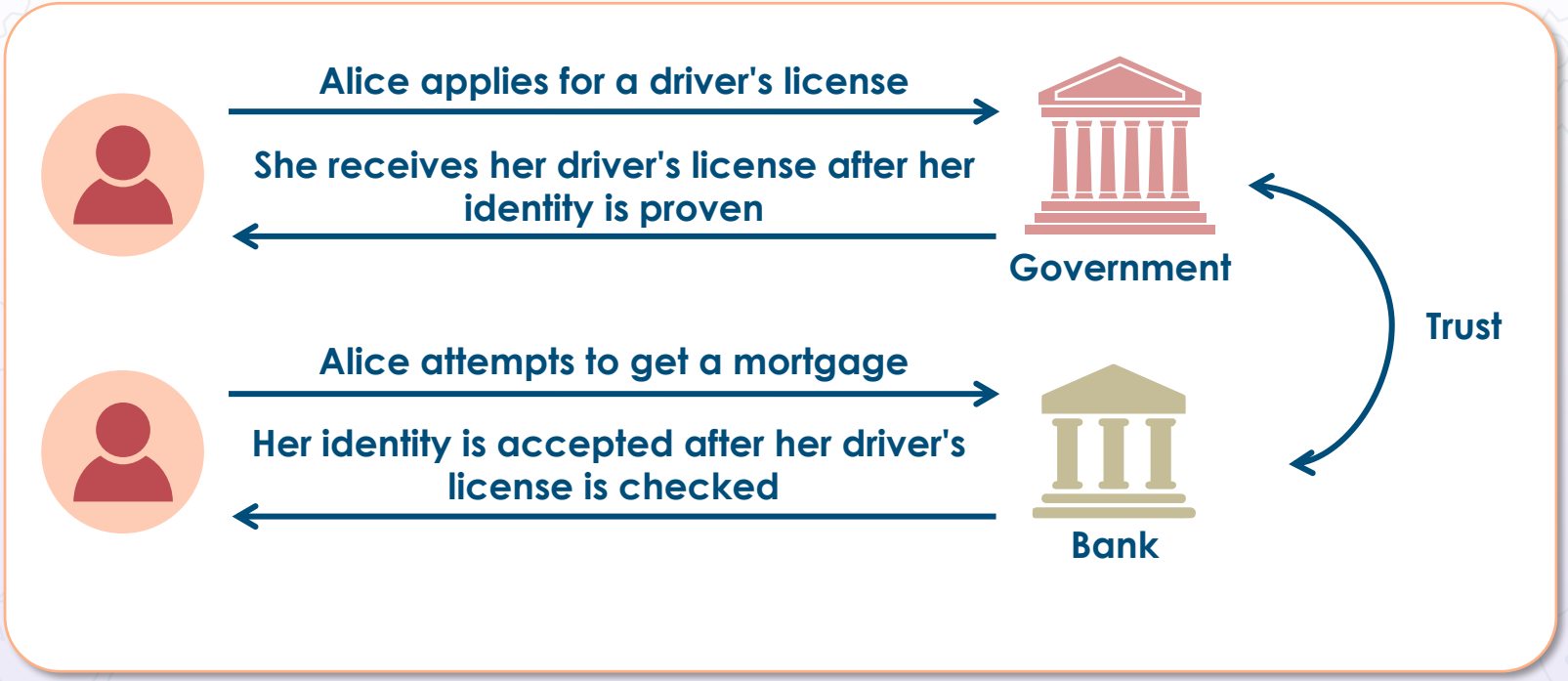
Web of Trust

- The web of trust concept was first put forth by PGP creator Phil Zimmermann in 1992
- It is a concept used in Pretty-Good-Privacy (PGP), GnuPG, and other OpenPGP-compatible systems to establish the authenticity of the binding between a public key and its owner
- Its decentralized trust model is an alternative to the centralized trust model of a public key infrastructure (PKI), which relies exclusively on a certificate authority (or a hierarchy of such)
- There are many independent webs of trust, and any user (through their public key certificate) can be a part of, and a link between, multiple webs

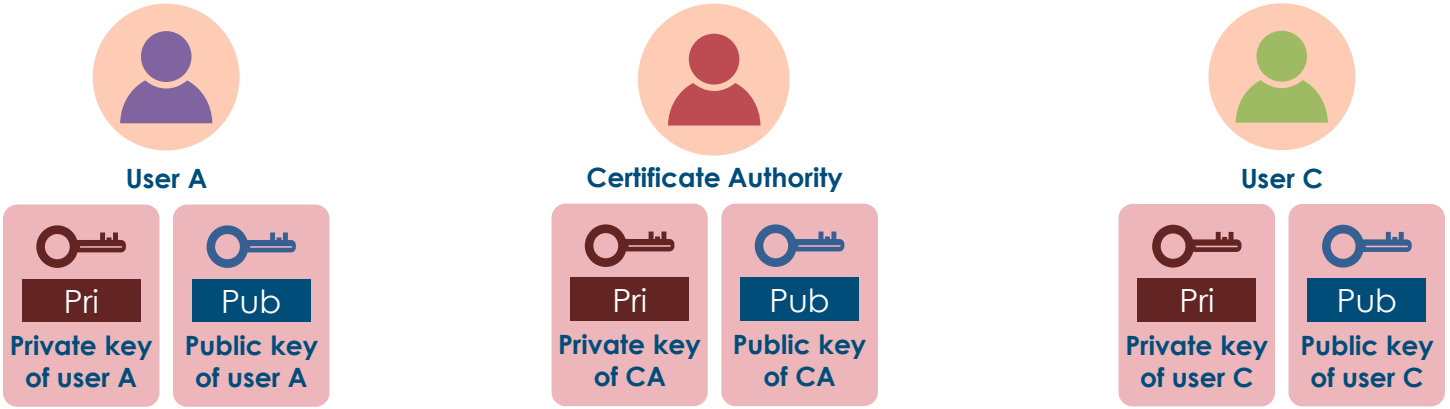
Web of Trust


Claudia
Friend
Direct trust
Penelope
Stranger
Direct trust
Indirect trust
Direct trust
Michael
Myself
Indirect trust
Indirect trust
Indirect trust
Ahmed
Stranger
Direct trust
Indirect trust
Direct trust
Carl
Friend
Indirect trust
Barb
Stranger

Trusted Third Parties



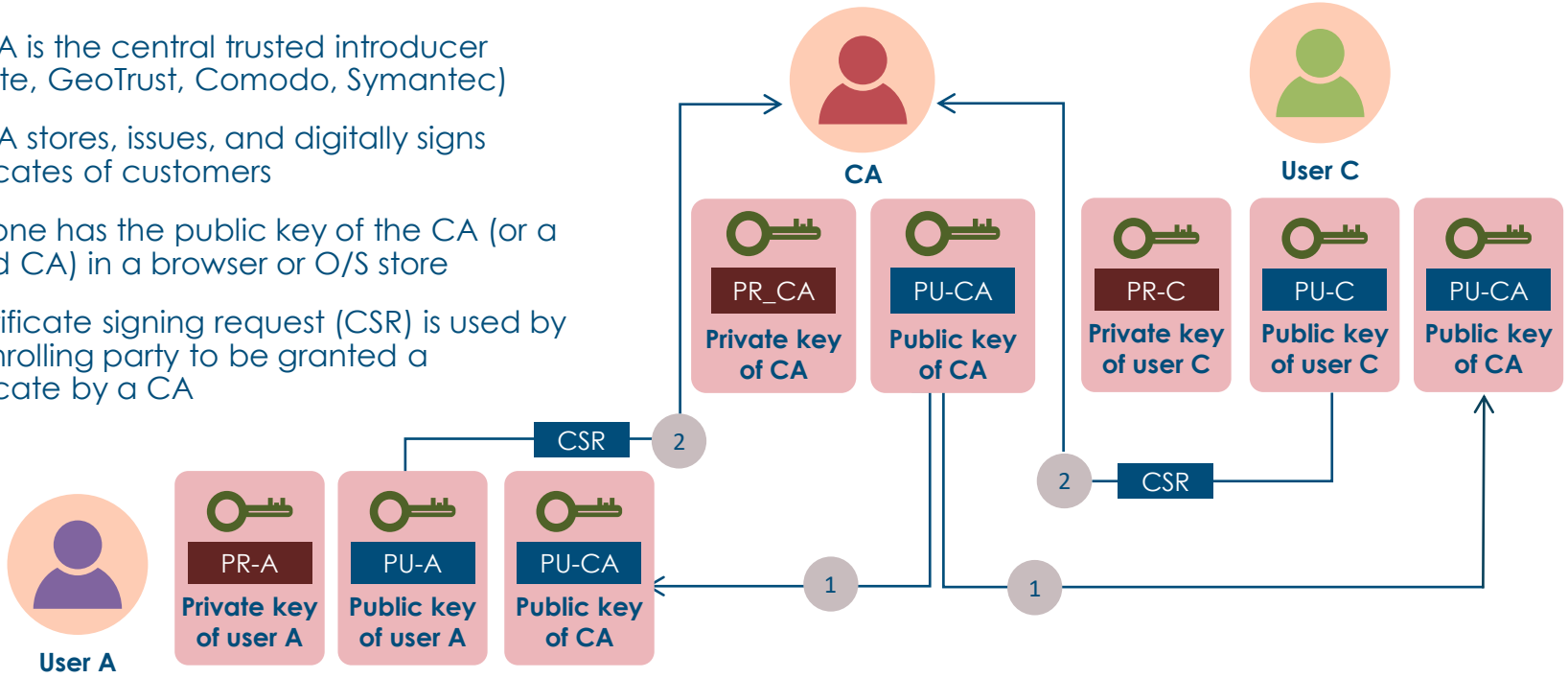
Public Key Infrastructure (PKI)



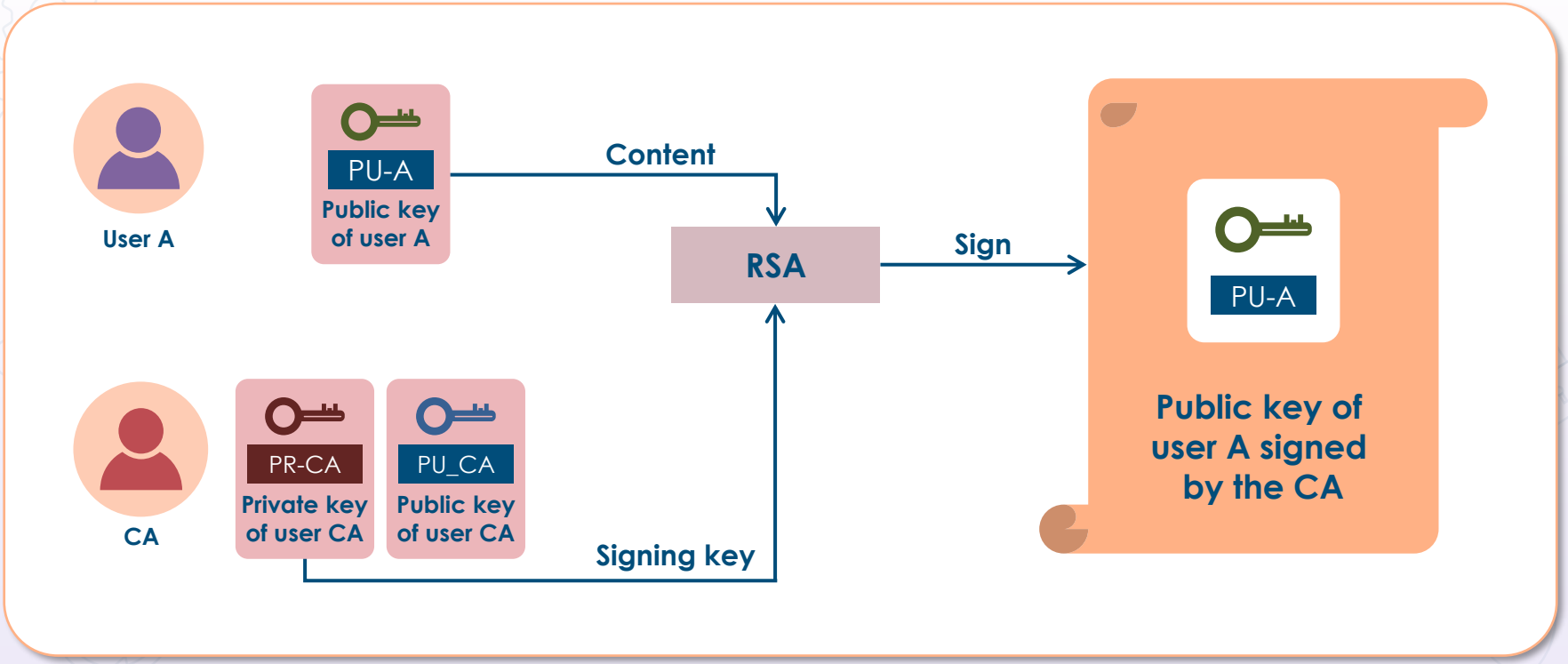
- PKI is a scalable binding of a public key with an entity identity
  - A person, system, or organization
- Digital certificates are registered and issued by a certificate authority (CA)
  - Can be automated or manual
  - The CA may also generate the key pair (usually RSA) for the requesting party

Public Key Infrastructure (PKI)

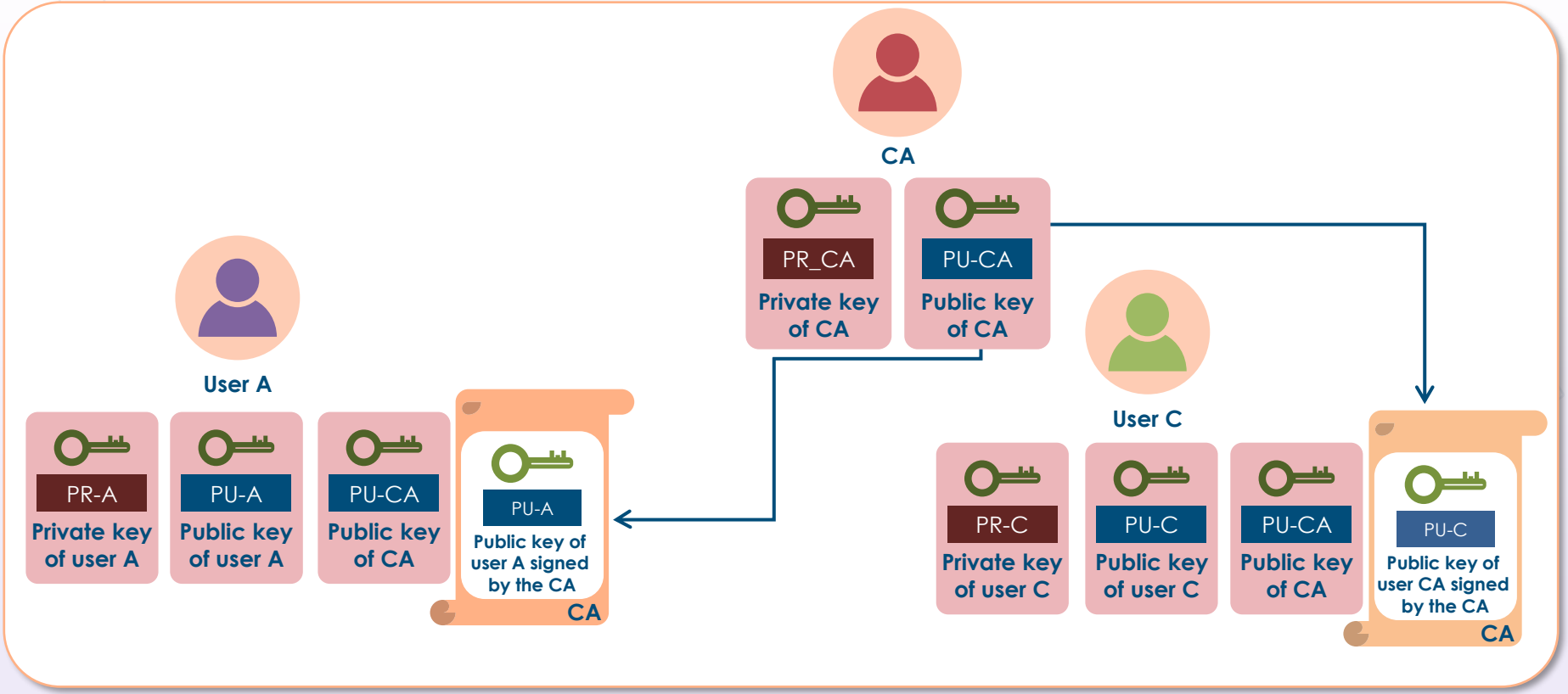
- The CA is the central trusted introducer (Thawte, GeoTrust, Comodo, Symantec)
- The CA stores, issues, and digitally signs certificates of customers
- Everyone has the public key of the CA (or a trusted CA) in a browser or O/S store
- A certificate signing request (CSR) is used by the enrolling party to be granted a certificate by a CA



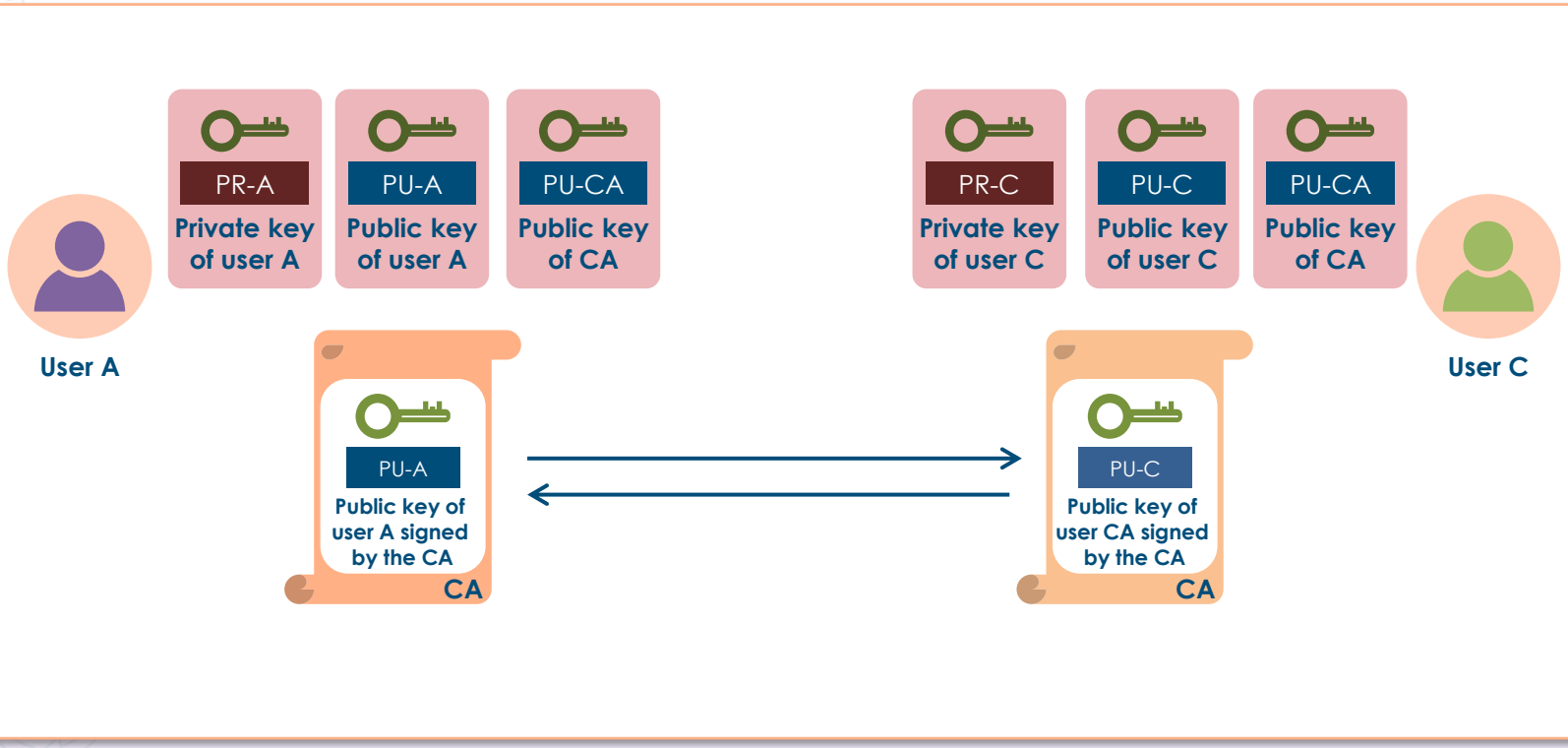
Public Key Infrastructure (PKI)



Public Key Infrastructure (PKI)

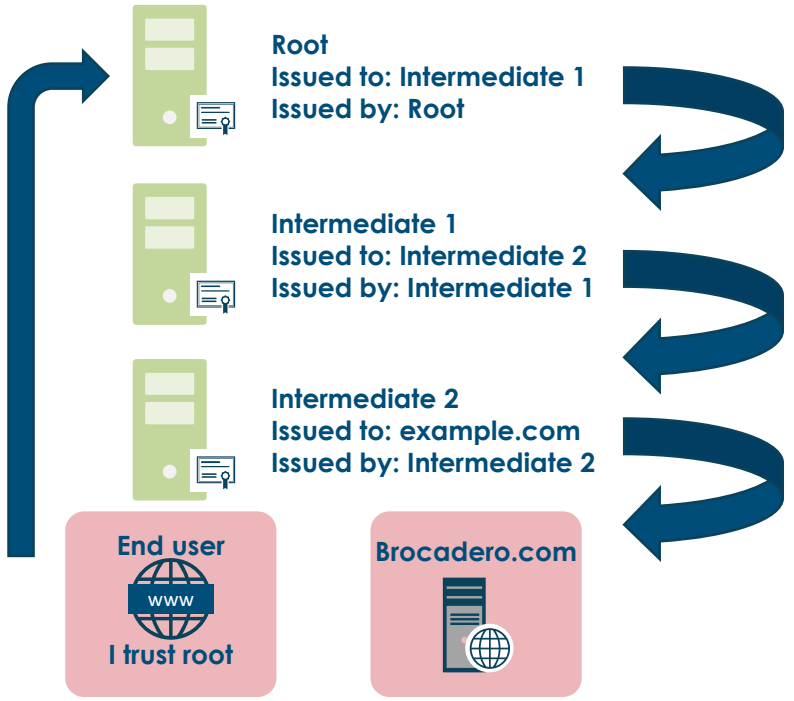


Public Key Infrastructure (PKI)



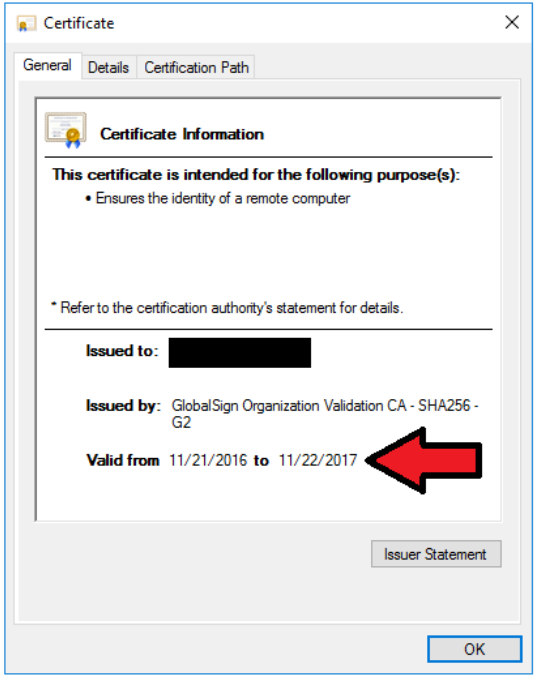
CA Trust Models

- **Single CA**
  - Responsible for directly providing certificates to everyone (enterprise PKI)
  - Must always be online
- **Hierarchical CA**
  - Combination of root CA and intermediate CAs
  - Root sends certificates to intermediates
  - 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



Certificate Revocation and Suspension

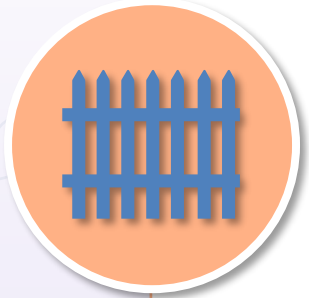
- For security reasons all keys must have a finite life due to brute force attacks
- Certificates are stamped with non-deterministic serial numbers and validity dates
- Certificate can be
  - revoked (permanent) – never used again
  - suspended/held (temporary) – can be reactivated
- Extension fields are critical for added functionality and security
- Certificate revocation list (CRL) is the original method for revoking certificates
- Online Certificate Status Protocol (OCSP) is an Internet-enabled transactional database that CAs and web servers utilize for suspension and revocation



Systems Security Certified Practitioner (SSCP)

Physical Security Operations

Fence Barriers



- Most organizations will have protective fence barriers around the perimeter to deter or prevent individuals from unauthorized entry and exit
- Fences may only be used in certain zones or areas to protect junction boxes, generators, dumpsters, and shredding service pickup points
- Fences are combined with entry/exit gates of varying strength
  - Barricade gates
  - Tire shredders

Types of Gates

I. Class I: residential gate operation

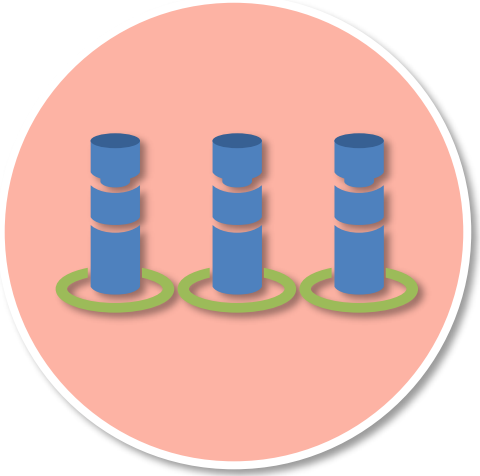
II. Class II: commercial, such as parking lot or garage

III. Class III: industrial/limited access (warehouse, factory, docks)

IV. Class IV: restricted access operation requiring supervisory control

Bollards

Pylons

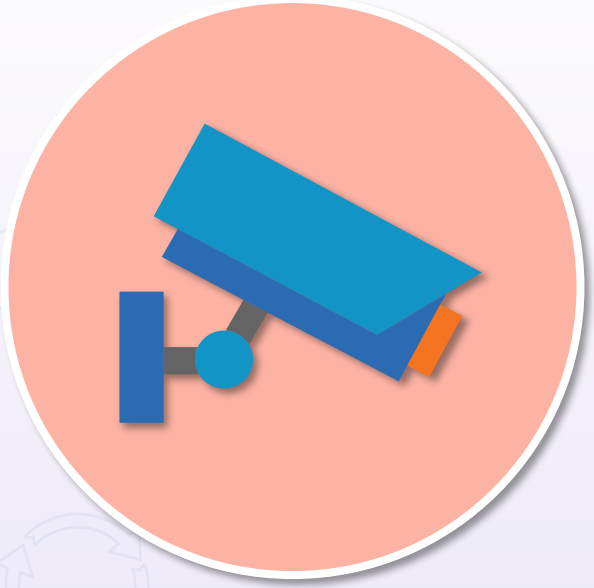


- Bollards are strategically placed pylons meant to prohibit vehicles from entering certain areas
- They can also be used to permanently or temporarily direct pedestrian or automobile traffic
- Typically, they are made of concrete or strong metal
- High-tech bollards can be mechanical and include cameras and sensors

Signage

- Signs and window stickers are a deterrent control designed to deter individuals from doing something unauthorized
  - Authorized Personnel Only
  - Do Not Enter
  - No Trespassing
  - Beware of Dog
  - Caution Electric Fence
  - Biohazard Danger

Cameras and Surveillance Methods



- Provide a way to monitor and record the property perimeter for intruders and potential attackers
- Are considered deterrent and detective physical controls
- Deliver a way to record intruders in action with recordings
- Should trigger alerts when a camera is disabled

Cameras

- Inside web cams or outside systems
- Closed-circuit to SOC/linked to third-party vendor
- Should be combined with lighting
- Need to locate all dead spots
- Back up video media to safe location

Industrial Camouflage

- Cameras and surveillance devices are often camouflaged in landscaping elements, statues, and tall trees
- For example, towers carrying cell phone and other equipment are covered by fake trees
- Certain high-security rooms can be underground and set at distance from main buildings

Personnel Controls

- Many organizations will have all guests register at a reception area security desk
- Collect and input identification information in visitor log
- Camera station with picture for temporary badge
- Distribute temporary access cards or badges
- Guests may need to always be escorted by another employee or security officer to provide two-person integrity and control

Security Guards

- Guards are typically present 24x7 but could be just during business hours
- They are a security control of multiple types
  - Detective
  - Deterrent
  - Preventative
- They can provide rapid security response if an intrusion or incident occurs

Security Guard Considerations

Do you hire or contract, freelance, certified/licensed?

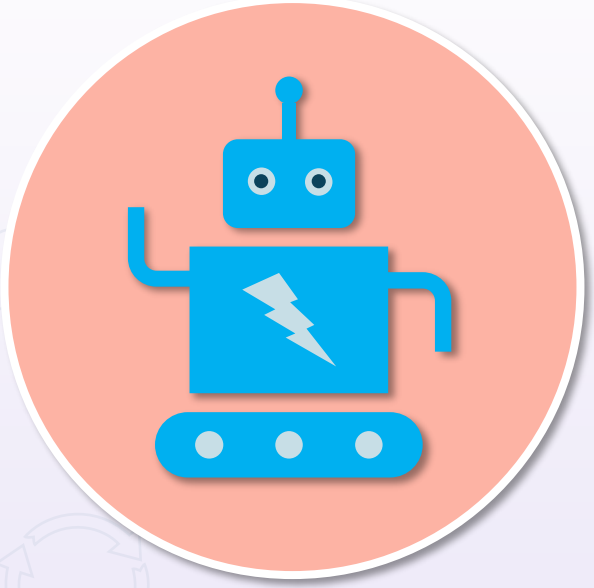
Will they be armed or unarmed?

What is the impact on insurance policies?

Are you involved with screening and background checks?

Who provides the ongoing training?

Robot Sentries



- Robot sentries can be used in home or commercial environments as security guards with cameras, sensors, and more
- The Samsung SGR-A1 is a type of sentry gun that was developed jointly with Korea University to support South Korean troops in the Korean Demilitarized Zone

Locking Mechanisms

- Locks are the most common physical security mechanism
- They are considered a preventative control although they technically only delay entry – not prevent it in the long run
- Locks keep honest people out but cannot deter resolute intruders, since most locks are easily bypassed, and most keys are readily duplicated
- They can be physical, electronic, and/or biometric

Picking Locks

- Picking involves using a tension wrench to rotate the key plug of the lock to find the lock tumblers
- At the same time, the pick is used to move the binding tumblers, one at a time, to the shear line
- When all the tumblers are aligned properly with the shear line, the lock opens

Raking Locks

- Raking uses a pick that has a wider tip inserted all the way to the back of the plug
- The pick is then pulled out quickly so that all the pins are bounced up
- As the rake exits, a tension wrench turns the plug
- Some of the upper pins will fall on the ledge created by the turning pins where the attacker can easily pick the remaining pins

Brute Forcing Locks

- Brute force techniques will always be successful given enough time and effort
- Involves using hammers, tire irons, firearms, and more
- Contributes to locks being a "delay" control

Types of Locks

- Warded key lock – wards are obstructions to the keyhole that prevent all but the properly cut key from entering
- Wafer/tumbler – wafers under spring tension are in the core or plug of the lock and protrude outside the diameter of the plug into a shell formed by the lock body
- Pin tumbler – key moves pins so that a shear line can be obtained, allowing the key to turn the plug and operate the lock
    - More secure than warded and wafer/tumbler locks

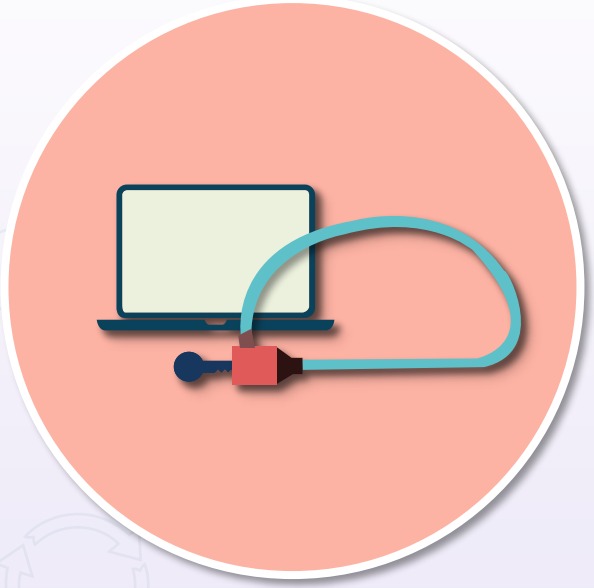
Types of Locks

- Deadbolt – a bolt inserted into the frame of the door for additional security when combined with other locks
- Interchangeable core – a lock with a core that can be removed and replaced using a special-change key
- Combination – a sequence of numbers in proper order

Types of Locks

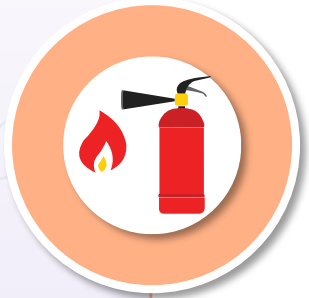
- Electronic combination
  - Digital readouts obtain power from the energy created when the dials are turned
  - Higher security than combination locks, but more expensive
- Keyless
  - Lock that has buttons that are pushed in sequence to open the door
  - Sometimes called a cipher lock
- Smart lock
  - Inexpensive plastic card that is pre-authenticated to open a door
  - Used in most hotels

Types of Locks



- Cable locks are used to secure devices to a desk or shelf and deter theft of the device
  - Can also be used in combination with laptop docking stations
- USB data blockers are a form of USB locking to prevent infecting your smartphone or tablet with malware
- They can also prevent attackers from executing or installing malicious code on your device to access your data

Fire Prevention and Suppression



- Prevention
  - Fire-rated construction materials, training, safety
  - Be prepared
- Detection
  - Smoke and fire detectors, sensors
  - Control quickly, minimize damage
- Suppression
  - Contain and extinguish the fire

Fire Controls

- Type A – common combustibles, such as wood products, paper, and laminates
  - Suppressed with water or soda acid
- Type B – combustible liquids, such as petroleum products and coolants
  - Suppressed using halon substitutes, carbon dioxide, dry powders, or soda acids
- Type C – electrical equipment and wires
  - Extinguished using gas, dry powders, or carbon dioxide
- Type D combustible metals
  - Can be suppressed only with dry powder

Sensors

Lighting is most common

- Controls to protect many internal systems
- Lighting is often used in combination with other and external areas
- Potential attackers prefer the cover of darkness
- Lighting is a detective and sometimes deterrent control
- Lighting can enhance other security controls, such as cameras, security guards, and sensors
- Should start at the perimeter and be used in every defense-in-depth mechanism to the "keep"

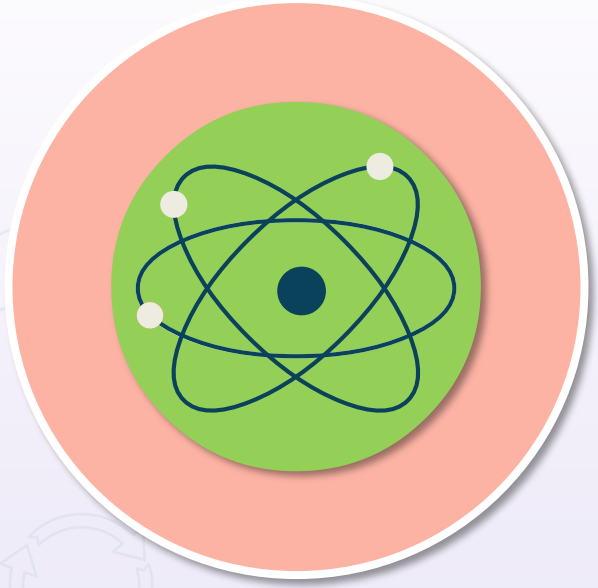
Types of Lighting

- Mercury vapor
- Sodium vapor
- Quartz
- LED
- Continuous lighting
- Trip lighting
- Standby lighting
- Emergency lighting

Types of Sensors

- Photoelectric – a break in a light beam
- Passive infrared – detecting infrared light
- Vibration – a change in the level of vibration
- Acoustical – noise detection of a change in sound waves
- Microwave – a change in high-frequency radio waves

Types of Sensors



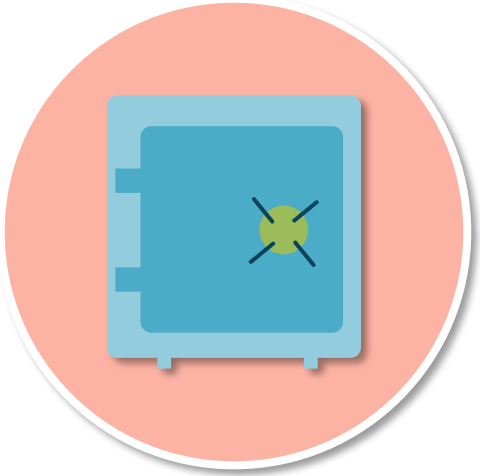
- Electro-mechanical – a break in electrical circuit
- Electrostatic – a change in an electrostatic field
- Moisture and temperature detection – for server rooms and data center environmental controls

Sensor Triggers and Alarms

- Static or flashing light on display panel
- Bell rings or horn blares
- SMS or text message sent
- Telephone call or software notification
- Silent alarms to security firm or law enforcement

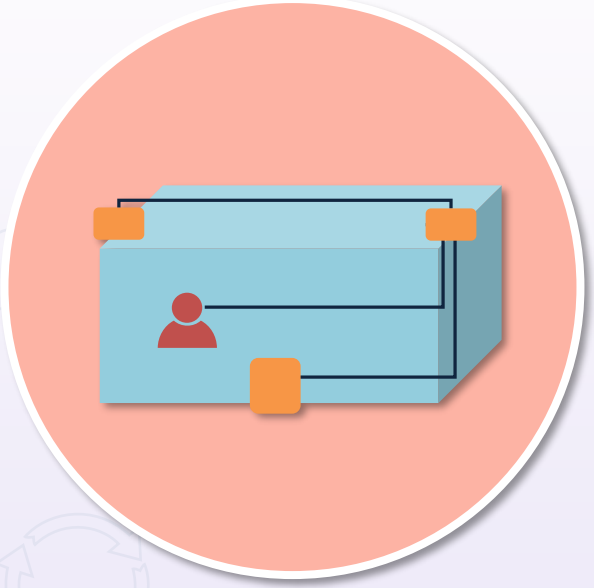
Secure Areas

Safes and vaults



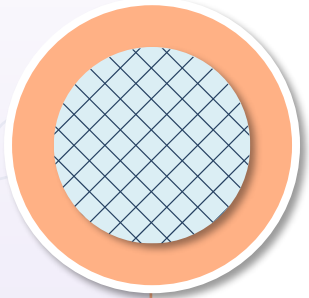
- Safes and vaults may often be where the most valuable corporate physical assets are stored
- Currency, deeds, licenses, precious metals, diamonds, securities, policies, and failsafe passwords
- They should be attached to the physical infrastructure so it cannot be easily carried away
- Considerations are location, fire and burglar-proof, type of lock (MFA), material of safe – tensile strength, weight, relocking devices (timers) – sensors, and alarms

Mantraps



- Mantraps and cages are often used to control access to a facility or a specific area of a facility
- There is an entry and exit door, but only one door can be open at a time
- One person at a time – no piggybacking (tailgating)
- The person can be identified and authenticated
  - Provide credentials and license or passport
  - Can include biometric readers
  - CCTV and intercom systems are often used
  - Security guard behind bullet-proof glass
  - The person is eventually allowed in through strong door with electronic locks

Faraday Cages



- Faraday cages are rooms, enclosures, or bags that block electromagnetic fields emanating from electromagnetic interference (EMI), Carrington events, solar flares, and electromagnetic pulses (EMP)
- The shield may be fashioned from a continuous covering of conductive material, or in the case of a Faraday cage, a mesh of similar materials
- These can often be found in data centers or other enterprise safe rooms

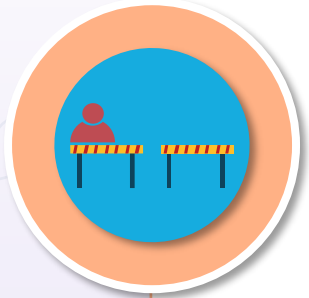
Cable Runs and Distribution Frames

- Remember all cable runs and distribution frame (MDF) rooms and closets
- Under the floor
- Above ceiling panels
- Lock all doors to server rooms
- Cameras can be used along with other types of sensors

Air Gap

- Secure system has no access to Internet
- Very limited access to LAN, if any
- Can be physical or logical
- Still vulnerable to rogue insider
- Stuxnet was introduced to air-gapped area

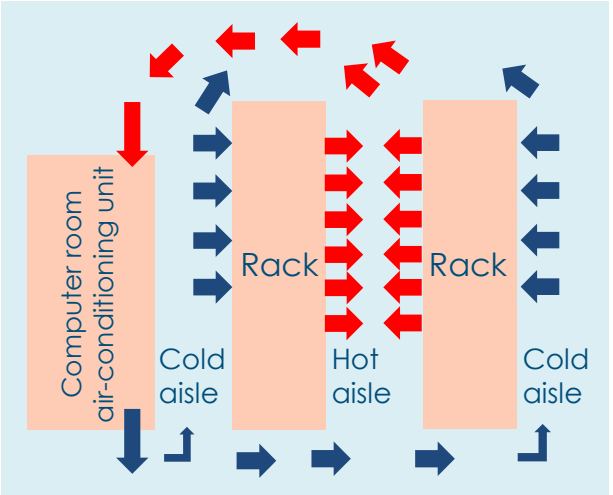
Air Gap



- Military and governmental agency networks and systems
- Financial systems, such as stock and cybercurrency exchanges
- Industrial control systems, like SCADA in water processing facilities
- Life-critical systems, such as nuclear power plants, computers used in aviation, and computerized medical equipment

Hot and Cold Aisles

- Heating, ventilation, and air-conditioning (HVAC) are vital environmental issues
  - Poor HVAC leads to extreme heat, cold, humidity, or dryness
  - Recommended temp: 72 to 76 degrees
  - Recommended humidity: 40 - 60%
- Maintain hot and cold aisles in the server rooms and data center to move hot air from devices into a hot aisle and redirect to an air conditioning unit or room



Environmental Controls

- Environmental systems and monitoring are often on separate networks and power sources
- Controls should be highly available
- Monitoring should be automated with redundant alarms and alerting systems
- Should also include specialty and embedded service security (PLC sensors, SoC, etc.)
- Coolers and chillers should be used
  - Secure locations (physical security outside)
  - Remote management and monitoring