



The Foundations of Cybersecurity

Security Concepts and Principles

Dr. Laurent Gomez, SAP Security Research
OSCP, OSWP, TOGAF certified
laurent.gomez@protonmail.com

Who am I ?

laurent.gomez@protonmail.com



Head of Security Testing Automation | SAP CPIT

Authors of ~ 70 scientific publications / patents

- Security for Machine Learning
- Security for Distributed Enterprise Systems, Industrial IoT
- Privacy Enhancing Technology (FHE, Garbled Circuit, TEEs, ...)

Certifications

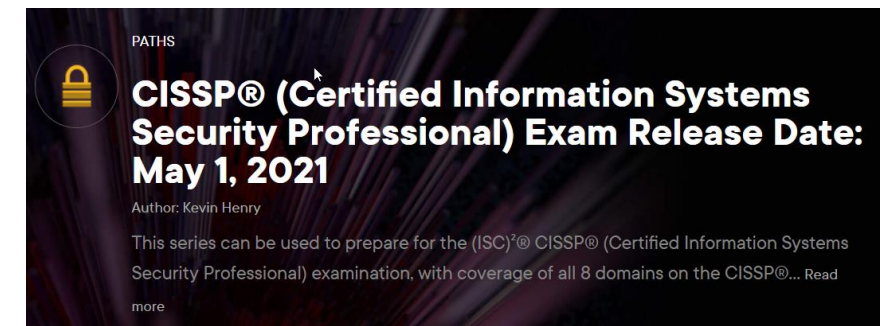
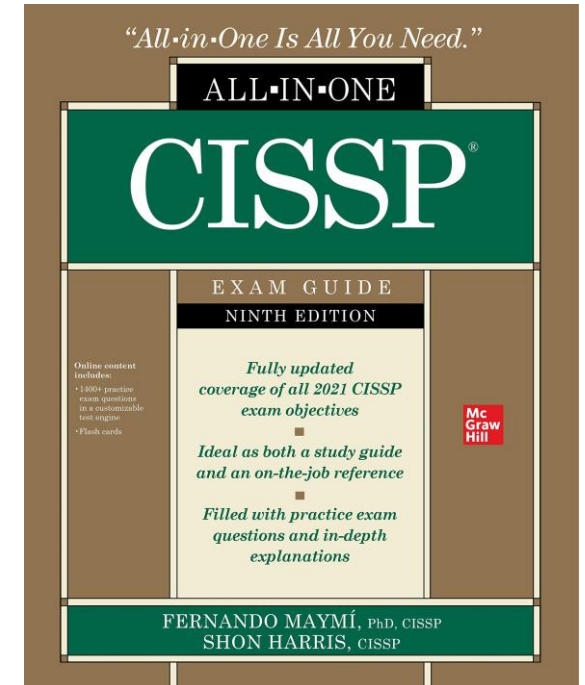
- Pentesting with Kali (PWK)
- Business Architect, TOGAF



Educational reference

Certified Information Systems Security Professional

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and testing
- Security Operations
- Software Development Security



Free for students, training
for CISSP

Name the first-ever malware !

The Creeper

The Reaper

COVID-1971

Stuxnet

Name the first-ever malware !



The Creeper

I'M THE CREEPER. CATCH ME IF YOU CAN!

In 1970, it self-replicated on TENEX computers, connected to the ARPANET network.

The Reaper

COVID-1971

Stuxnet

Cybersecurity

Definition



The art of protecting organizational assets from attacks. It comprises of an evolving set a tools, risk management approaches, technologies, training and best practices [1](#)

Organizational Assets

- People
- Network
- Application
- Data
- Infrastructure
- Hardware

Attacks

- Identity Theft
- Cryptojacking
- Social Engineering
- Malware
- Ransomware
- Phishing
- ...

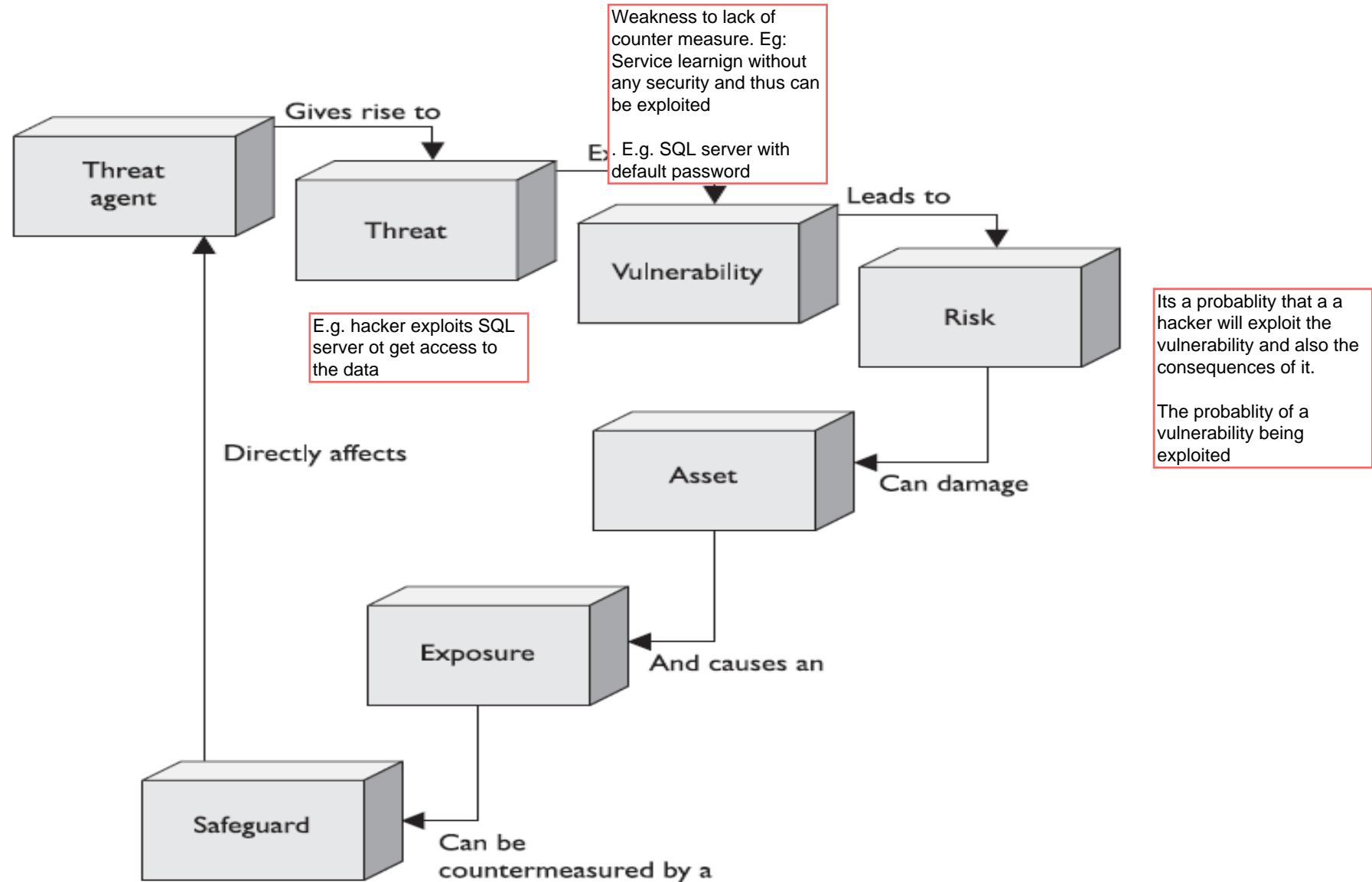
When you download for free an app and suddenly the mobile starts being slow. In the back the app is using the device for mining crypto

Tools

- Encryption
- Access Control
- Identity and Access Management (IAM)
- Security Awareness Training
- Risk Assessment

Terminology

Prof expects to be able to tell this at the end.



Cybersecurity ‘fun’ facts for 2023¹

The cost of cybercrime to hit **\$8 trillion in 2023**, increasing to \$10.5 trillion by 2025.

81% of **organizations** were **affected** by cybercrime last year.

A **malicious hacking attack** occurs every **39 seconds**.

Routers and connected cameras account for **90% of attacked devices**.

- Usernames such as “Root” and “admin” must be avoided, as well as passwords that duplicate the username or are a variation of it.

2013’s **Yahoo data breach** compromised **3 billion accounts**.

Every hour of downtime due to a ransomware attack costs an average of **\$250,000**

It takes an average of **277 days** for security teams to identify and contain a data breach

The largest **internal data breach** event **lasted for 30 years**.

The number of phishing attack victims increased by 34% in 2021, and remains the #1 type of cyber crime.

Emerging Threats

CYBER ATTACKS MAKE HEADLINES, PROMPT GOVERNMENT RESPONSES

Ransomware Attack Affecting Likely
Thousands of Targets Drags On

July 2021 | THE WALL STREET JOURNAL.

EU wants emergency team for
'nightmare' cyber-attacks

June 2021 | **BBC**

SolarWinds Hack Grabs Senate Spotlight
With CEO in the Hot Seat

February 2021 | **Bloomberg**

Executive order aims to protect software
supply chains

June 2021 |  REUTERS®

More than 20,000 U.S. organizations
compromised through Microsoft flaw

March 2021 |  REUTERS®

U.S. Pipeline Cyberattack Forces Closure

May 2021 | THE WALL STREET JOURNAL.

Emerging Threats¹

Work-from-home Attacks

With many staff using home broadband connections for both personal use and their jobs, the corporate attack surface has increased by a lot.

- [445 million](#) cyber-attacks were reported during the first three months of the pandemic — a 20% increase as compared to the previous quarter.

Ransomware

Accounted for [27%](#) of the data breaches involving malware infections last year.

Recent Thales attacks by Lockbit ¹

The percentage of users impacted by targeted ransomware doubled in the first 10 months of 2022.

Credential-related breaches

Data breaches involving lost or stolen credentials take longer to identify and cost \$150,000 more than the average data breach.

DDoS and IoT

A DDoS is a cyber attack that disrupts the availability of online services or systems by overwhelming the server with huge traffic/request volume. To launch a DDoS attack, attackers must first assume control of multiple computer systems, including IoT devices.

- As many as [5200](#) cyber attacks are launched against IoT devices each month
- Use of Shodan.io

Emerging Threats¹

CryptoJacking²

In 2021, hackers stole more than [\\$283 million](#) worth of cryptocurrency

In 2020 [cryptojacking](#) increase by 163% in Q2'21

Cryptojacking incidents grew by 230% in 2022, with hackers earning an average of approximately \$1,600 per month.

Supply Chain Attacks – [SolarWinds](#)

Targets an organization, or a set collaborative organizations, through vulnerabilities in its supply chain.

Gartner predicts that by 2025, 45% of global organizations will be impacted by a supply chain attack.

- Third-party software updates
- Malware installed on connected devices, for example, external hard drives, cameras, phones, etc.
- Application installers

Exposed over 18,000 private and government clients' data exposed, with an estimated cost of [\\$100 Billion to recover from](#).

AI-powered cybercrime

Automation of vulnerability identification

Sophisticated phishing and social engineering attacks

- [A Voice Deepfake Was Used To Scam A CEO Out Of \\$243,000](#)
- [Mimic writing style](#)
- [Disinformation and Conspiracy spreading](#)

SolarWinds Attack Process

SUPPLY CHAIN ATTACK

Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE

When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

DEFENSE EVASION

The backdoor has a lengthy list of checks to make sure it's running in an actual compromised network.

RECON

The backdoor gathers system info

INITIAL C2

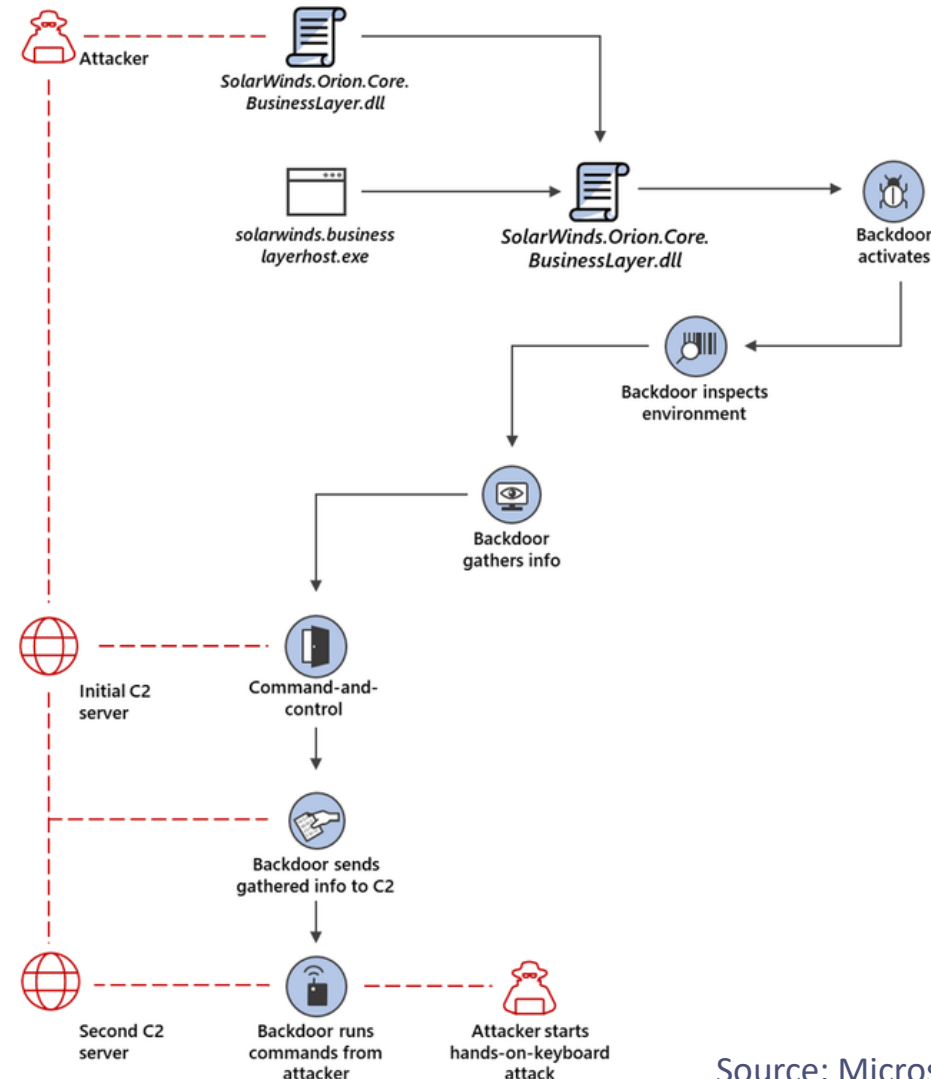
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

EXFILTRATION

The backdoor sends gathered information to the attacker.

HANDS-ON-KEYBOARD ATTACK

The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.



Source: Microsoft.com

Impact of Cyber Crime on the Industry

Financial loss

Reputation damage

Disruption of operations

Intellectual Property theft

Regulatory Consequences

Increased Costs of
Cybersecurity Measures

Escalating Cybersecurity
Insurance Costs

Loss of Sensitive Data

Workforce Challenges

Global Economic Impact

Security Principles

Life safety is THE priority !!!

- [EU-OSHA](#)

Compliance with regulation

- Data protection regulation
 - EU GDPR, HIPAA, California Consumer Privacy Act (CCPA), ...
- Due care and due diligence

Protection of IP and Data Privacy

Security must be

- Aligned with business strategy
- Be supported by senior management

Risk Management Frameworks

NIST Risk Management Framework

Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

Committee of Sponsoring Organizations of the Treadway Commission (COSO) Risk Management Framework

ISO 31000 (series)



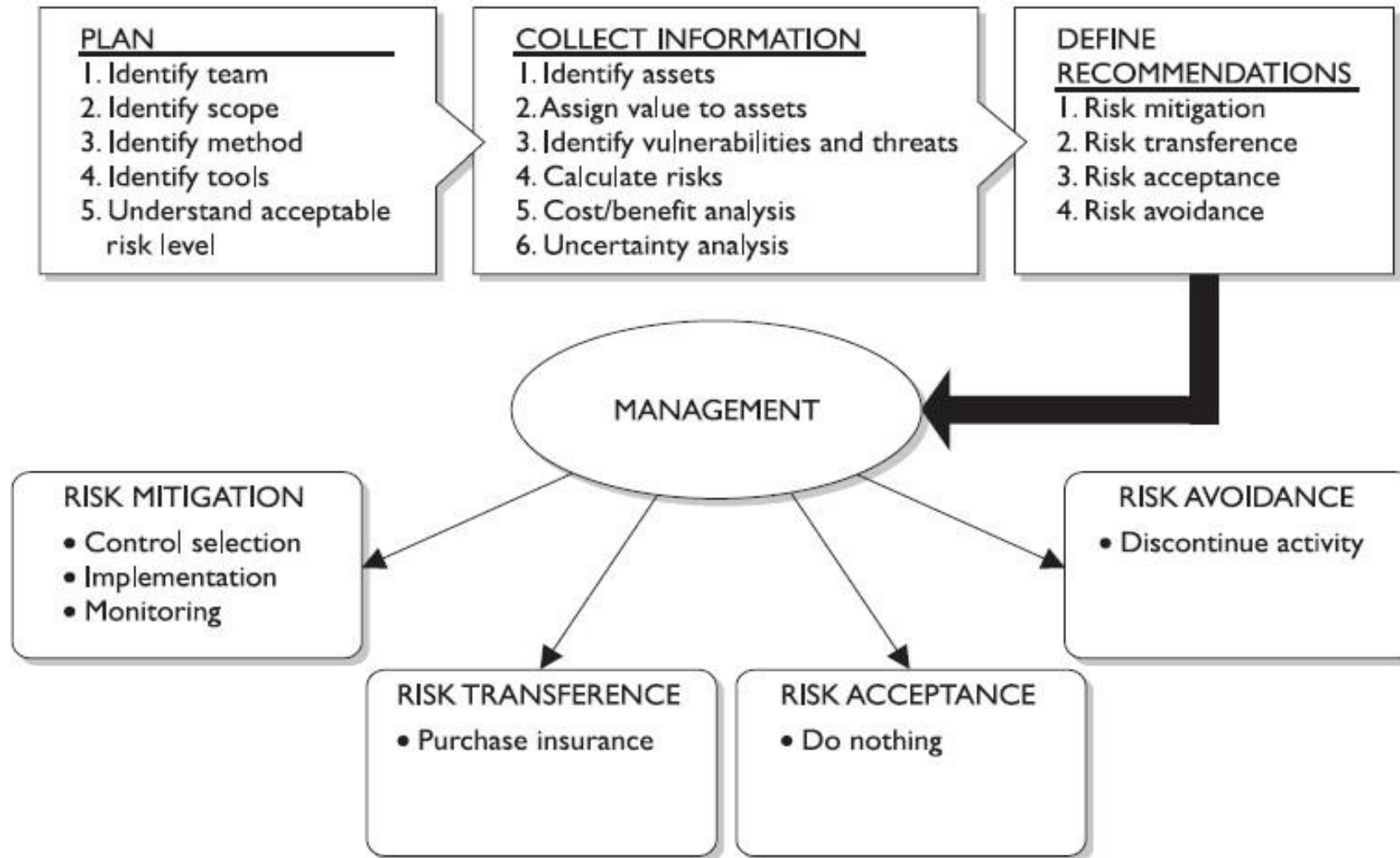
Control Objectives for Information and Related Technology (COBIT)

Threat Agent Risk Assessment (TARA)

Factor Analysis of Information Risk (FAIR)

Risk Management in a Nutshell

Evaluate and Mitigate Risk



Risk Assessment

Threat Modeling¹

Think like a hacker!

Done at the beginning so when designing the architecture of the product

Enumerate potential threats within information systems

OWASP Top 10²

- Target web application security

MITRE ATT&CK Framework³

- Framework for threat modeling, penetration testing, defense development

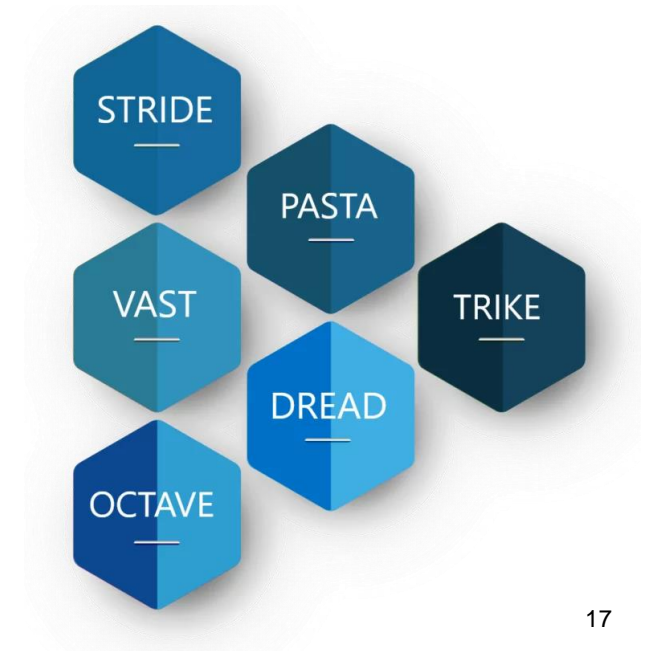
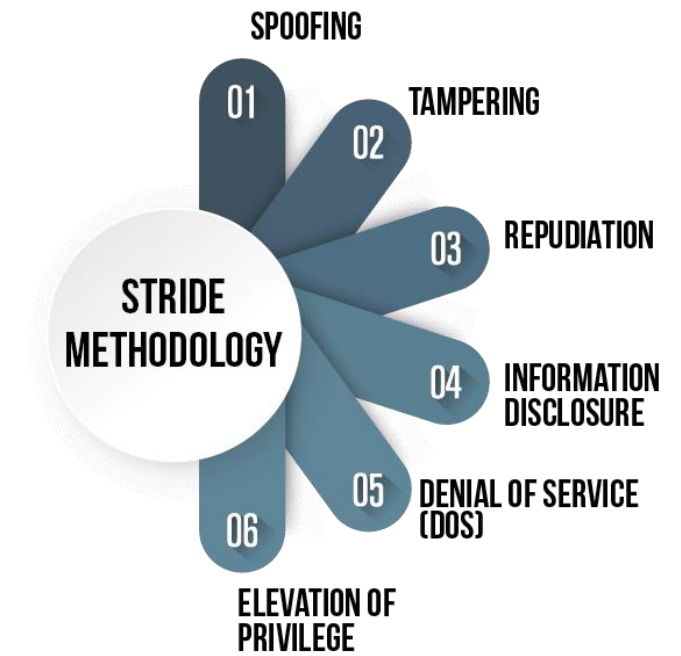
MITRE Common Weakness Enumeration (CWE)⁴

- List of 25 common weakness

Methodologies

STRIDE⁵

SAP Threat Modeling



Pentesting



A **penetration test** is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source

The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered

Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution

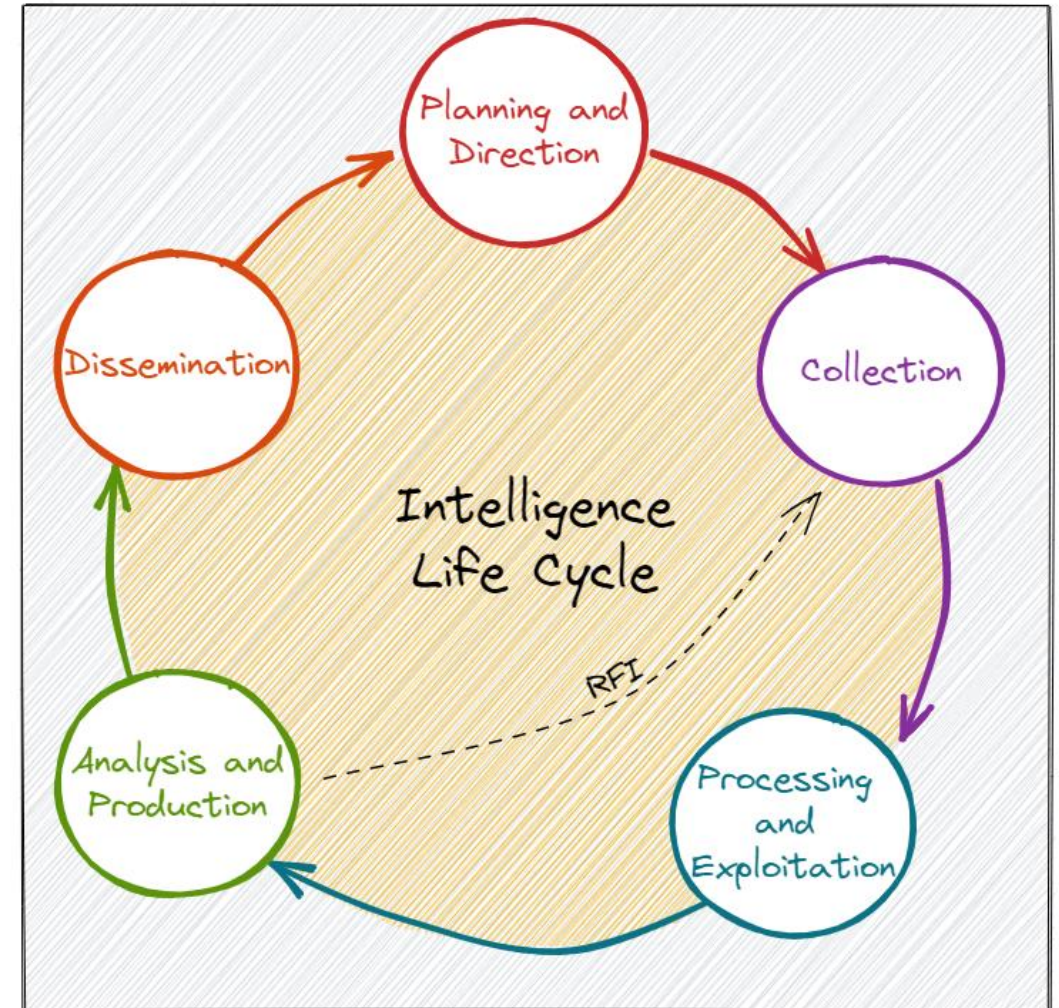
Black box and white box approach

E.g. as a pentester you identify what is running on the machine and then check for the vulnerabilities of the systems, to identify the potential threats.

Cybersecurity Threat Intelligence

Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors.

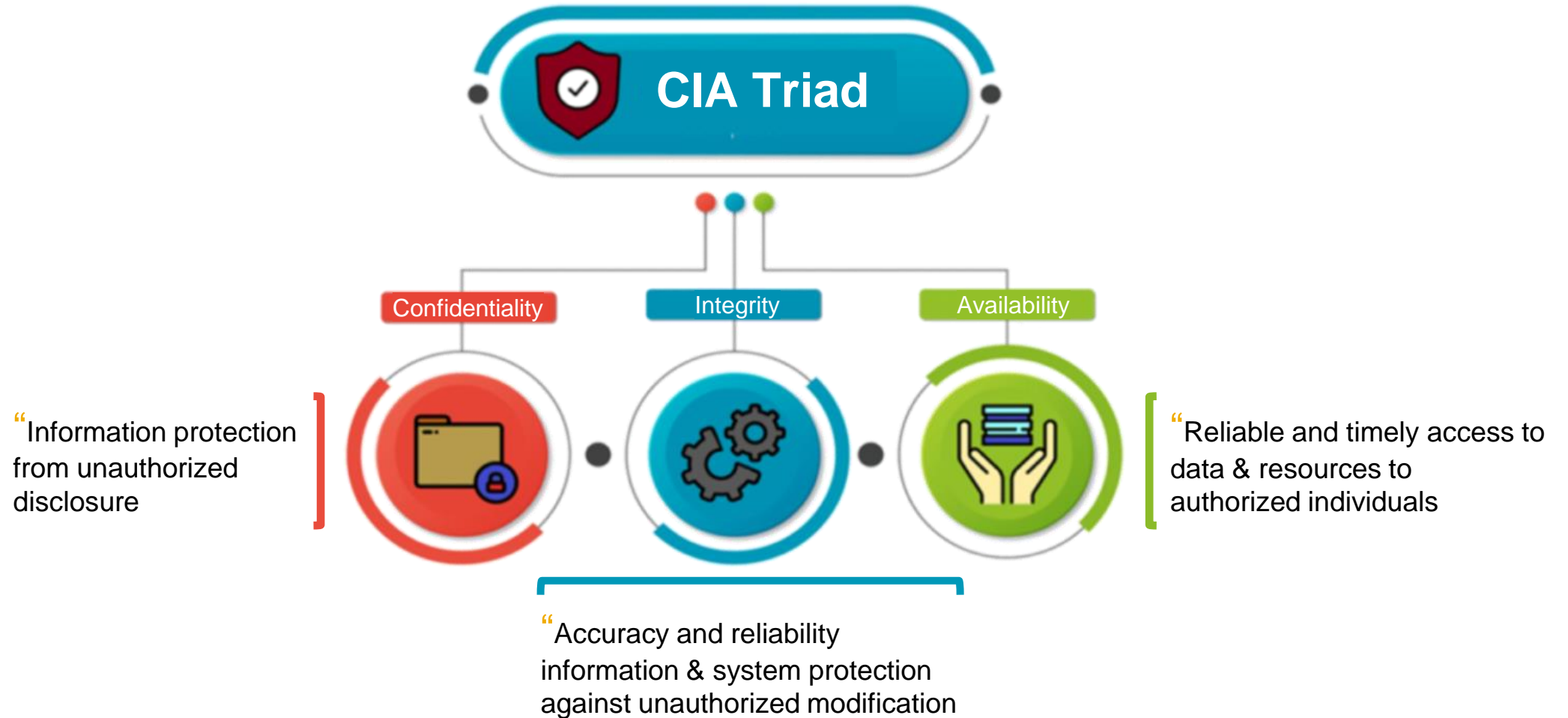
Threat intelligence is evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets. – Gartner



Confidentiality, Integrity, and Availability

CIA Triad

The CIA are within the security policy



Confidentiality, Integrity and Availability

Importance of Confidentiality, Integrity and Availability lies into the organization operational environment

- Protection of information & information systems
- Managing cybersecurity as any business risk

Security Strategy.

- Documented in **Security Policy**
 - Password Management
 - Identity and Access Management
 -
- Enforced through **Security Controls**
 - Physical (fences, door, fire extinguishers)
 - Procedural (incident response processes, security awareness and training, disaster management)
 - Technical (access controls, antivirus software, firewalls, encryption)
 - Legal and regulatory (data privacy regulation, contractual terms and conditions)

Confidentiality

Protect sensitive asset from improper disclosure

Intellectual Property

- Research
- Business plans

Information

- People
 - HR information
 - Personal Identifiable Information (PII)
- Organization (deals organization knowledge)
 - Financial data
 - Strategic plans
- Customer
 - User passwords
 - Credit card information
 - Financial Data

Confidentiality Breaches

Intentional

- Information harvesting
 - Boeing engineer case
 - Yahoo data breach

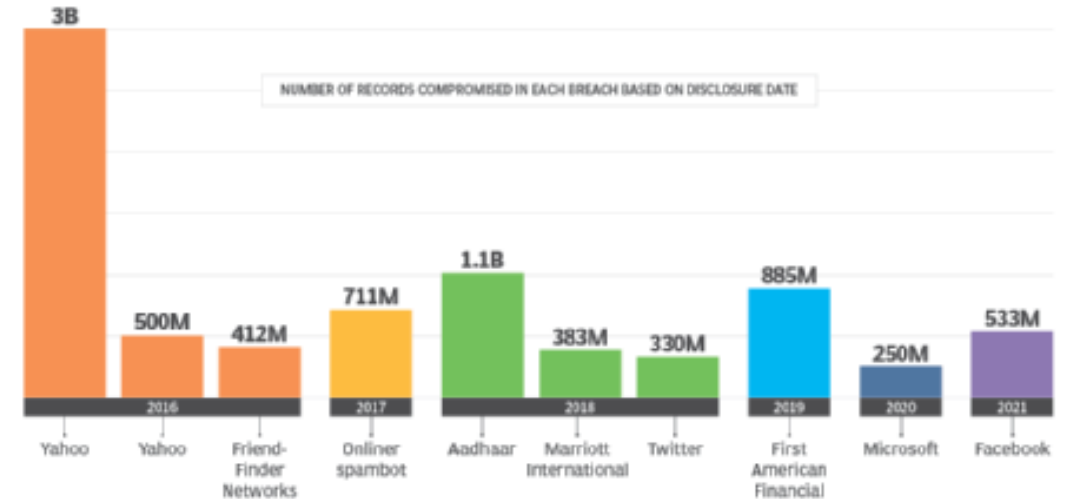
Accidental

- Information Disclosure in public spaces
 - Sensitive information interception on public wifi hotspot

Displayed data (in public spaces)

- Reports
- Screens
 - Clean desk, screen, user screen filters
- Discussion eavesdropping
 - Airbus information eavesdropping

10 of the biggest data breaches in history

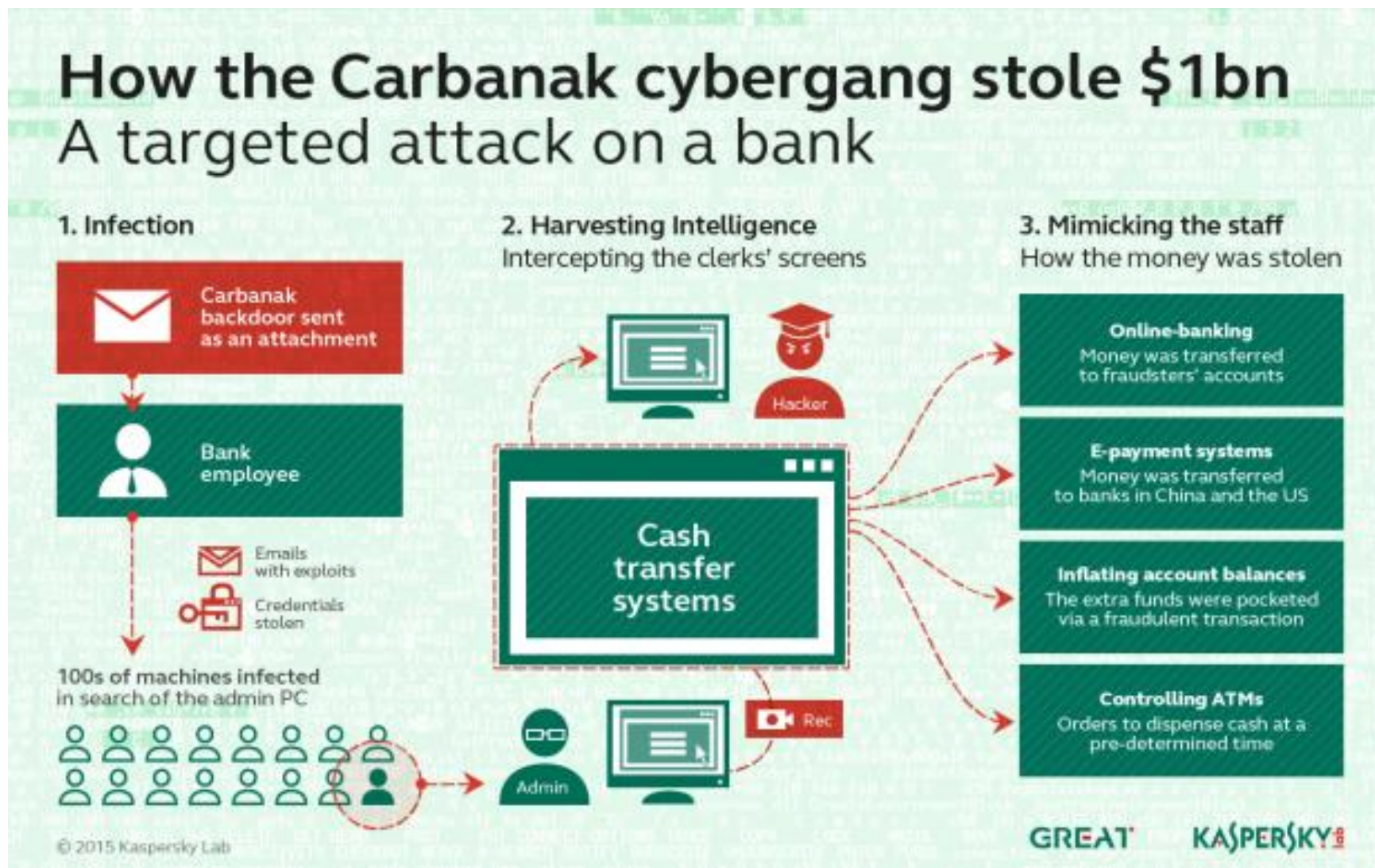


Covert channels

- Timing
 - Observe change in resource usage
- Storage
 - Lost of media storage containing sensitive information
 - Paper
 - USB
 - Laptop

Confidentiality Breaches

Carbanak: the Great Bank Robbery



Impact of Confidentiality Breaches

Legal Penalties

- Contractual defined, in case of information disclosure
- In particular if organization ignore due care and due diligence
 - Negligence

Financial penalties

- Loss of revenue
- Missing opportunities
- Reputation damage

“The average cost of corporate data breach is \$3.83 millions

“The loss of one million records costs \$40 million on average.

Guarantee Confidentiality

Policy

- Document organization/company data protection measure (on behalf of customers)

Access control

- Get out everyone from information in not sufficient
- Need-to-know
 - Disclose information Only individual who need to know (for their daily business)
- Least privilege
 - You can read but not modify

Encryption

Enforce Confidentiality

Make the information unavailable to unauthorized entities

Encryption

- At rest
- In transit
- Privacy Enhancing Technologies
 - Processing over encrypted data
 - FHE, MPC, Functional Encryption

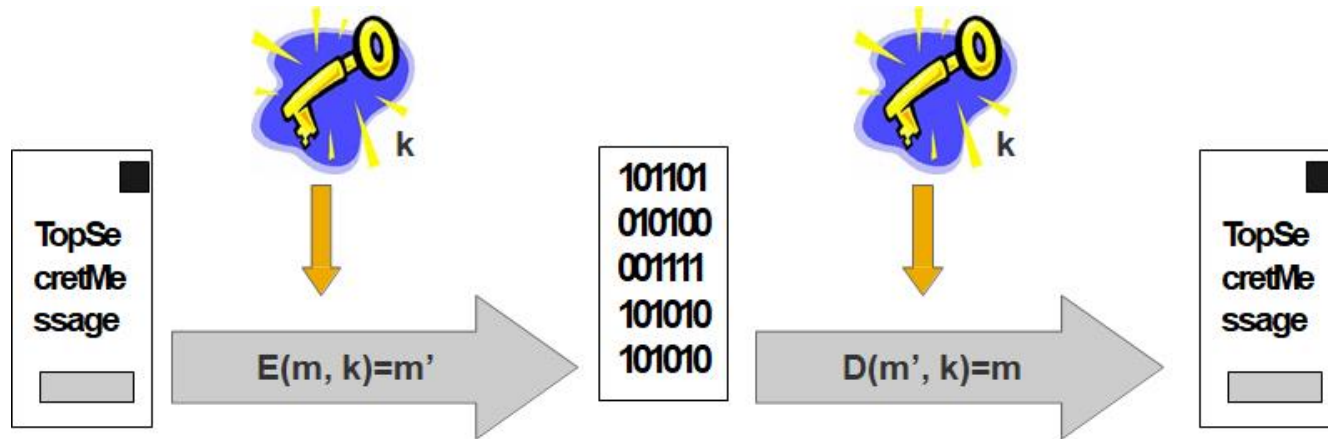
Anonymization

- Degrading original data
 - Differential Privacy
- Mimic original data
 - Synthetic Data Generation

Tokenization

- process of replacing actual sensitive data elements with non-sensitive data elements that have no exploitable value for data security purposes

Symmetric Encryption



Efficiency

Use single key for encryption and decryption.

The adv: its very efficient

Advanced Encryption Standard (**AES**)

- Supported key size: 128-192-256
- Block size: 128 bits

In AES everyone knows how the protocol works. So the key is the most important to keep secret.

Encryption

$$E(m, k)=c$$

Decryption

$$D(c, k)=m$$

Property

$$D(E(m, k), k)=m$$

With symmetric encryption, you MUST guarantee the secrecy of ...

Everyone knows the
encryption and decryption
algo here.

Encryption
Algorithm

Decryption
Algorithm

Key

Message

With symmetric encryption, you MUST guarantee the secrecy of ...

Encryption
Algorithm

Decryption
Algorithm

Key

Message

Name a disadvantage to symmetric encryption !

Algorithm
Complexity

Key Distribution

Key Secrecy

Key Size

Name a disadvantage to symmetric encryption !

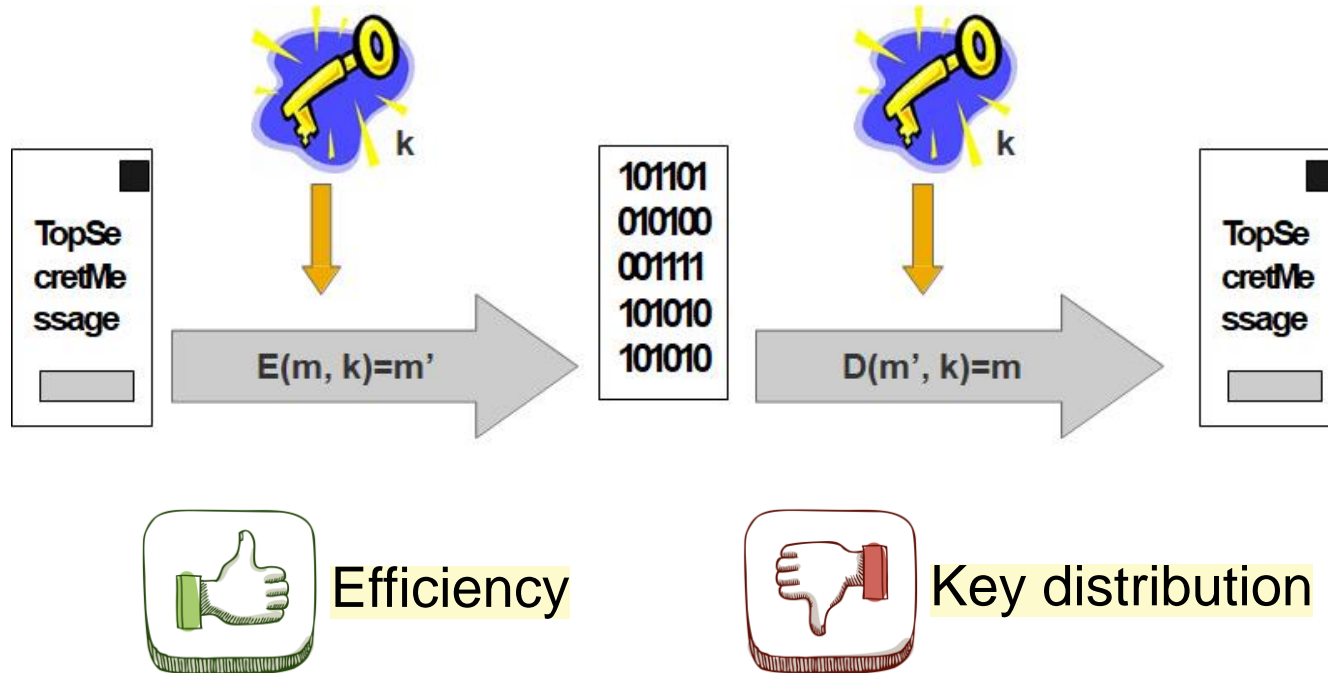
Algorithm
Complexity

Key Distribution

Key Secrecy

Key Size

Symmetric Encryption



Encryption

$$E(m, k) = c$$

Decryption

$$D(c, k) = m$$

Property

$$D(E(m, k), k) = m$$

Advanced Encryption Standard (**AES**)

- Supported key size: 128-192-256
- Block size: 128 bits

Symmetric Encryption

Sample Python Code¹

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad

# Output file
output_file = 'encrypted.bin'
# Message
message = b'Top secret message'
# 16 bytes Encrypted Key
key = b'POLYTECHPOLYTECH'

# Encrypt message
print("[ ] Encrypt message: "+str(message))
print("[ ] with key: "+ str(key))
## Create Cipher
cipher = AES.new(key, AES.MODE_CBC)
## Encrypt message
encrypted_message = cipher.encrypt(pad(message , AES.block_size))
print("[ ] Encrypted message: "+str(encrypted_message))

# Persist encrypted message in a file
file_out = open(output_file, "wb")
## write iv
file_out.write(cipher.iv)
## write encrypted message
file_out.write(encrypted_message)
file_out.close()
```

Symmetric Decryption

Sample Python Code¹

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad

# Input Encrypted File
input_file = 'encrypted.bin'
key = b'POLYTECHPOLYTECH'

# Read iv and encrypted data from file
file_in = open(input_file, 'rb')
## get the IV
iv = file_in.read(16)
## get the encrypted data
encrypted_data = file_in.read()
file_in.close()

# Decrypt
## set the cipher engine
cipher = AES.new(key, AES.MODE_CBC, iv=iv)
## decrypt
print("[ ] Encrypted message: " + str(encrypted_data))
original_message = unpad(cipher.decrypt(encrypted_data), AES.block_size)
## print decrypted text
print("[ ] Decrypted message: " + str(original_message))
print("[ ] with key: " + str(key))
```

Integrity

Prevent unauthorized modification

Accuracy, and Reliability of Information (and Information Systems)

- Application
- Process
- Platforms

Related to

- Authenticity

Integrity Breaches

Unauthorized modifications

Intentional

- Modify your bank account balance

Accidental

- Wrongly fill a form/document

(Network)Transmission errors

Impact of Integrity Breaches

Life safety

- **Damage to equipment / processes / people**
 - Stuxnet¹, 2010

Breach of contract

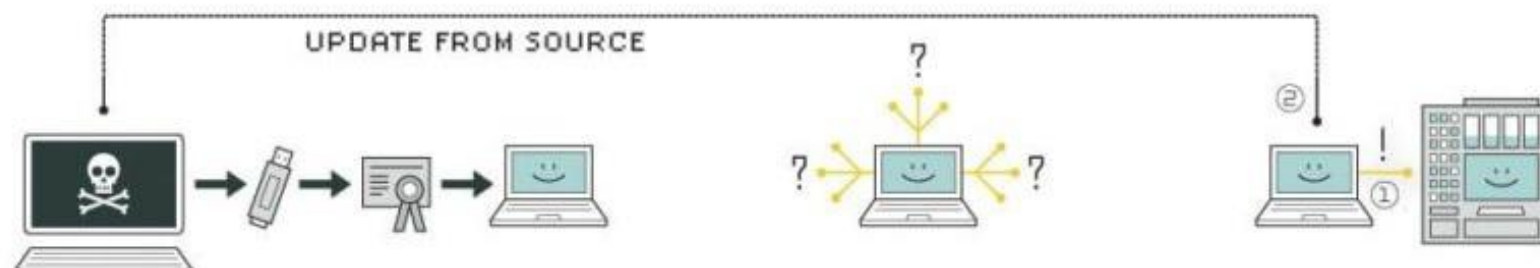
- Financial loss due to penalties
- Loss of customers

Reputational damage

- Poor control on process can damage business ecosystems relationship

Stuxnet

Attack Anatomy



1. infection

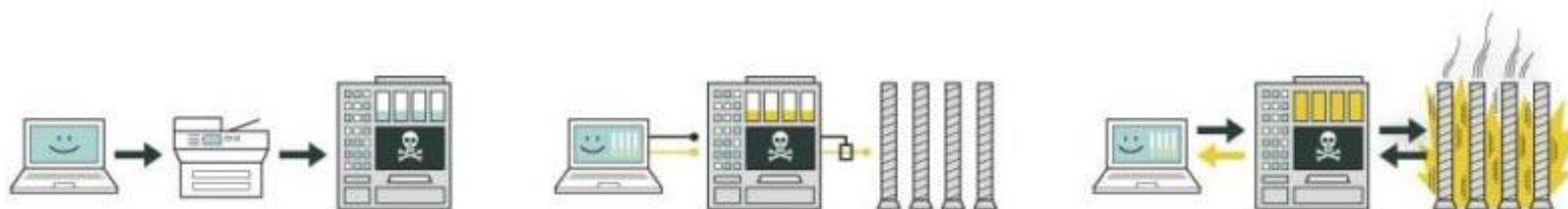
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Stuxnet

Mitigation Security Measures

Siemens released a detection and removal tool for Stuxnet

Automate Microsoft Security Update

Prohibit use of USB flash drives

Update Password Access Code

PLCs auditing for malware removal

Guarantee Integrity

Separation of duties

E.g. in a bank a single person has the complete control over a transaction. For example when getting a loan there are different people you encounter at each step. Also ensuring that the person approving your loan should not be related to you.

- Internal transaction control
 - Prevent & detect non-compliance and fraudulent activity
 - No single individual has sole control over the lifespan of a transaction
 - Reduces the risk of both erroneous and inappropriate actions
- Mutual exclusivity
 - No individual can input AND approve the same transaction
 - One person inputs travel expenses, and approve by somebody else
- Dual control
 - Tasks require the involvement of multiple parties.
 - Ensuring tasks are completed with oversight from more than one individual, enhancing accountability and security.

E.g. Cannot approve your own travel expense.

Enforce Integrity

The first two are transforming data into a fixed type string

Checksum

- **Purpose:** Verifies the integrity of data by generating a value representing the data's content.
- **Use Case:** Ensuring files are not altered or corrupted during storage or transmission.

Hashing

- **Purpose:** Transforms data into a fixed-size string of characters, typically a digest, which represents the data.
- **Use Case:** Verifying data integrity and securely storing passwords.

Digital Signature

- **Purpose:** Provides authentication and ensures data integrity by cryptographically signing documents.
- **Use Case:** Validating the authenticity and integrity of digital messages or documents.

Separation of Duties

- **Automate Service Requests:** Streamline service requests for IT and accounting departments to prevent manual errors and maintain control integrity.
- **Compile Audit Trails:** Maintain detailed logs of transactions and activities for accountability and traceability.
- **Enforce Role-Based Access Control (RBAC):** Limit users' access to systems and data based on their roles to enhance security.

Hashing

One-Way Function

A hash function is any function that can be used to map data of arbitrary size to fixed size data.

$$\forall m \in M, H(m) = n$$

For each m , n (*digest*) is unique.

It is impossible to recover m from n .

H easy to compute.

Its a one way function
which is not to encrypt
data but to maintain the
integrity of the data.

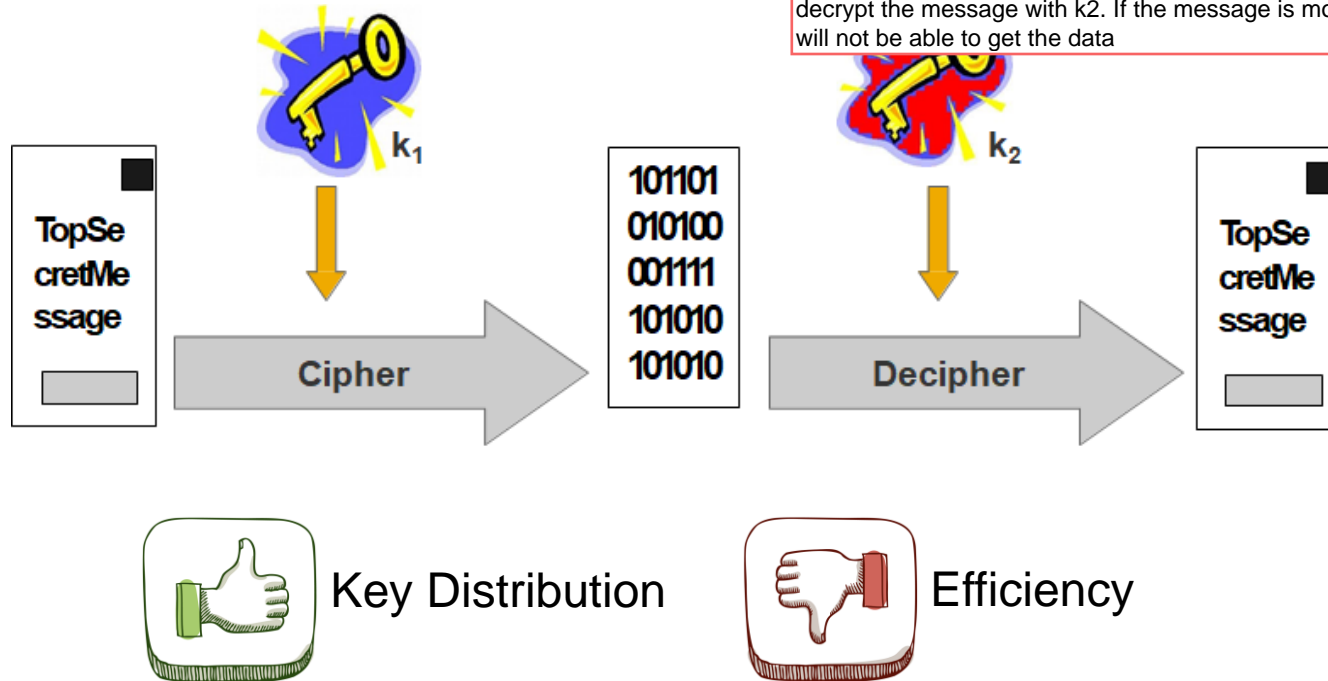
e.g. used for digital
signature.

Asymmetric Encryption

Can use it for integrity.

Here we use different keys for encryption and decryption. k_1 = public key and k_2 = secret key

Anyone can encrypt a message with k_1 and only the owner can decrypt the message with k_2 . If the message is modified then k_2 will not be able to get the data



Encryption $E(m, k_1)=c$

Decryption $D(c, k_2)=m$

Property $D(E(m, k_1), k_2)=m$

Ron Rivest, Adi Shamir, and Leonardo Adleman (**RSA**)

- Supported key size: multiple of 256, generally 2048 bits

$\{k_1, k_2\}$ is known as the public/private key pair $\{k_{\text{public}}, k_{\text{private}}\}$

- K_{public} is publicly known
- K_{private} is kept secret

If Bob encrypts a message to his k_{private} , he achieves

Message Integrity

Message
Confidentiality

This is technically
impossible

If Bob encrypts a message to his k_{private} , he achieves

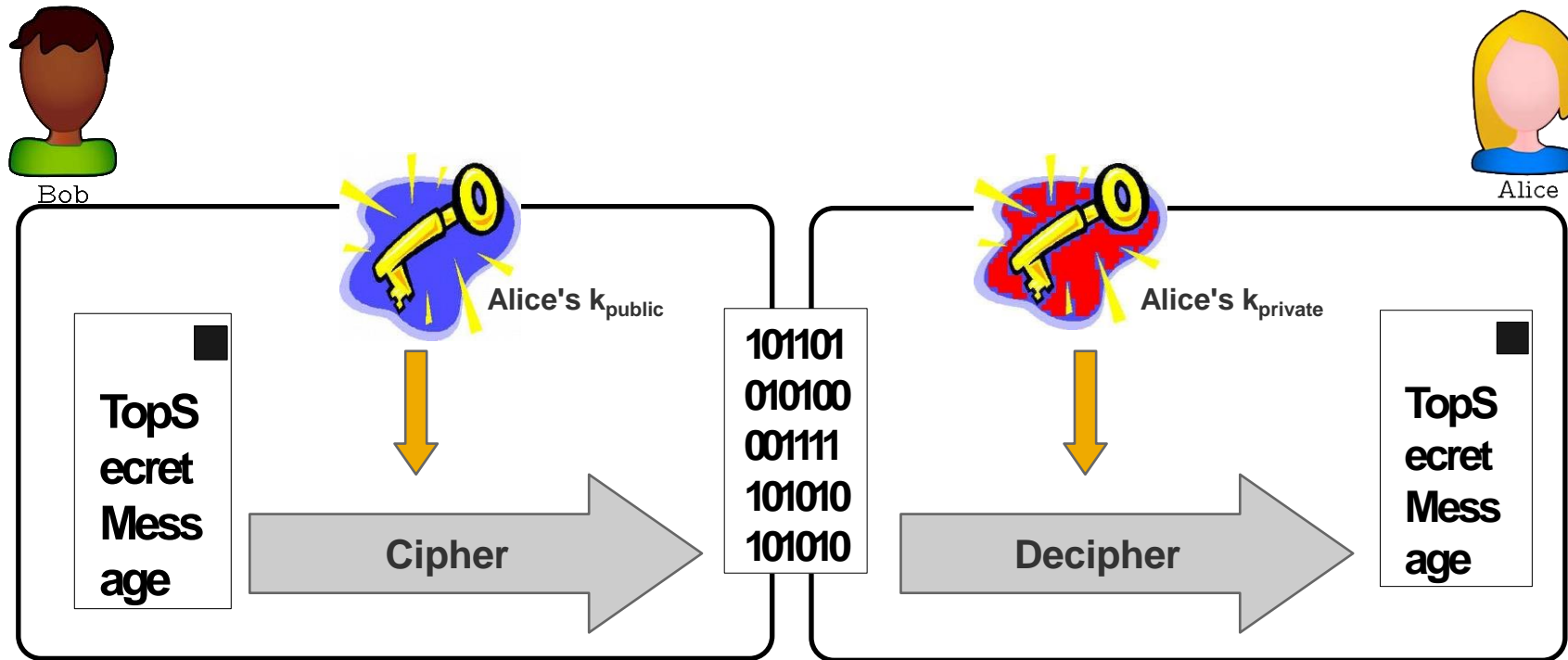
Message Integrity

Message
Confidentiality

This is technically
impossible

Asymmetric Encryption

Integrity



If Alice encrypts a message to Bob's k_{public} , she achieves

Message Integrity

Message
Confidentiality

This is technically
impossible

Anonymity

If Alice encrypts a message to Bob's k_{public} , she achieves

Message Integrity

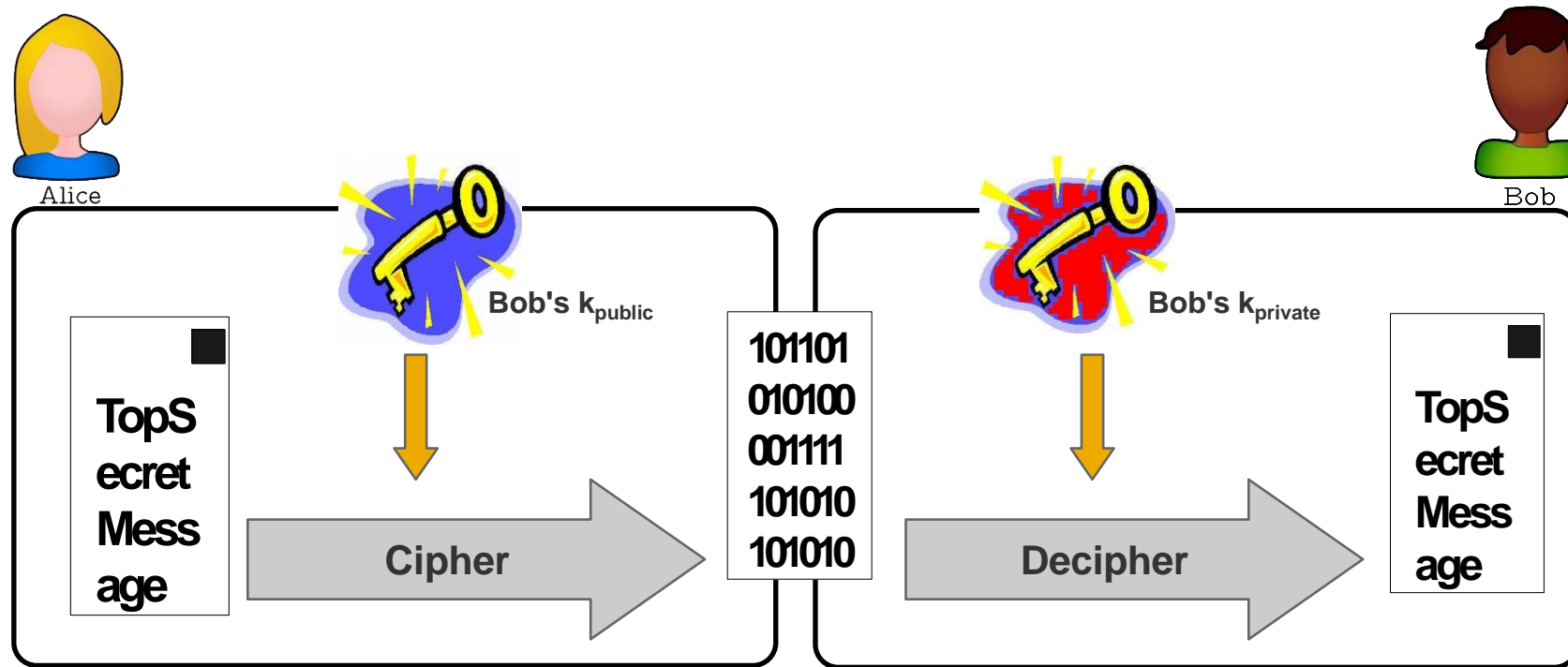
Message
Confidentiality

This is technically
impossible

Anonymity

Asymmetric Encryption

Confidentiality



Asymmetric En/Decryption in Python¹

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
import binascii

# GENERATE KEY PAIR
keyPair = RSA.generate(3072)

pubKey = keyPair.publickey()
print(f"Public key: (n={hex(pubKey.n)}, e={hex(pubKey.e)})")
pubKeyPEM = pubKey.exportKey()
print(pubKeyPEM.decode('ascii'))

print(f"Private key: (n={hex(pubKey.n)}, d={hex(keyPair.d)})")
privKeyPEM = keyPair.exportKey()
print(privKeyPEM.decode('ascii'))

# ENCRYPT with PUBLIC KEY
msg = b'A message for encryption'
encryptor = PKCS1_OAEP.new(pubKey)
encrypted = encryptor.encrypt(msg)
print("Encrypted:", binascii.hexlify(encrypted))

# DECRYPT with PRIVATE KEY
decryptor = PKCS1_OAEP.new(keyPair)
decrypted = decryptor.decrypt(encrypted)
print('Decrypted:', decrypted)
```

Digital Signature

A **digital signature** of a message is a number dependent on some secret known only to the signer, and, on the content of the message being signed

Security goals

Message integrity

Non repudiation of origin of the message

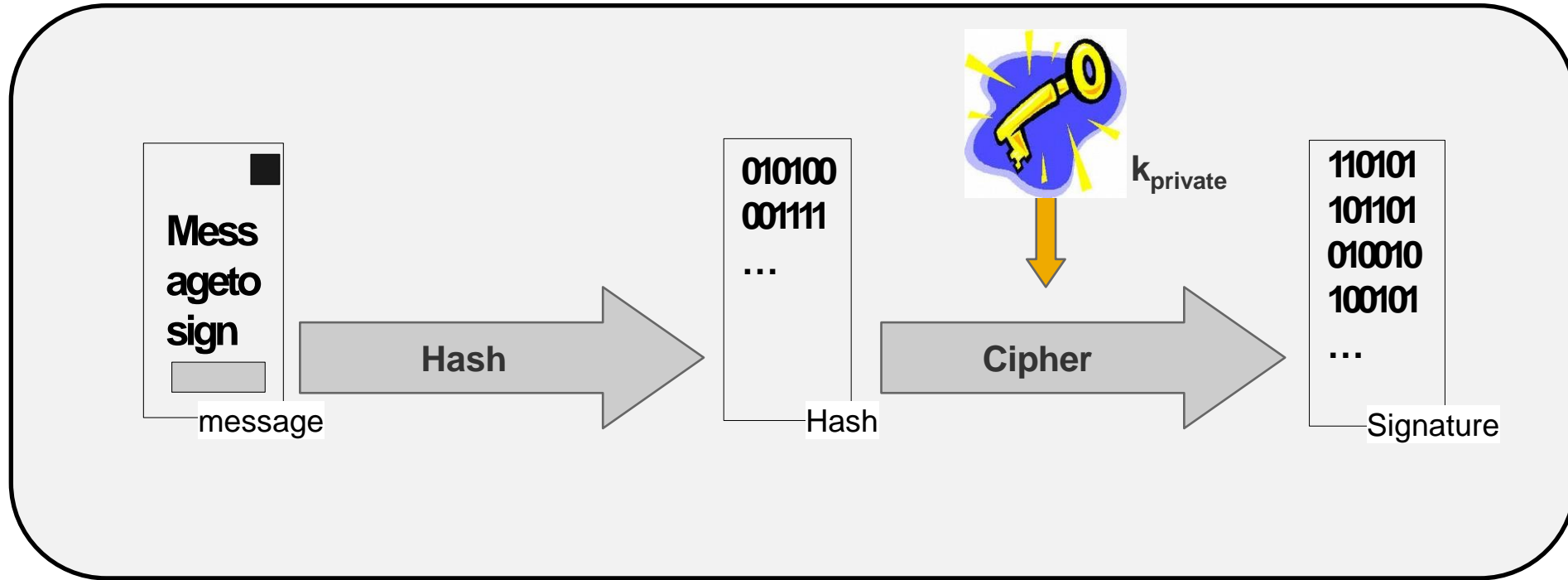
Digital signature schemes is composed of

Signature processing

Verification

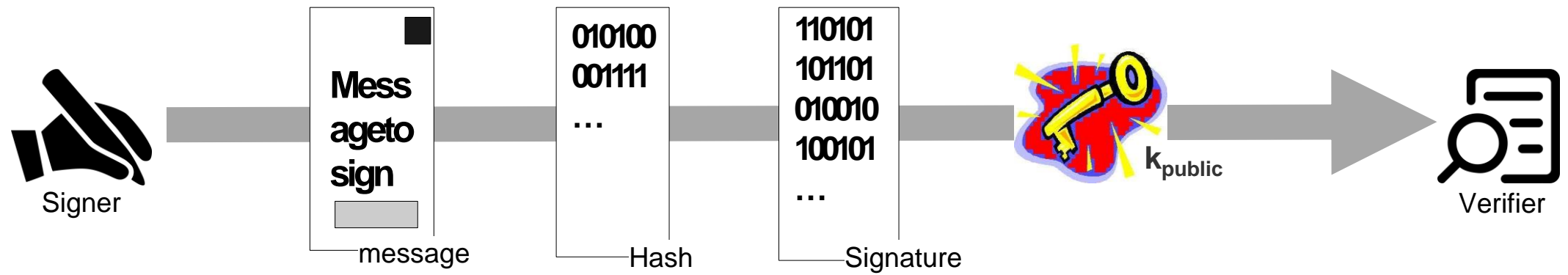
Digital Signature

Signature Processing

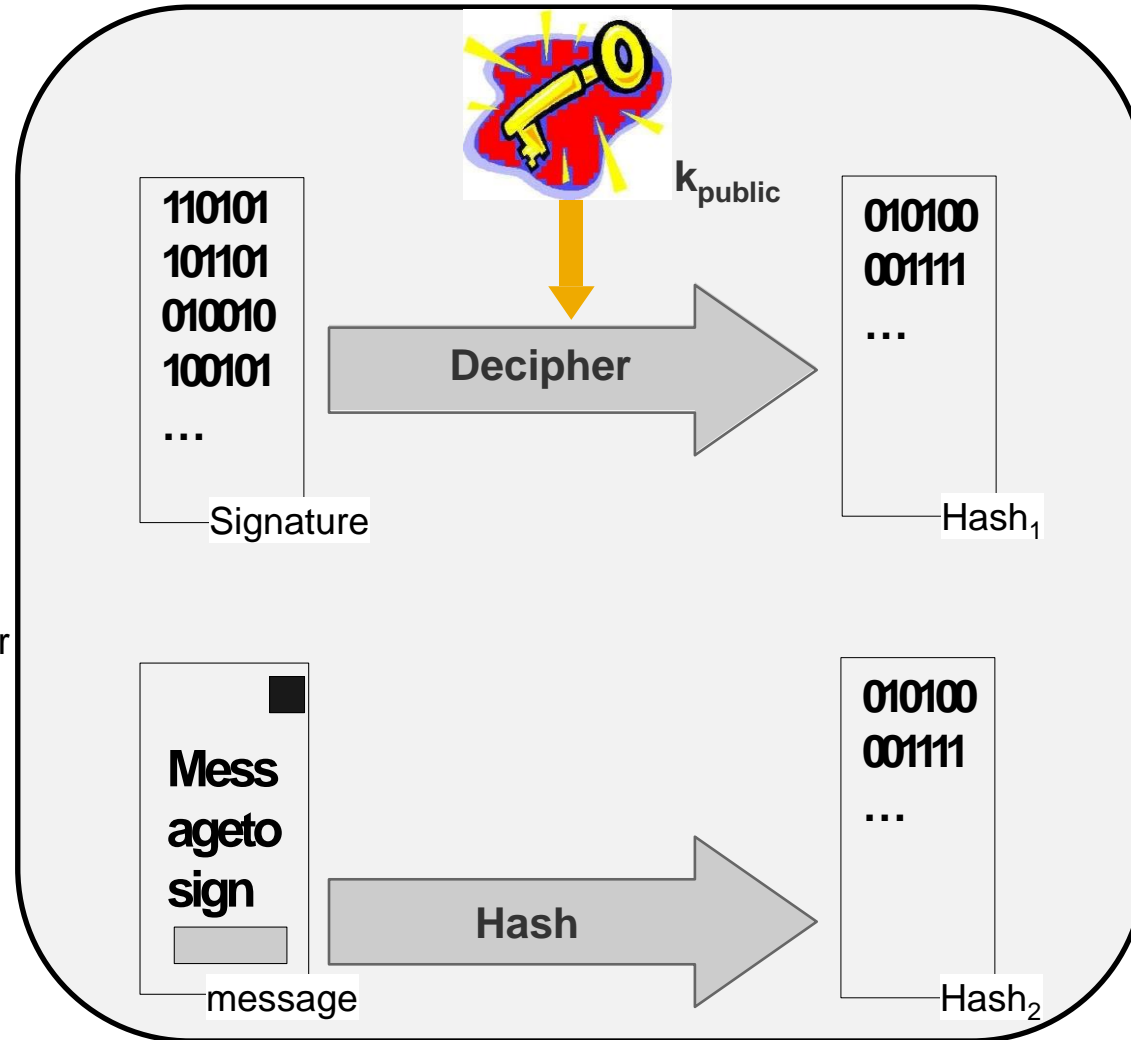


$$\text{Cipher}(k_{\text{private}}, \text{Hash}(\text{message})) = \text{Signature}(\text{message})$$

Digital Signature



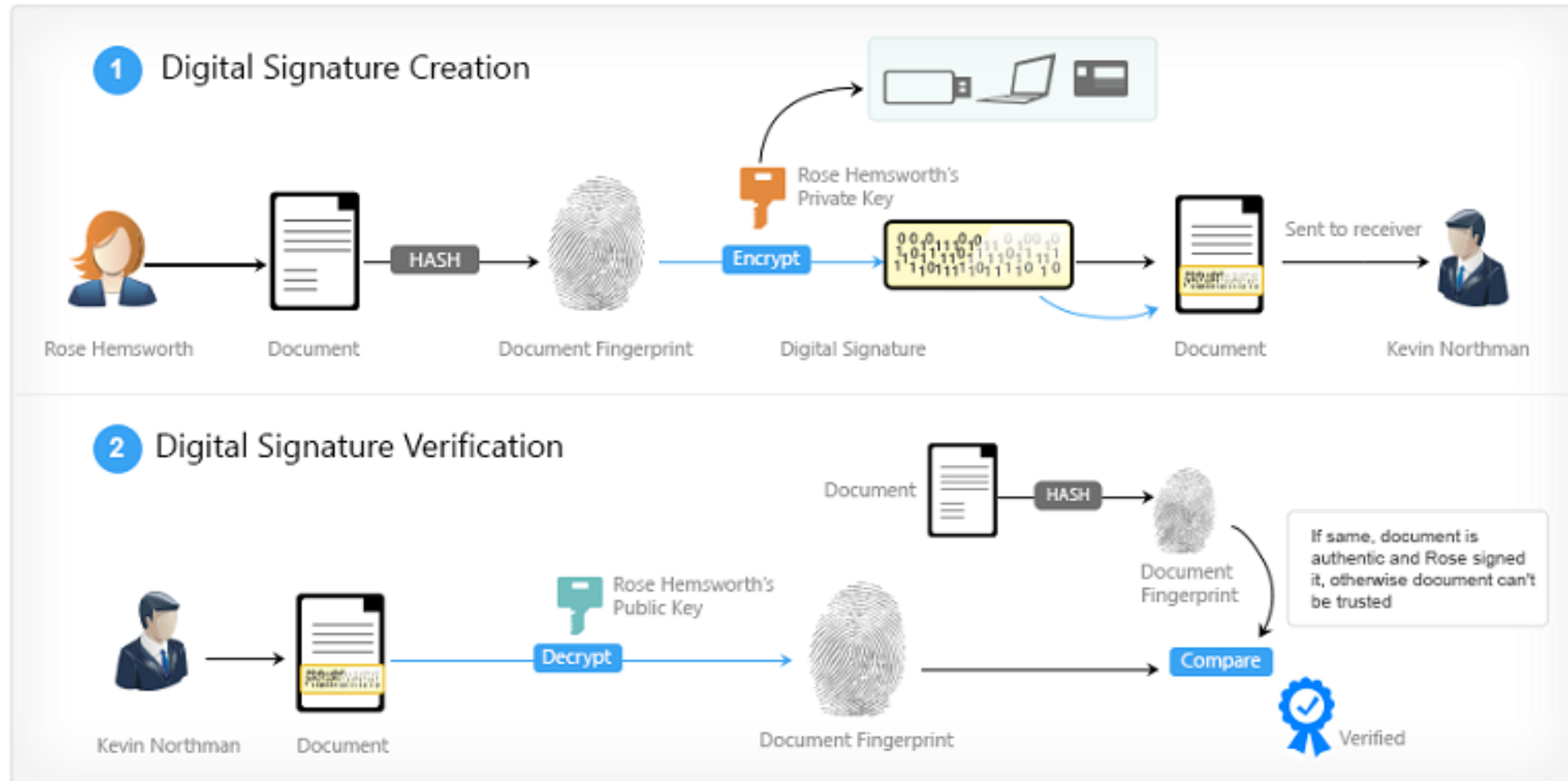
Digital Signature Verification



**The digital signature is valid
only if $\text{Hash}_1 = \text{Hash}_2$**

If somebody has modified the signature the hash of the message will be different to the hash on the system.

Digital Signature



Source: [4points](#)

Enforce Integrity

Policy

- Clear specification of entities with modification access rights.
- **Control Implementation:** Effective policies to enforce access restrictions.

Access Control

- **Separation of Duties:** Ensures no single individual has complete control over critical functions.
- **Role-Based Access Control (RBAC):** Limits access based on predefined roles.

Not based on identity but
roles

Input Validation

- **Error Checking:** Validates all inputs to prevent erroneous or malicious data entries.
- **Data Integrity Checks:** Ensures consistency and accuracy of input data.

Audit

- **Policy Enforcement Documentation:** Comprehensive records of policy enforcement for accountability.
- **Regular Audits:** Scheduled audits to ensure continuous compliance and identify areas for improvement.

Availability

“Sound easier to accomplish than it really is !!!

Guarantee reliable and timely access to resources

- Data network
 - High uptime and redundancy
- Systems
 - Robust infrastructure and failover mechanisms
- Process
 - Streamlined operations and quick incident response
- People
 - Skilled staff and clear roles

Availability Breaches

Intentional disruption of service

DoS (Denial of Service)

Overloading a server to disrupt access (e.g., Ping of Death).

DDoS (Distributed Denial of Service)

Multiple systems flood the bandwidth (e.g., Mirai Botnet attack).

Malware/Ransomware

Infecting systems for malicious control or extortion (e.g., WannaCry ransomware).

Sabotage

Deliberate damage to systems or data by insiders or outsiders (e.g., disgruntled employee deleting critical files).

Accidental

Deletion of Wrong File

Unintended deletion causing data loss (e.g., accidentally deleting an important database).

Misconfiguration

Incorrect system settings leading to downtime (e.g., wrong firewall configuration blocking network traffic).

Power Off

Switching off critical servers accidentally (e.g., unplugging the wrong power cable, causing a data center outage).

Availability Breaches

Failure

Hardware Failure

Physical component malfunction (e.g., a server hard drive crash).

Software Failure

Errors or bugs in applications (e.g., software update introducing critical bugs).

Natural Events

Flooding

Water damage affecting data centers (e.g., data center flooded during Hurricane Katrina).

Pandemic

Disruption due to widespread health crisis (e.g., COVID-19 impacting IT staff availability).

Utility Failure

Power

Electricity outages disrupting services (e.g., regional blackouts).

Network

Connectivity loss preventing access (e.g., ISP failure causing widespread internet downtime).

Impact of Availability Breaches

Life safety

- Medical equipment
- [Düsseldorf Hospital Ransomware Attack](#), 2020

Disruption of operations

- Delay in production
- Violation of regulatory
- Violation of contractual terms and conditions
 - Cloud, network
 - OVH case (data hostage timing/loss of data)



Guarantee Availability

Avoid Business Disruption

Replication

Replicating across
different areas

Backups:

Daily server backups to secure data (e.g., nightly database backups).

Redundancy

Alternate or Diverse Networks:

Using multiple ISPs to ensure continuous internet access (e.g., primary and secondary internet connections).

Media Mirroring:

Duplicating data across different storage media (e.g., RAID configurations).

Clustering

Server Clusters:

Multiple servers working as a single system for load balancing and failover (e.g., web servers in a cluster).

Scalability

Resource Capacity Checks:

Ensuring computational power and network expand to meet demands (e.g., auto-scaling groups in cloud infrastructure).

Resiliency

Failover:

Automatic switch to a standby system (e.g., hot standby datacenters).

Fault Tolerance:

Automated recovery systems (e.g., error handling in software to retry failed operations).

Disaster Management:

Comprehensive plans to handle catastrophic failures (e.g., emergency protocols for data recovery after a natural disaster).

Enforce Availability

Ensuring Continuous Operations

Policies

- Recognize criticality:
Identify and prioritize critical systems and processes to ensure they receive the appropriate resources and attention.

Security by Design

- Identification of Single Points of Failure:
Assess systems to detect and eliminate vulnerabilities that could cause complete system failure.
- Load balancing:
Distribute workloads evenly across resources to prevent any single system from being overwhelmed.

Access Control

- Least Privilege enforcing read only:
Enforce the minimum level of access necessary for users to perform their duties, such as read-only permissions when appropriate, to mitigate risk.

Cross training

- Sustain critical business operation when key personnel is unavailable:
Ensure critical operations can continue when key personnel are unavailable by cross-training staff and documenting procedures.

Guarantee that all essential tasks can continue even if key person is not available

Non Repudiation

Protect the interest of all parties involved in a transaction

Prevent transaction denial

- Non repudiation of origin
- Non repudiation of receipt

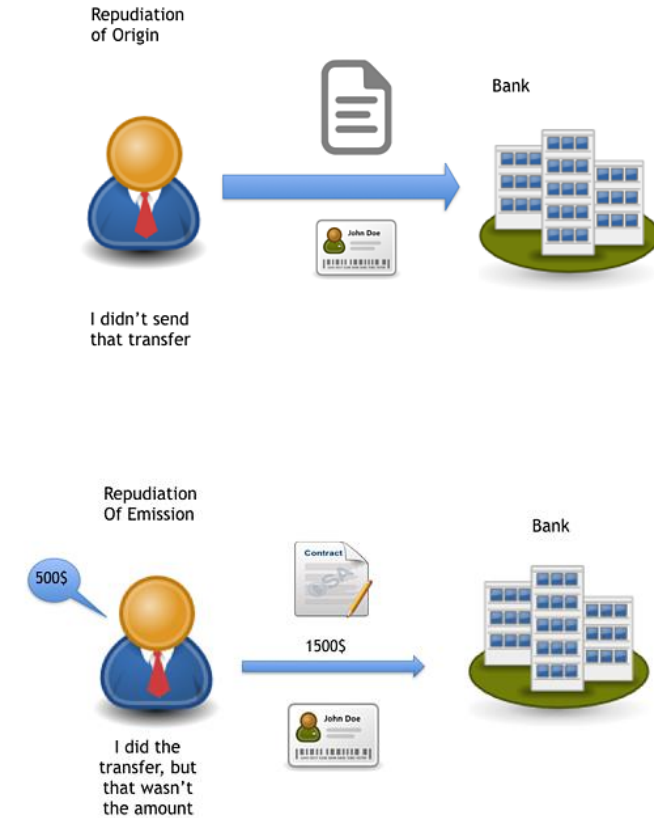
E.g. a customer can cannot deny a transaction happening. And the receipient cannot deny that they have not received the trasnaction.

This can be doen through a digital signature, logs etc.

Proof linking an action to an identity

- Electronic contract
- Logs
- Digital Signature

Essential for business trustworthiness



Source: [Cryptomathic](#)

Non-Repudiation Breaches

Inability to Link an Activity to an Identified Entity

Activity is untraceable to a specific individual.

Deletion of Logs

Logs that track actions are erased, removing traceability.

Falsification of Digital Signature

Digital signatures are forged, compromising authenticity.

Shared ID

Multiple users share the same credentials, making it impossible to determine who performed an action.

Invalid Linkage

Incorrect linking of an action to an identity.

Falsification of Identity / Fake Certificate

Using false identities or counterfeit certificates to misrepresent authenticity.

Impact of Non-Repudiation Breaches

Loss of Trust

Customers and partners lose faith in the application|system.

Lack of Evidence for Further Investigation

Inability to trace and resolve incidents.

Breach of Contract

Legal and financial repercussions.

Establishing Trust is Crucial in Business Operations

Vital for digital interactions and transactions.

Guarantee Non-Repudiation

Access control

- Preventing shared ID

Digital signature

- Distributed ledgers

Protection of logs

- Ensuring tamper proof records

Public Key Infrastructure

- Verifying and securing the communications

Authenticity of

- Transactions: through process certification
- Identity: Ensuring verified identities

Enforce Non-Repudiation

Digital Certificates and Signature

- Verify the identity of parties and guarantee the integrity of digital documents

Multi-factor Authentication

- Use multiple authentication methods to verify user identities, reducing the risk of unauthorized access.

Audit Trails and Logging

- Maintain detailed records of all transactions and activities for accountability and forensic analysis.

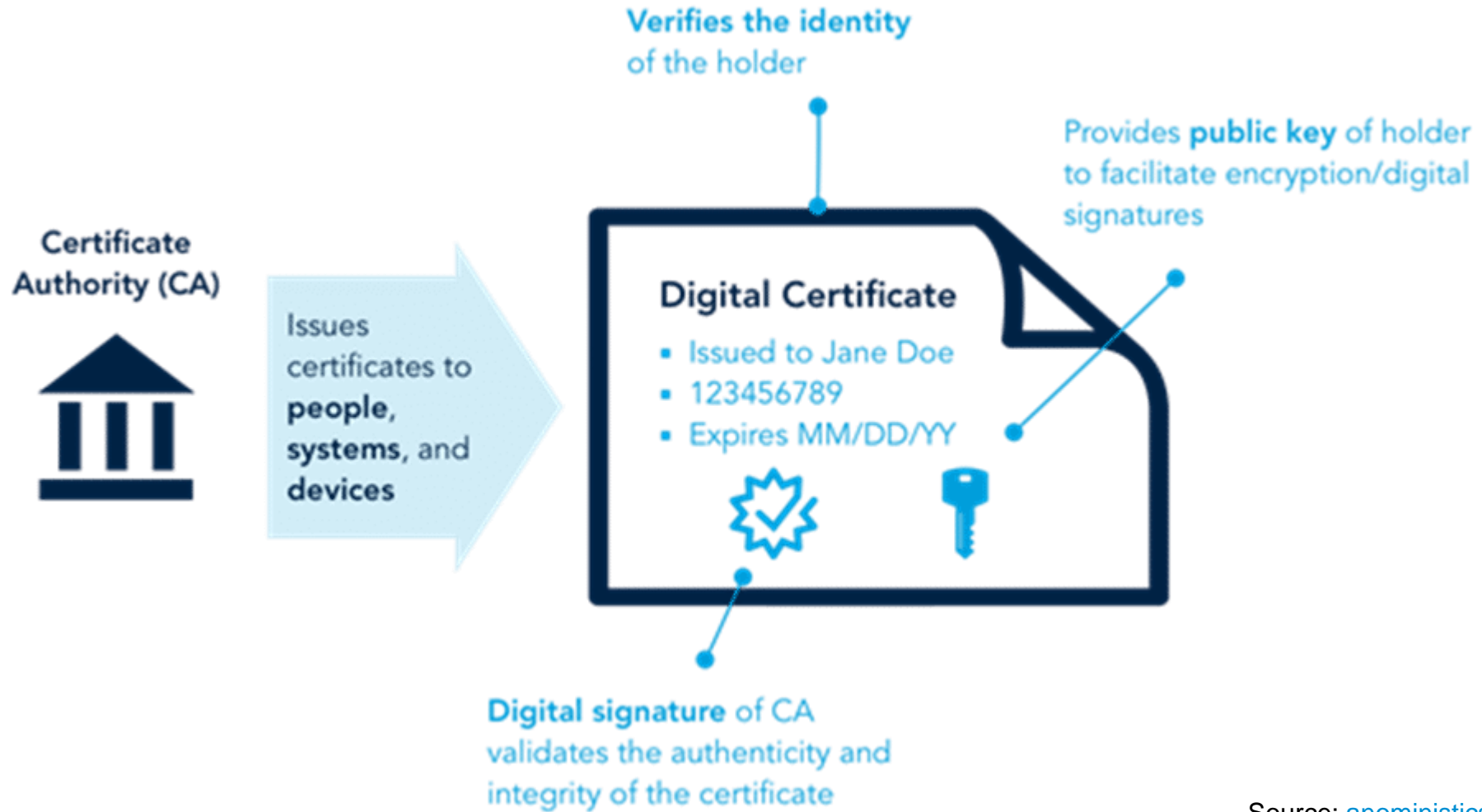
Legal and Binding Agreement

- Ensure that all digital agreements are legally binding and enforceable in a court of law

Legal and Regulatory Compliance

- Comply with industry-specific regulations and standards to ensure legal accountability and maintain trust.

Digital Certificates



Source: [anoministics](#)

Key Take Away

Safety is the top priority !



Cybersecurity is the art of protecting organizational assets from attacks. It comprises of an evolving set a tools, risk management approaches, technologies, training and best practices [1](#)


Security is only as strong as its weakest link.

Security aims at balancing Confidentiality, Integrity and Availability security objectives, based on organization operational environment and business strategy.

No organization is 100% secure

Thank you.


Contact information:




Dr. Gomez Laurent
Security Testing Automation Lead | CPIT

SAP Labs France
805 Avenue Dr. Donat
06250 Mougins

laurent.gomez@sap.com





Follow us



www.sap.com/contactsap

© 2021 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/trademark for additional trademark information and notices.