Critical Infrastructure Security

Lecture 3

Dr. Naveed Anwar Bhatti

Webpage: naveedanwarbhatti.github.io

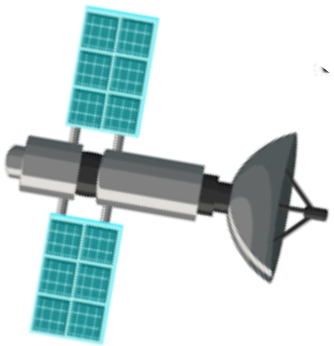
Administrative

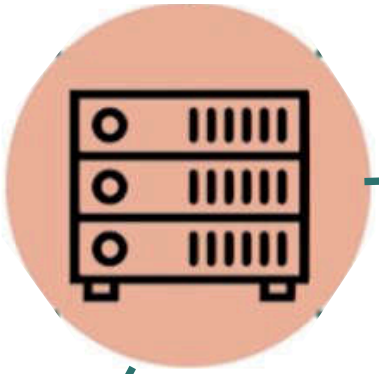
Presentation Schedule

Presentation Date	Papers	Presentation	Opponent	Defender
		Student Name (Roll No.)	Student Name (Roll No.)	Student Name (Roll No.)
7th March 2022	Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective	Hamda Tehami(220283)	Muhammad Hannan(220371)	Shajeera Tehami(220284)
7th March 2022	Who's in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems.	Shajeera Tehami(220284)	M. Bilal Rasool (220337)	Hamda Tehami(220283)
21st March 2022	Cyber-security on smart grid: Threats and potential solutions	Hamda Tehami(220283)	Muhammad Hannan(220371)	Shajeera Tehami(220284)
21st March 2022	Lest We Remember: Cold Boot Attacks on Encryption Keys	M. Bilal Rasool (220337)	Shajeera Tehami(220284)	Muhammad Hannan(220371)
11th April 2022	RFDIDS: Radio Frequency-based Distributed Intrusion Detection System for the Power Grid	Muhammad Hannan(220371)	Shajeera Tehami(220284)	M. Bilal Rasool (220337)
11th April 2022	Light commands: laser-based audio injection attacks on voice-controllable systems	M. Bilal Rasool (220337)	Hamda Tehami(220283)	Muhammad Hannan(220371)
25th April 2022	What You Corrupt Is Not What You Crash: Challenges in Fuzzing Embedded Devices	Shajeera Tehami(220284)	M. Bilal Rasool (220337)	Hamda Tehami(220283)
25th April 2022	Adversarial Attacks against LiDAR Semantic Segmentation in Autonomous Driving	Muhammad Hannan(220371)	Hamda Tehami(220283)	M. Bilal Rasool (220337)

Background: Network and Security

What is Computer Network?





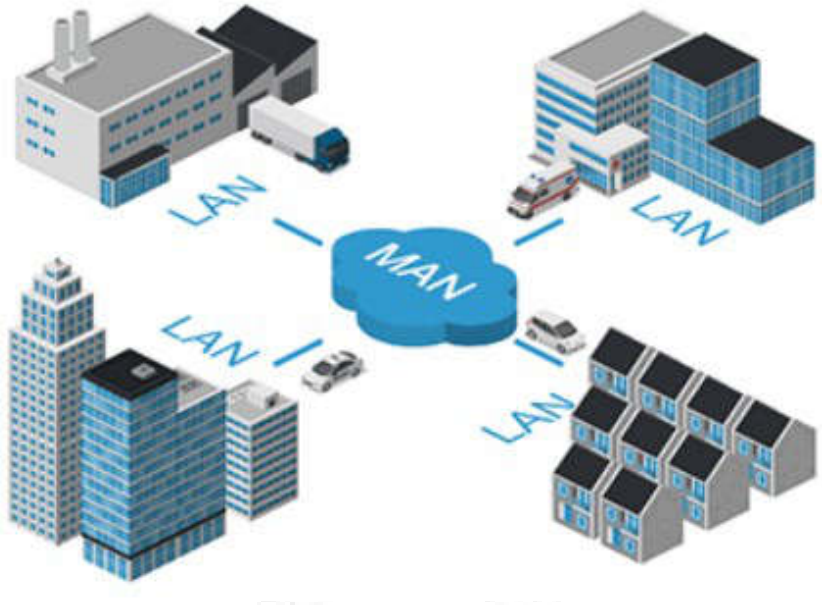
Types of Network

Body Area Network

Types of Network

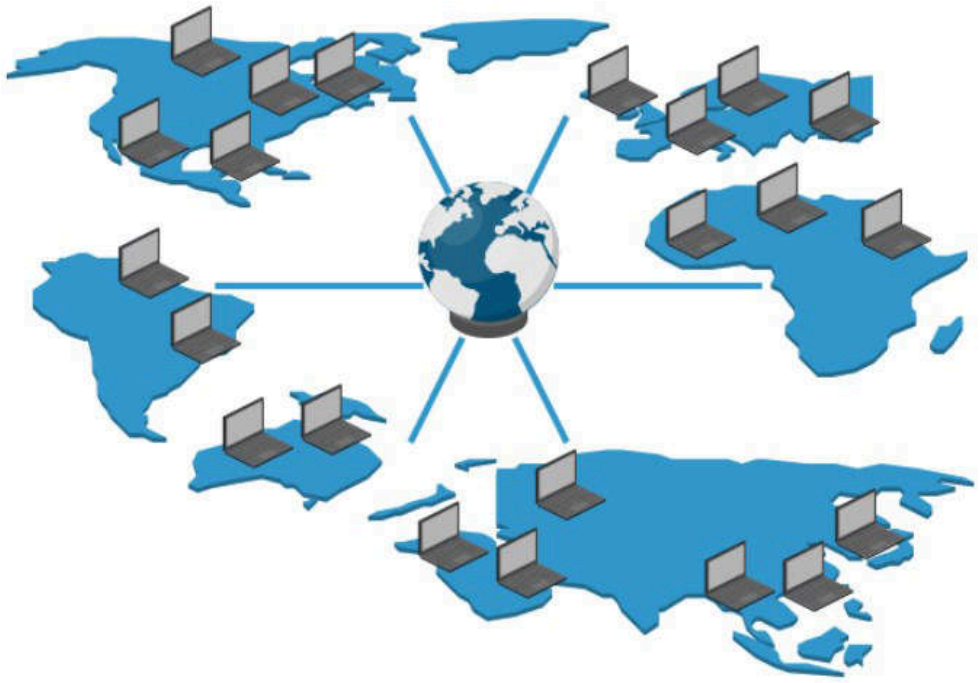
Local Area Network

Types of Network



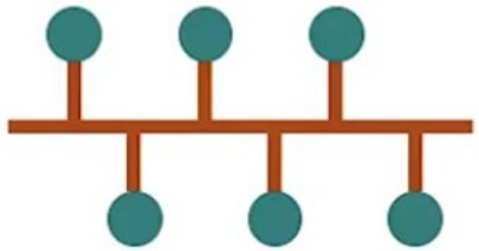
Metropolitan Area Network

Types of Network



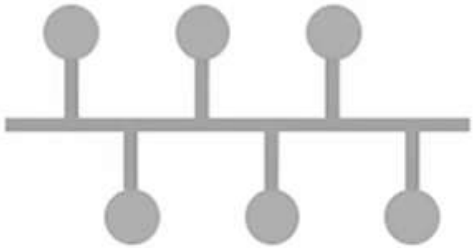
Wide Area Network

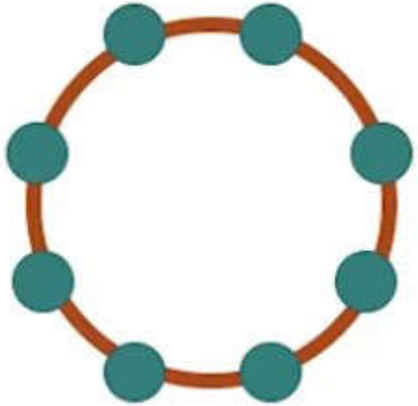
Network Topology



Bus Topology

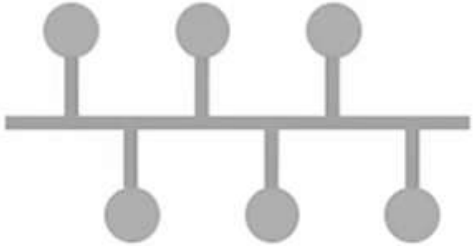
Network Topology



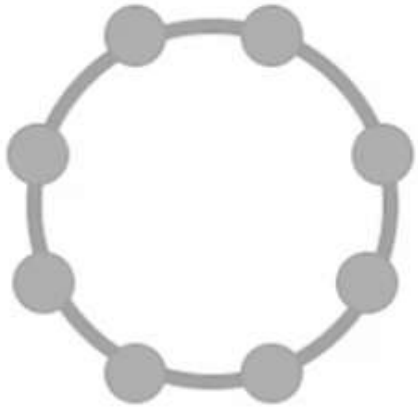


Ring Topology

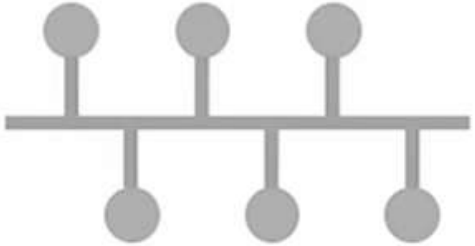
Network Topology

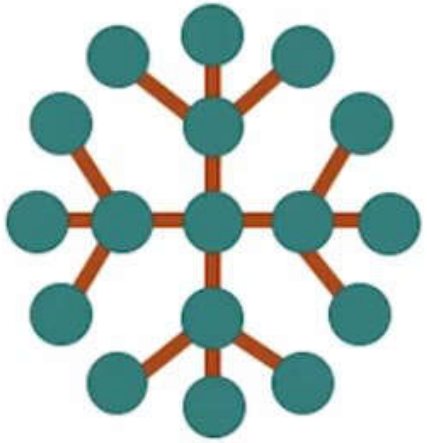


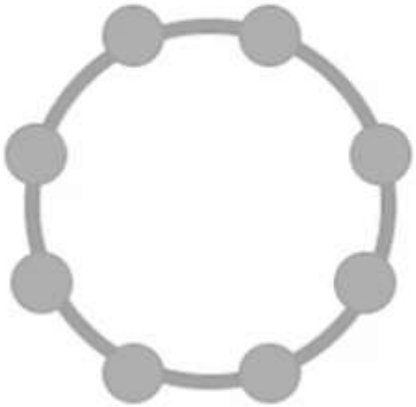
Star Topology



Network Topology

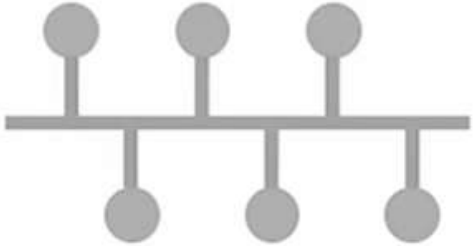


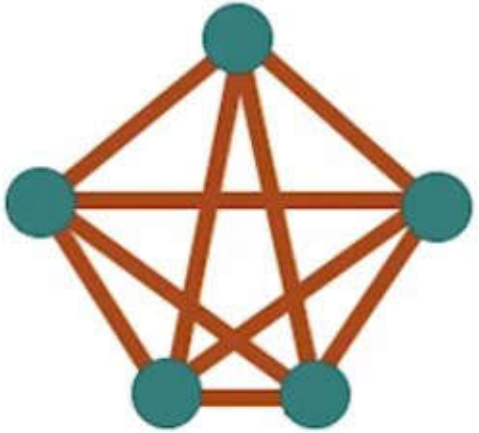




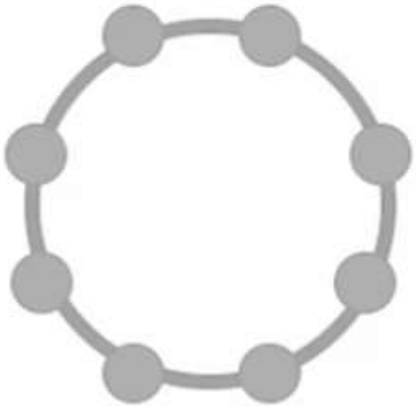
Extended Star Topology

Network Topology





Mesh Topology



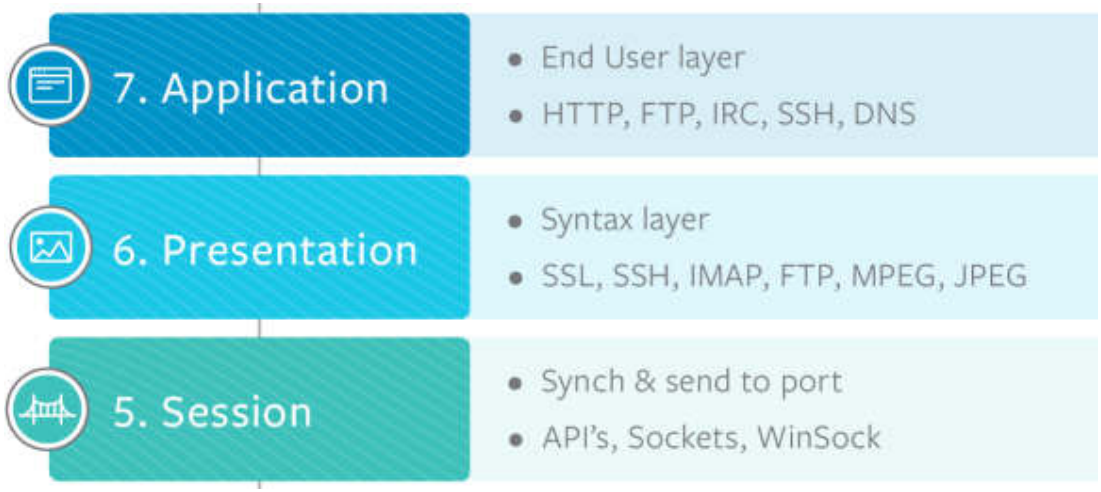
OSI Model

To Allow Access to Network resources

OSI Model

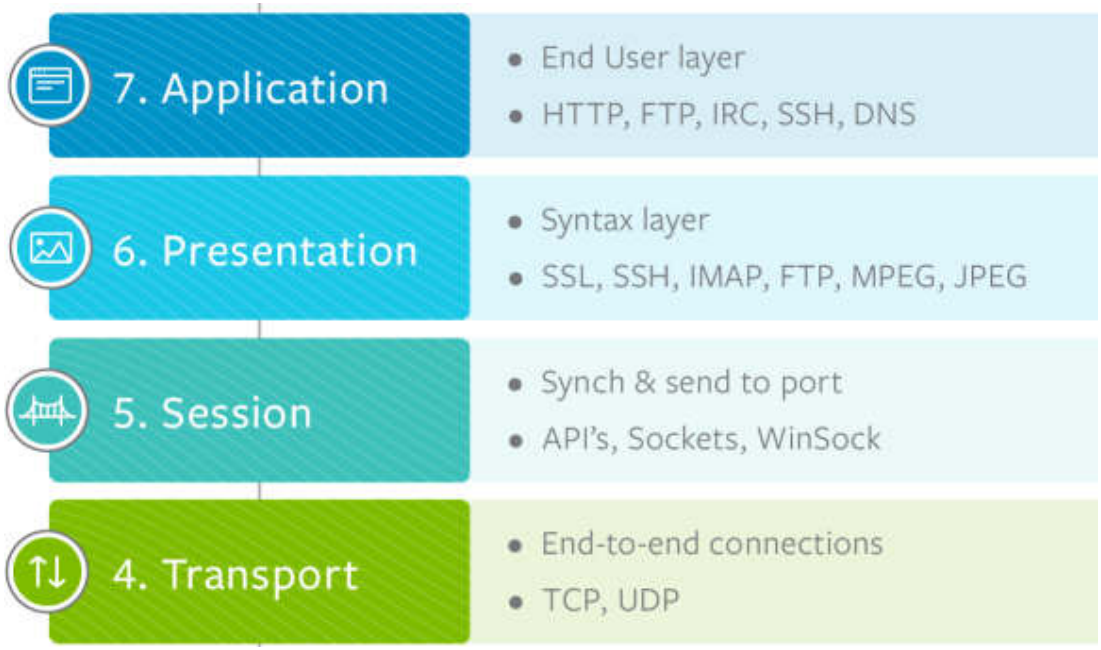
To translate encrypt and compress data

OSI Model



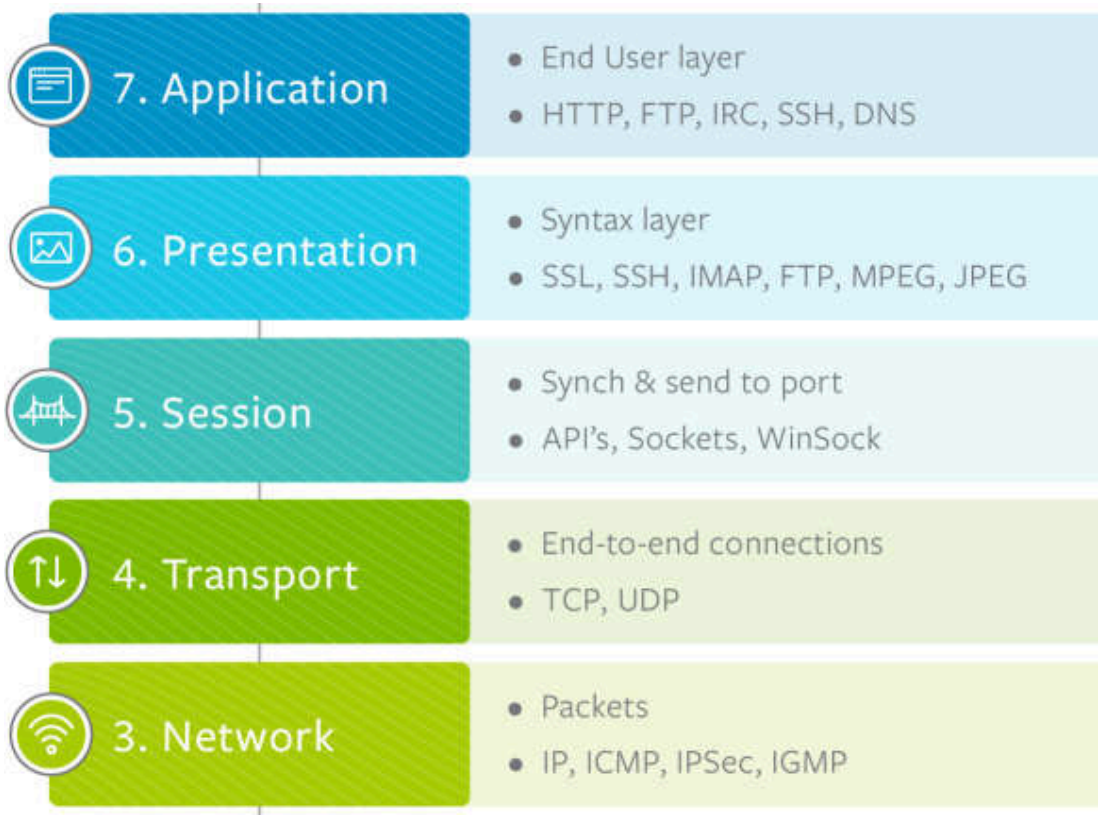
To establish, manage and terminate sessions

OSI Model



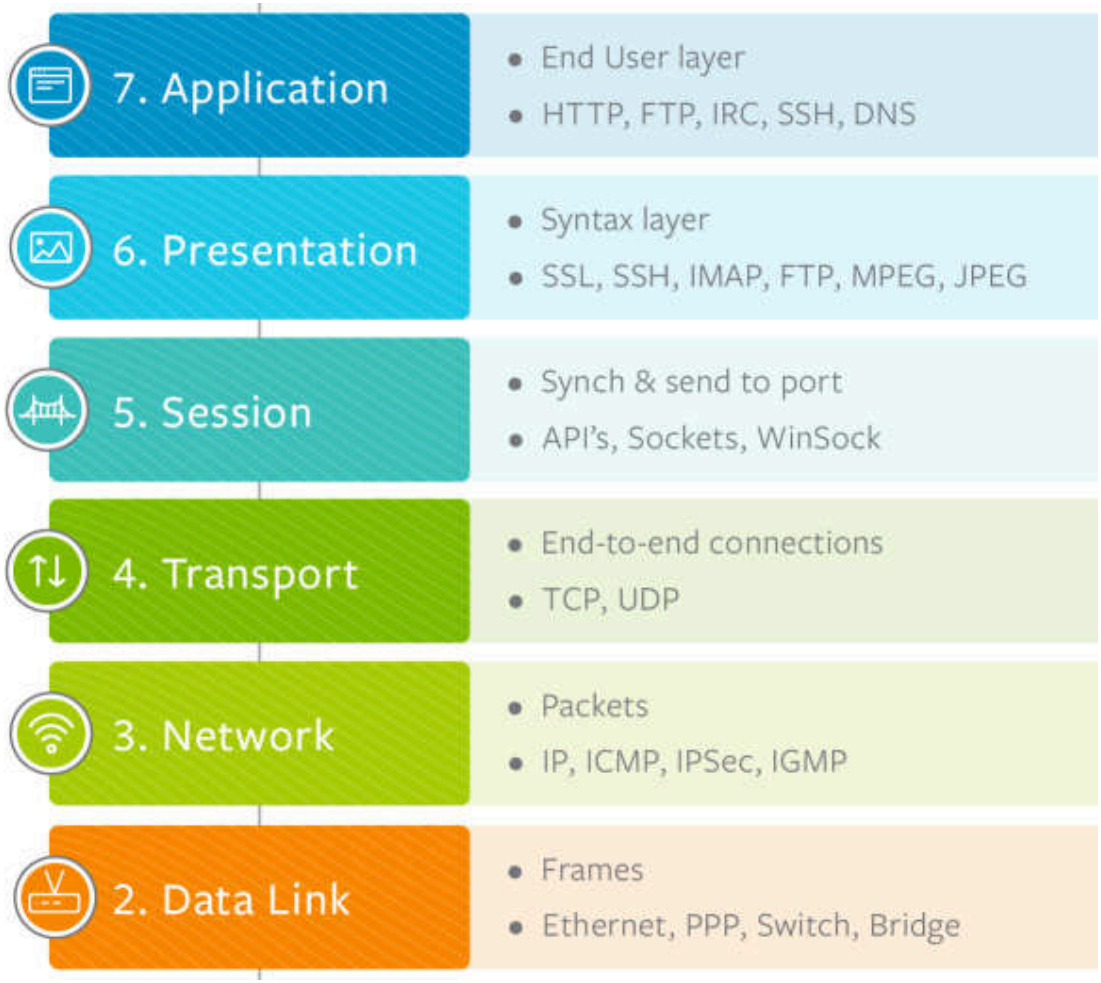
Reliable process-to-process message delivery

OSI Model



Packet transport and internetworking

OSI Model

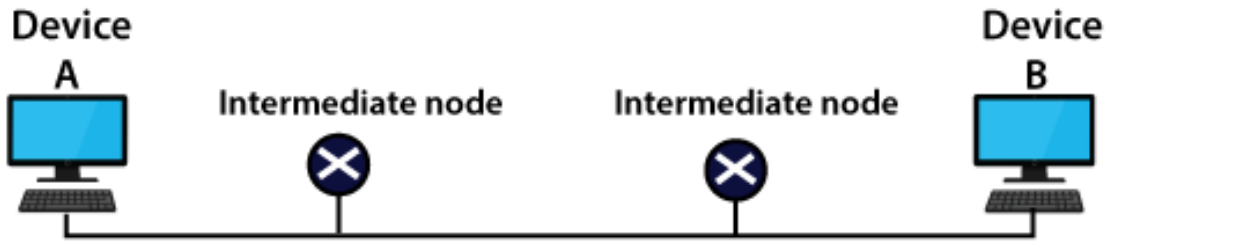


Bits->frames, hop-to-hop delivery

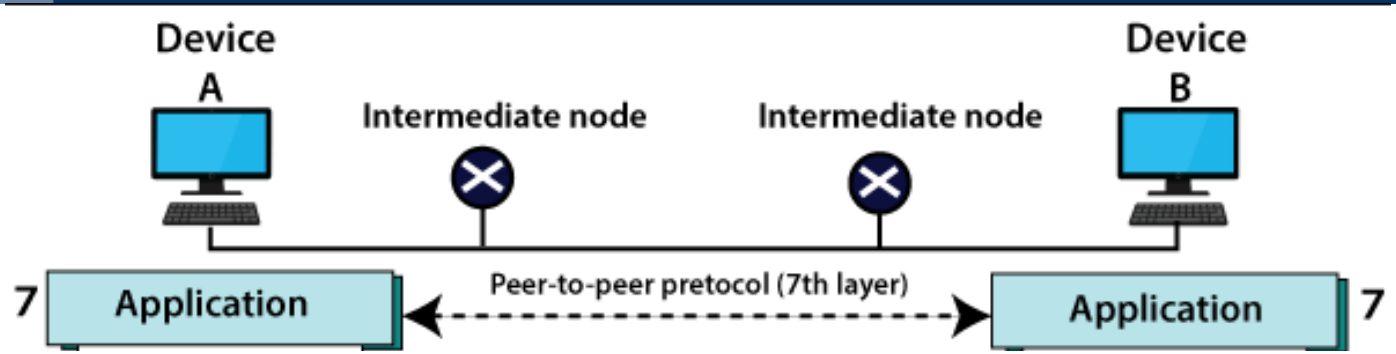
OSI Model

Transmits bits over physical medium

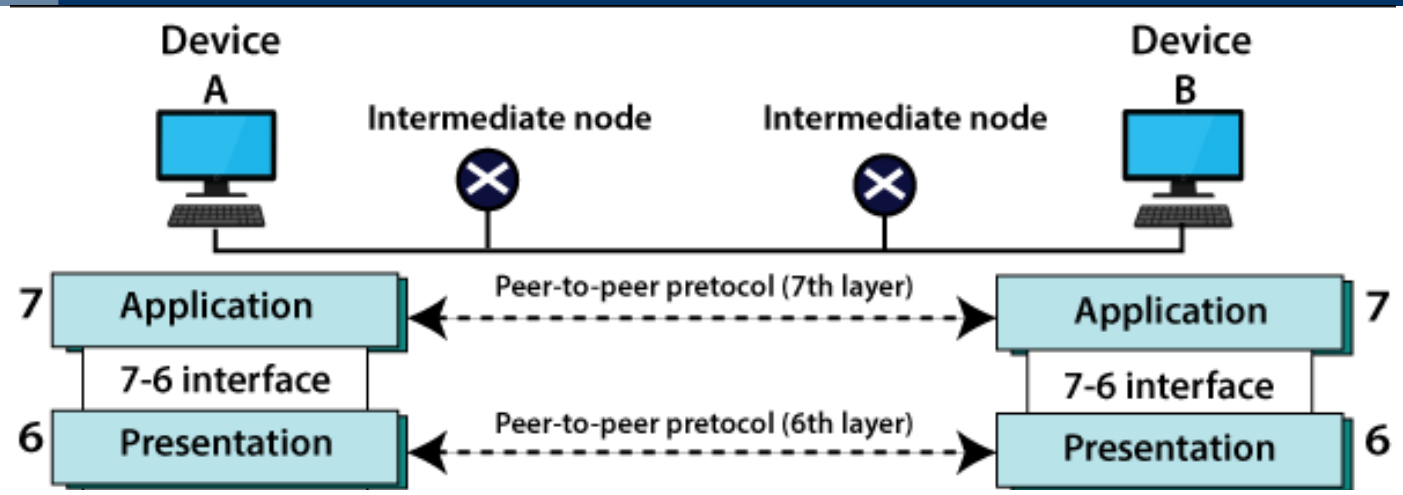
OSI Layer



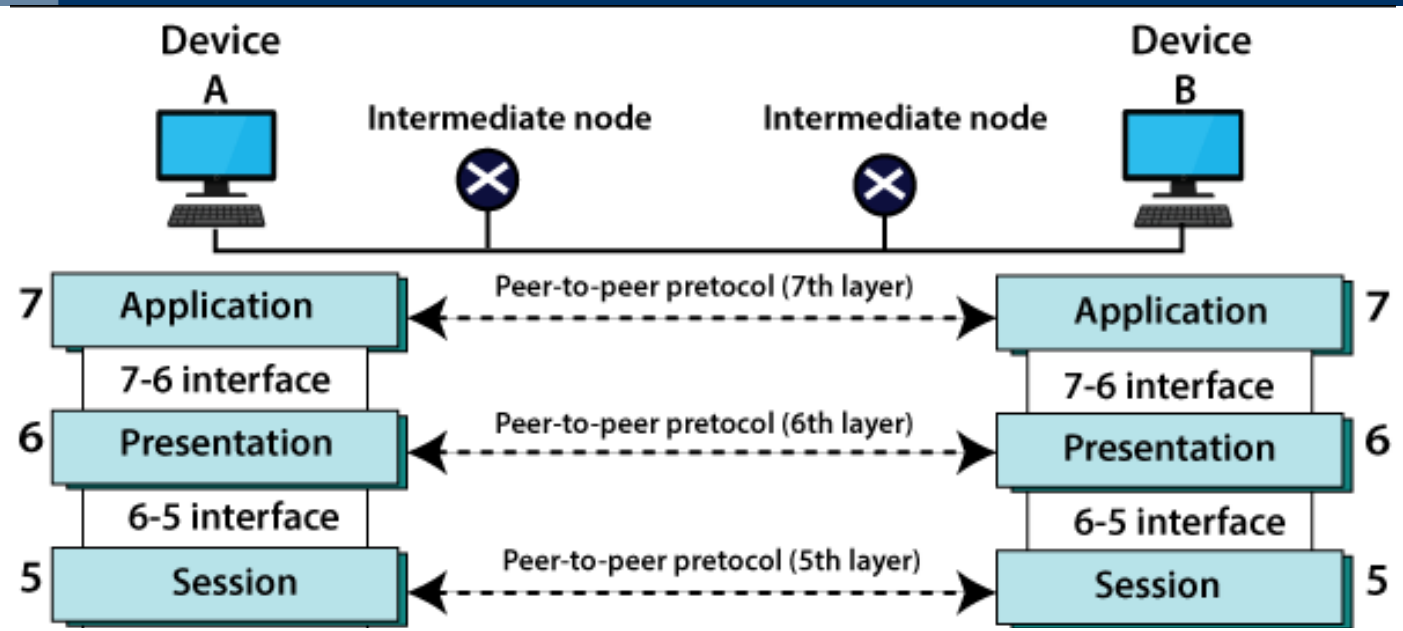
OSI Layer


Device
A
Intermediate node
Intermediate node
Device
B
7
Application
Peer-to-peer pretocol (7th layer)
Application
7

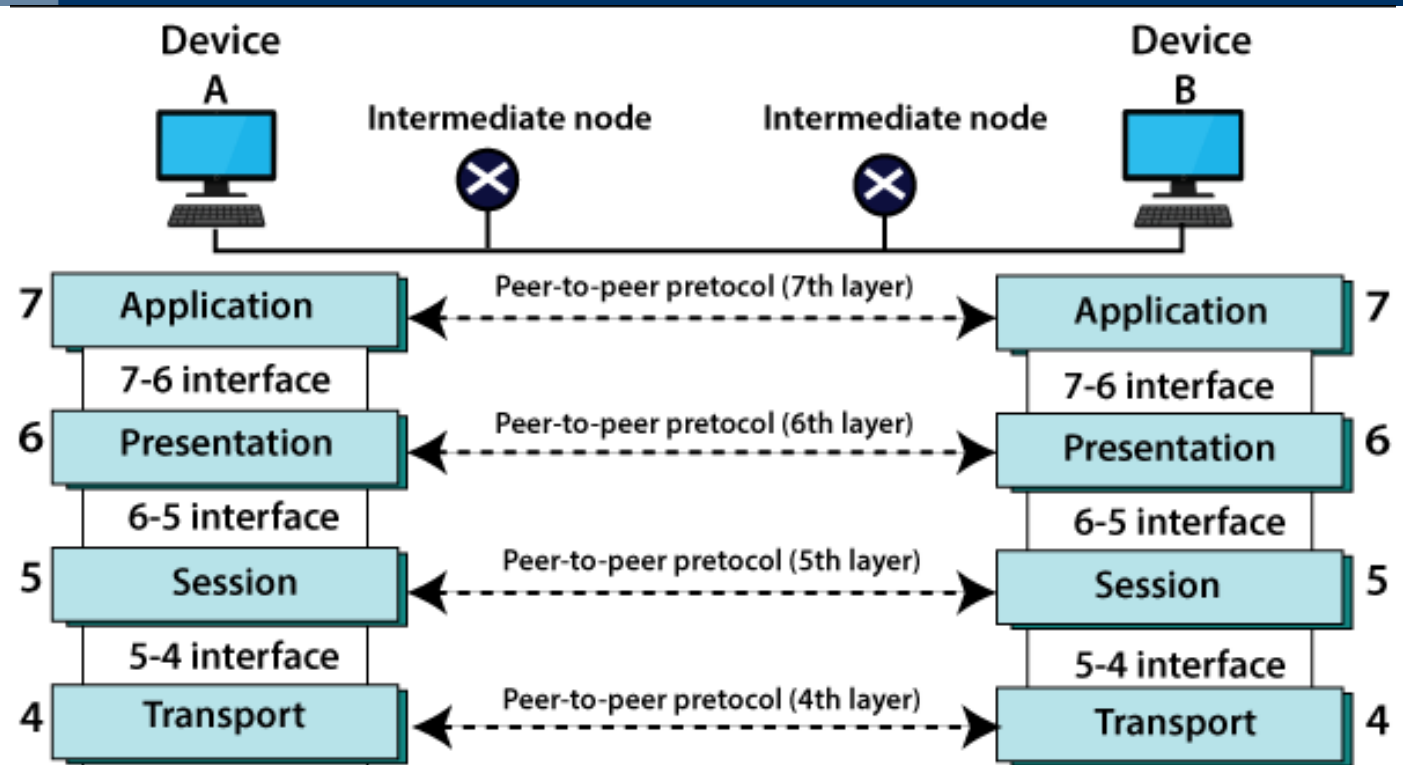
OSI Layer


Device
A
Intermediate node
Intermediate node
Device
B
7
Application
Peer-to-peer pretocol (7th layer)
Application
7
7-6 interface
7-6 interface
6
Presentation
Peer-to-peer pretocol (6th layer)
Presentation
6

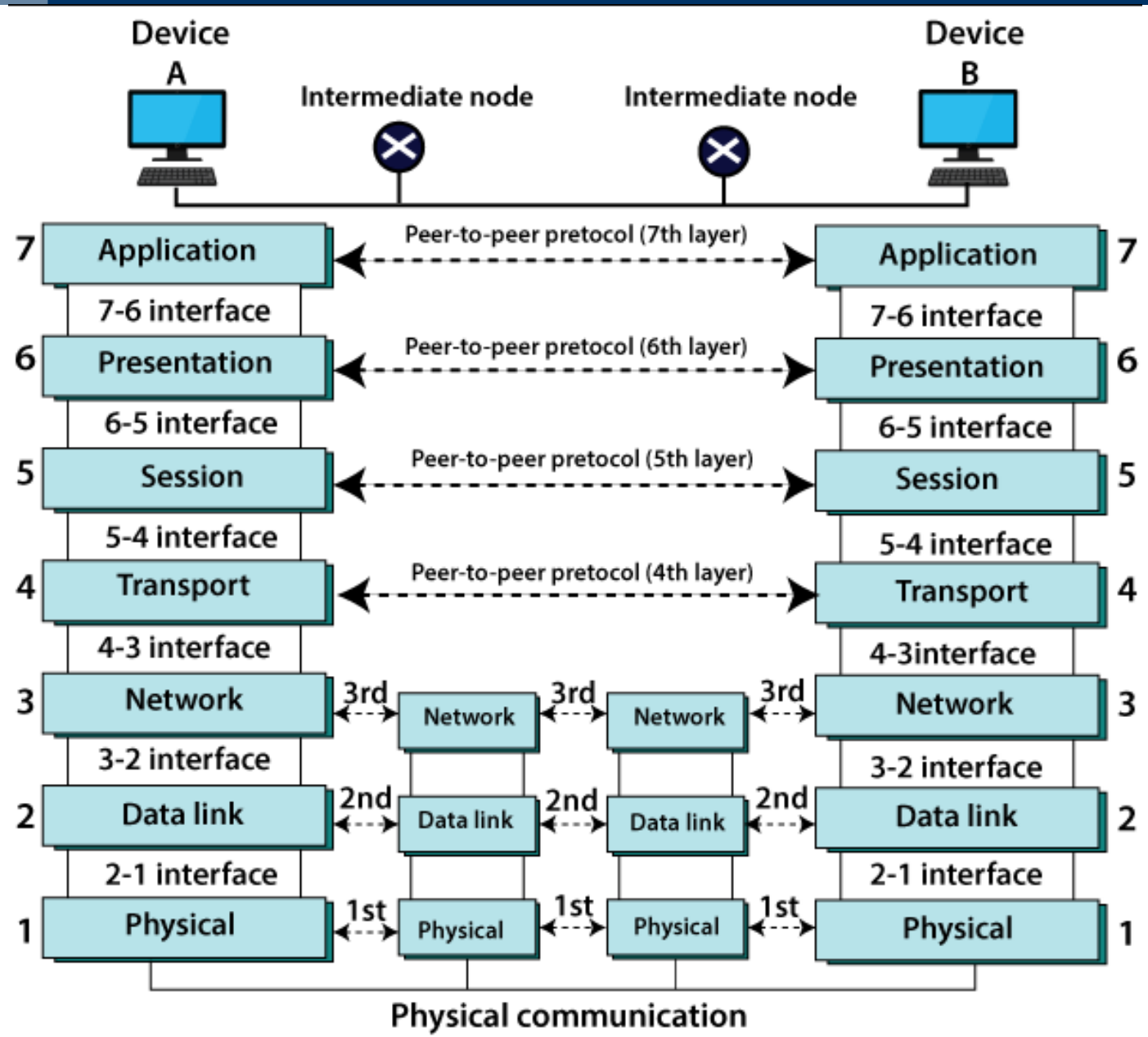
OSI Layer


Device
A
Intermediate node
Intermediate node
Device
B
7
Application
Peer-to-peer pretocol (7th layer)
Application
7
7-6 interface
7-6 interface
6
Presentation
Peer-to-peer pretocol (6th layer)
Presentation
6
6-5 interface
6-5 interface
5
Session
Peer-to-peer pretocol (5th layer)
Session
5

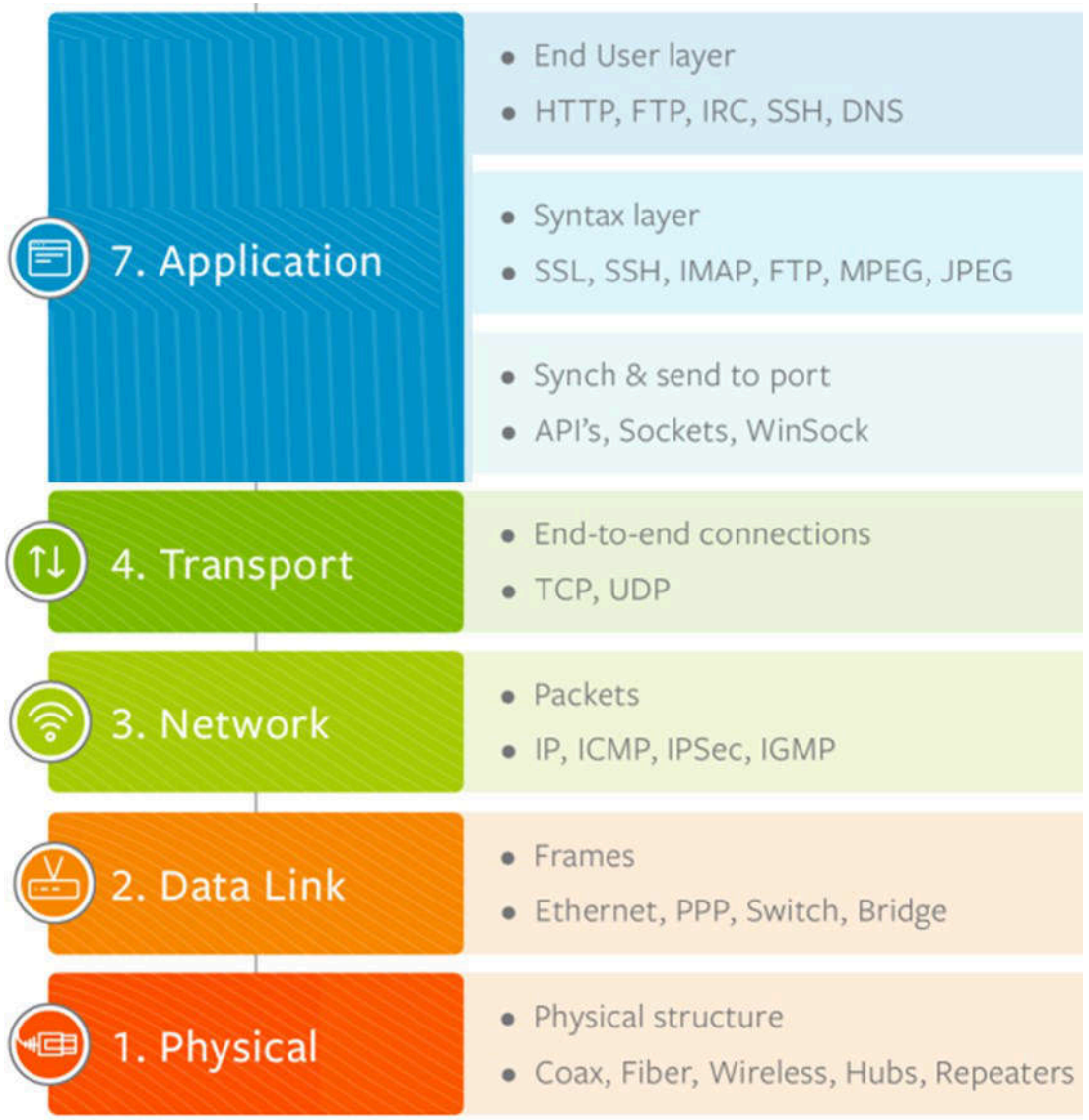
OSI Layer


Device
A
Intermediate node
Intermediate node
Device
B
7
Application
Peer-to-peer pretocol (7th layer)
Application
7
7-6 interface
7-6 interface
6
Presentation
Peer-to-peer pretocol (6th layer)
Presentation
6
6-5 interface
6-5 interface
5
Session
Peer-to-peer pretocol (5th layer)
Session
5
5-4 interface
5-4 interface
4
Transport
Peer-to-peer pretocol (4th layer)
Transport
4

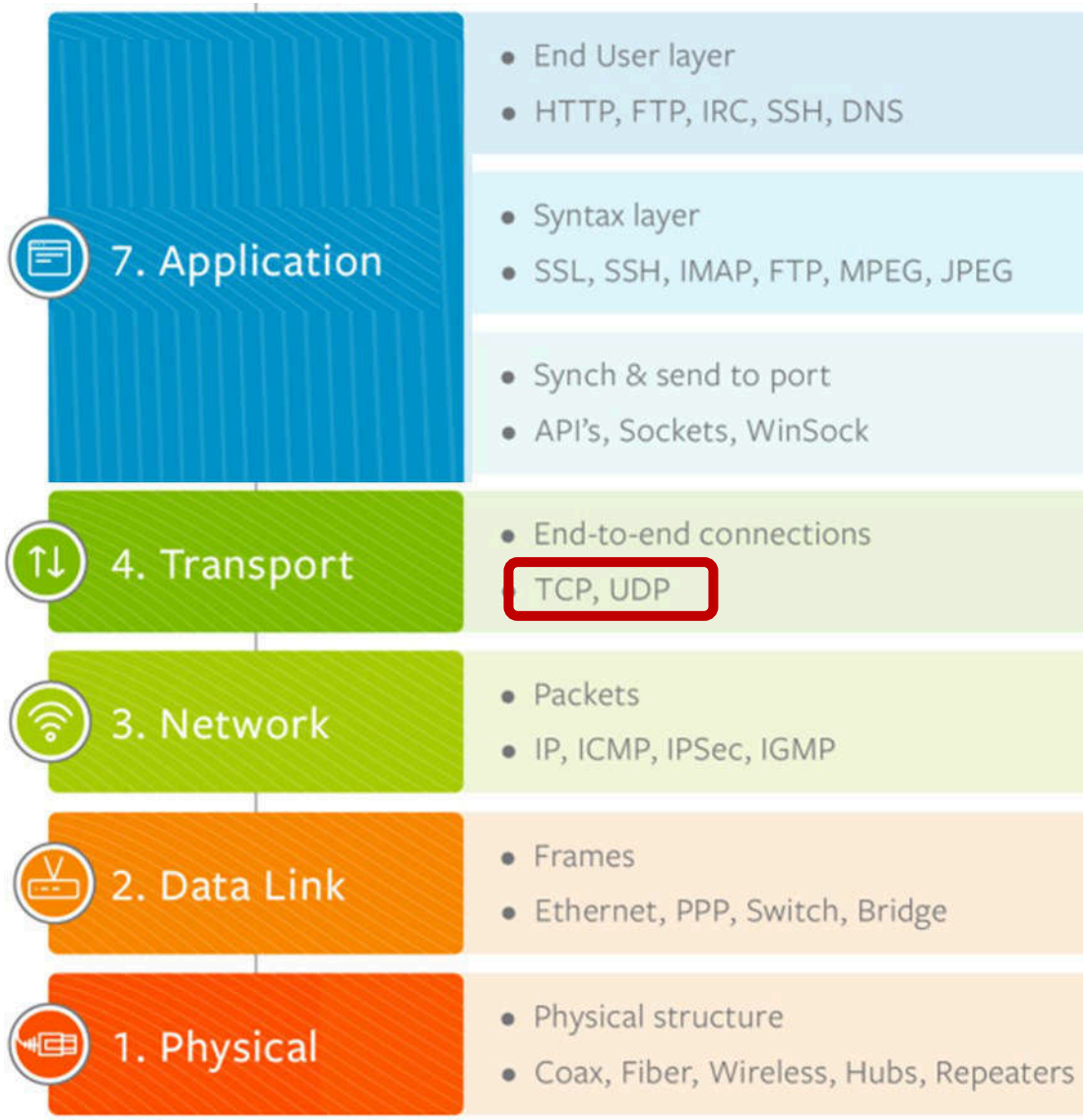
OSI Layer


Device A
Intermediate node
Intermediate node
Device B
7 Application
Peer-to-peer pretocol (7th layer)
Application 7
7-6 interface
6 Presentation
Peer-to-peer pretocol (6th layer)
Presentation 6
6-5 interface
5 Session
Peer-to-peer pretocol (5th layer)
Session 5
5-4 interface
4 Transport
Peer-to-peer pretocol (4th layer)
Transport 4
4-3 interface
4-3interface
3 Network
3rd
Network
3rd
Network
3rd
Network 3
3-2 interface
2 Data link
2nd
Data link
2nd
Data link
2nd
Data link 2
2-1 interface
1 Physical
1st
Physical
1st
Physical
1st
Physical 1
Physical communication

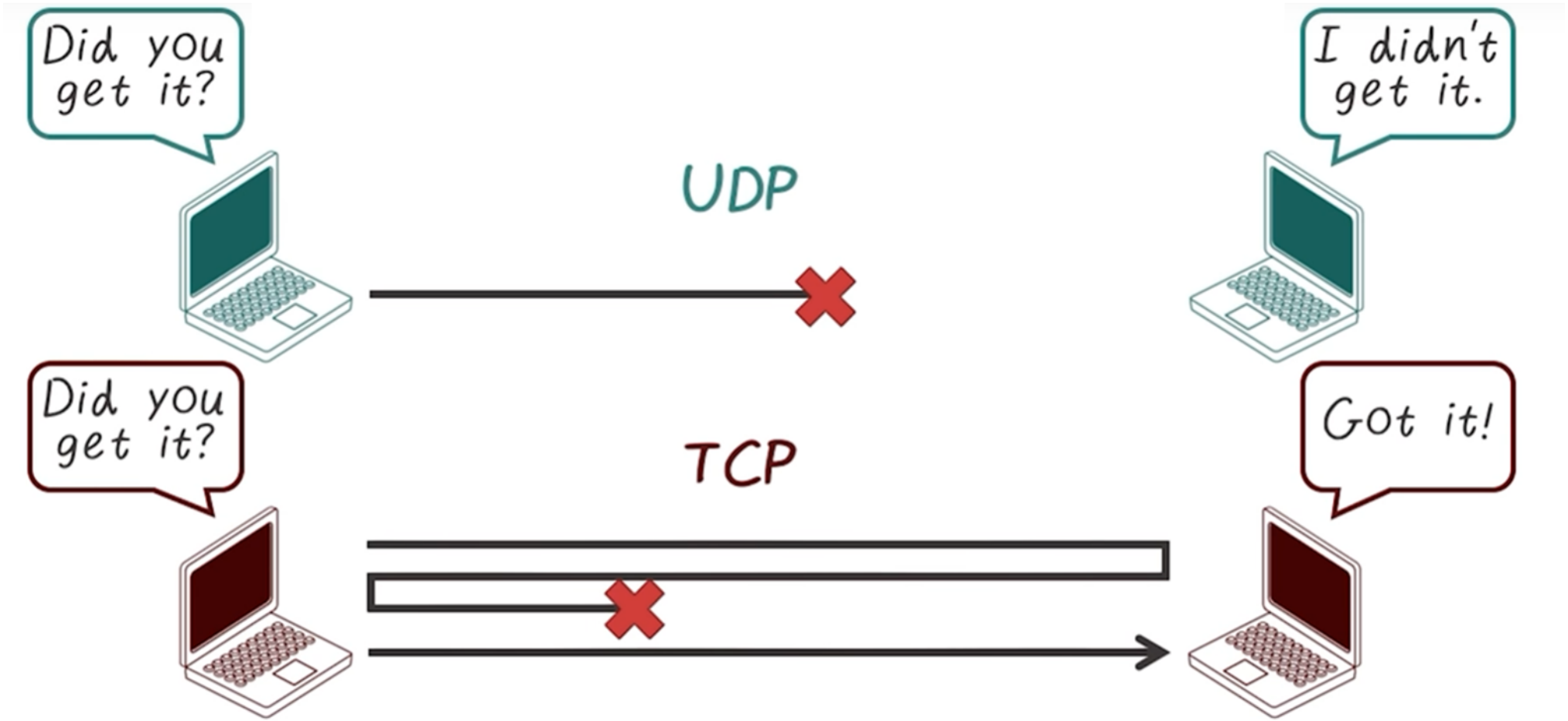
OSI Model vs TCP/IP model



OSI Model vs TCP/IP model



TCP vs UDP



Now comes **Security**

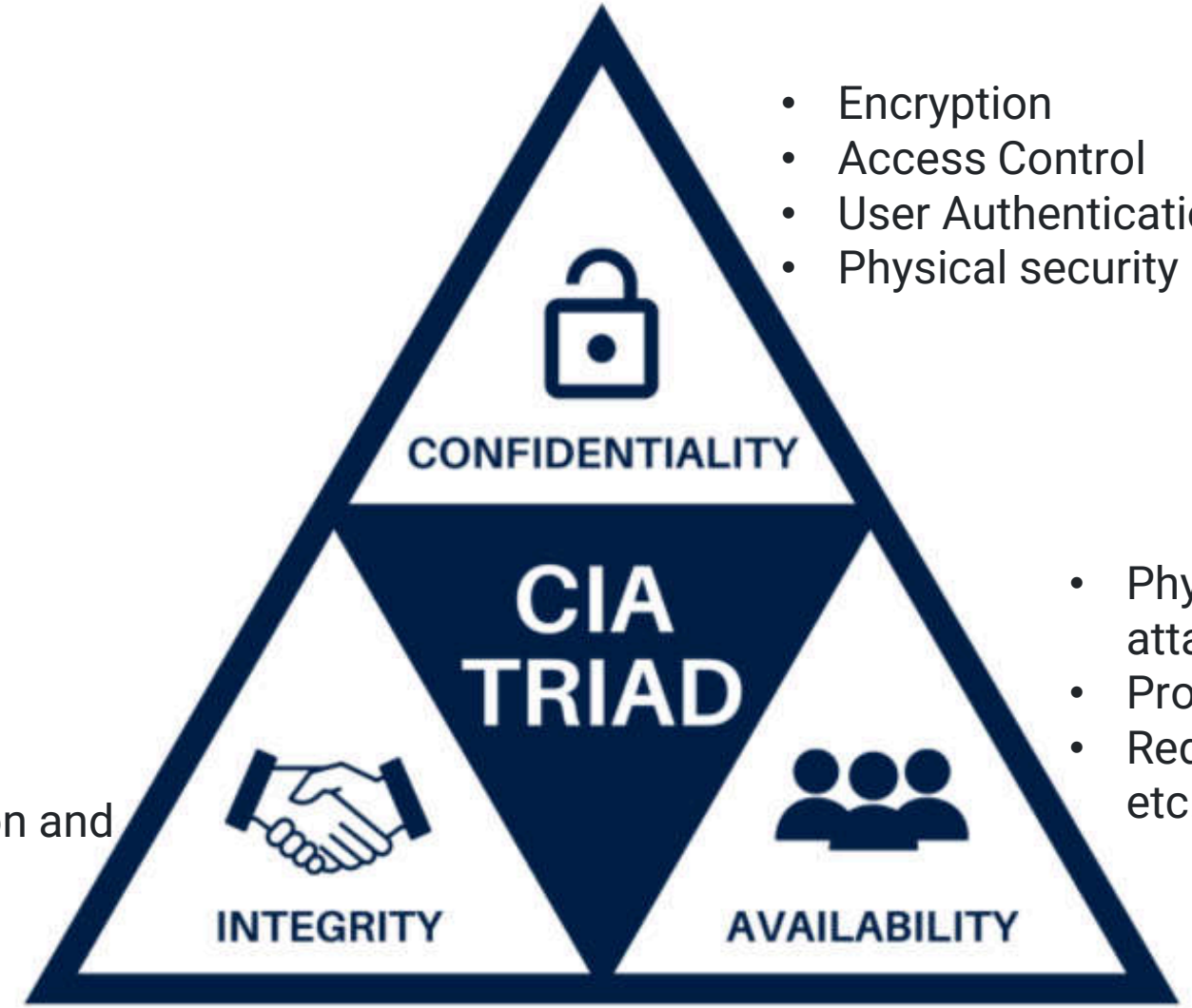
Defining Security

"Cybersecurity is the practice of **protecting systems, networks, and programs** from **digital attacks**. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal processes."

CISCO

Three Goals of Security

- Encryption
- Access Control
- User Authentication / identification
- Physical security

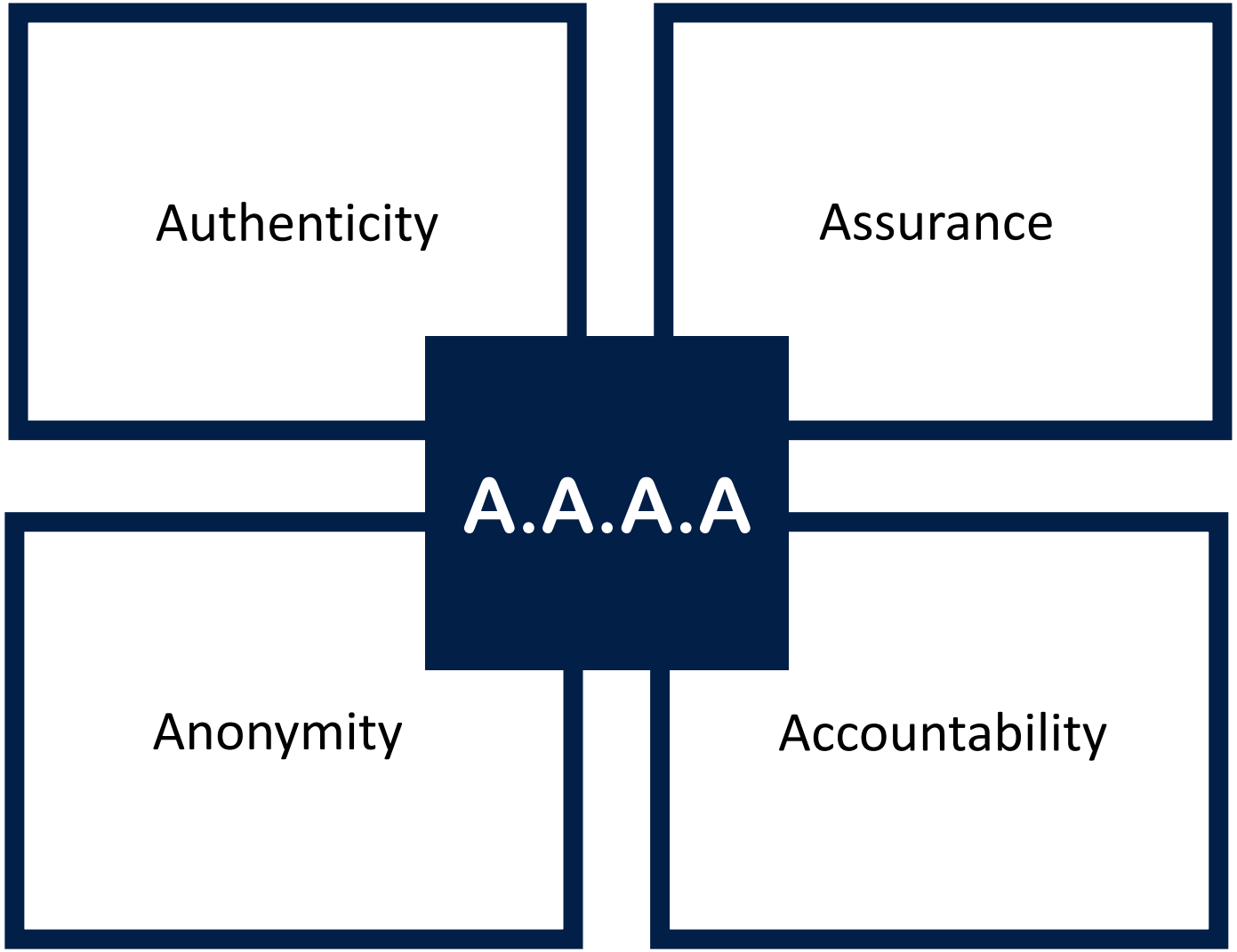


- Backups
- Checksums
- Error correcting codes
- Message authentication and digital signatures

- Physical protection from attacks and nature
- Protection from Cyber Attacks
- Redundancy of storage, servers, etc.

Other Security Concepts

A method for verifying that policies and permissions are genuine



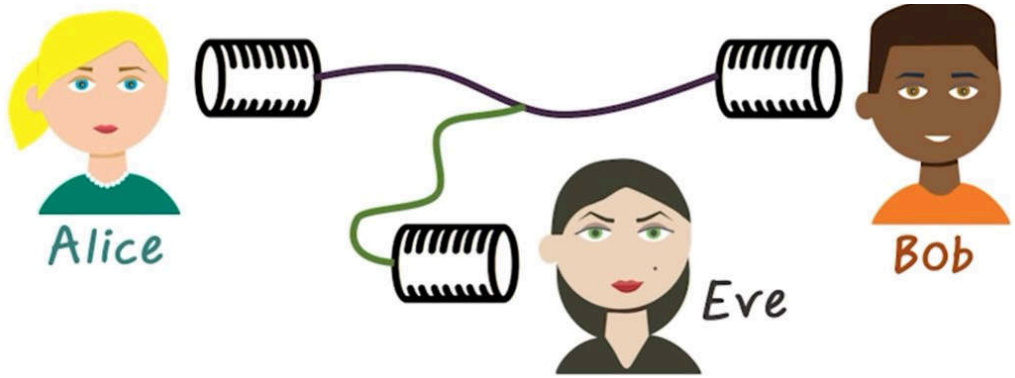
Guarantee that the system provides the properties it has been trusted to provide

Certain records or actions cannot be attributed to a particular individual.

Actions of an entity are traceable

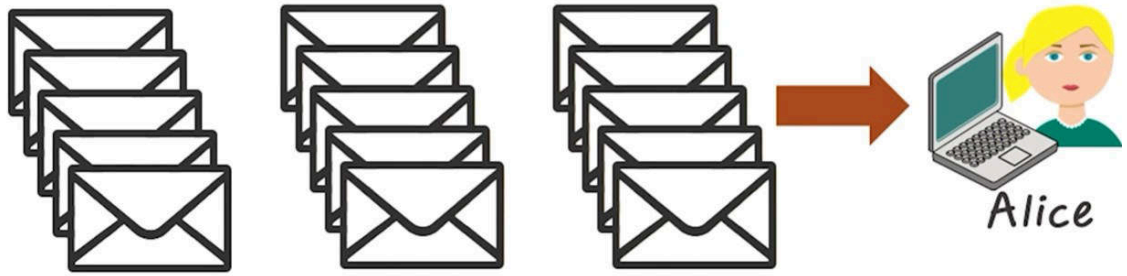
Threats and Attacks

Eavesdropping



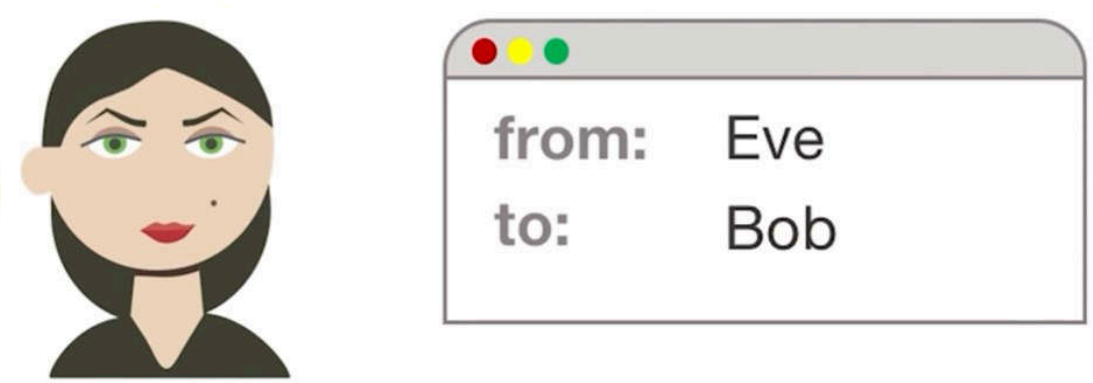
Alteration

Denial of Service



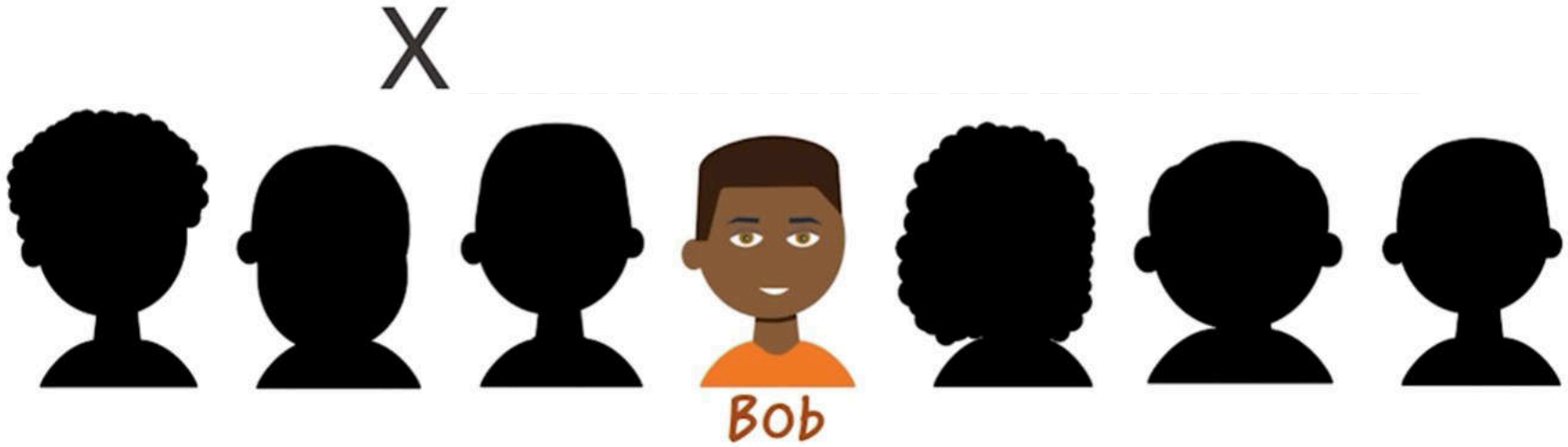
Threats and Attacks

Masquerading

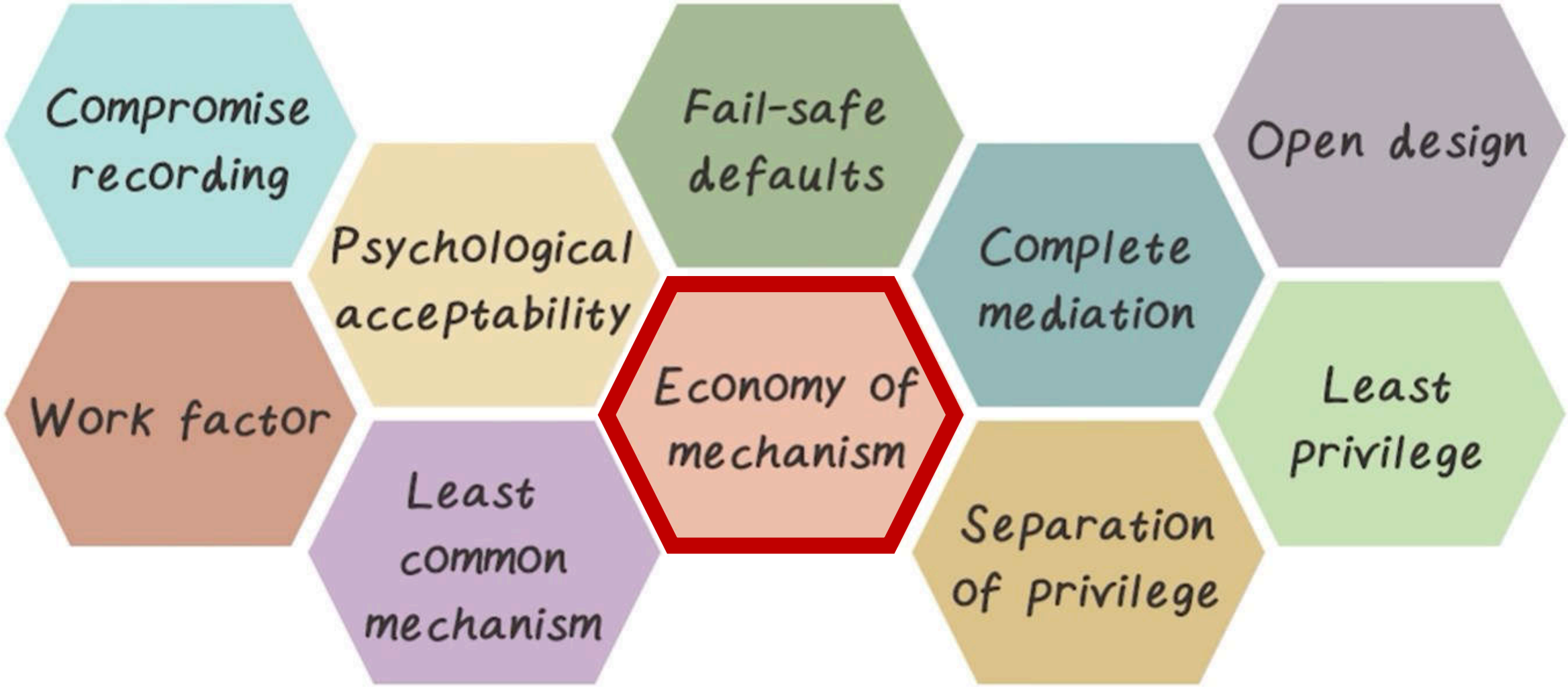


Repudiation

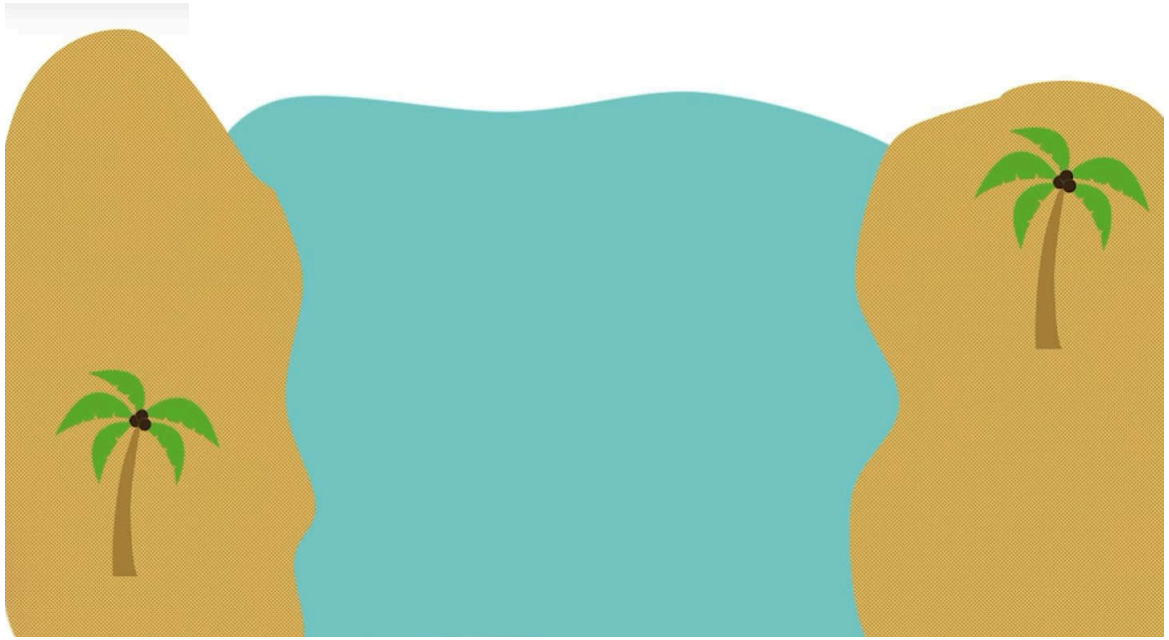
Correlation and Traceback

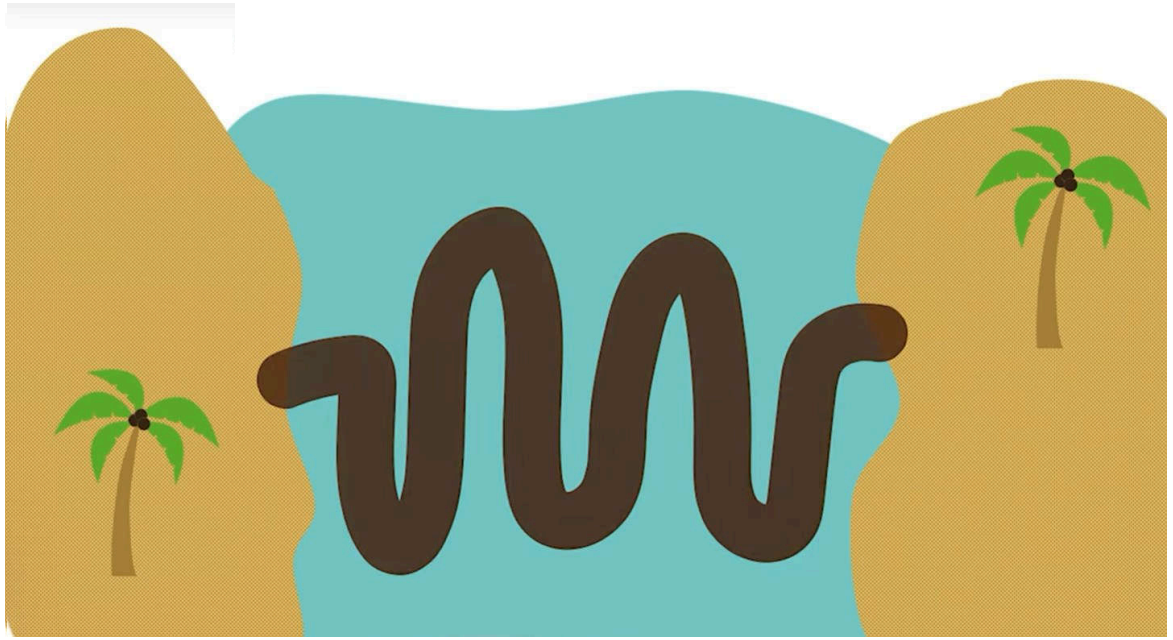


Ten Principals of Security

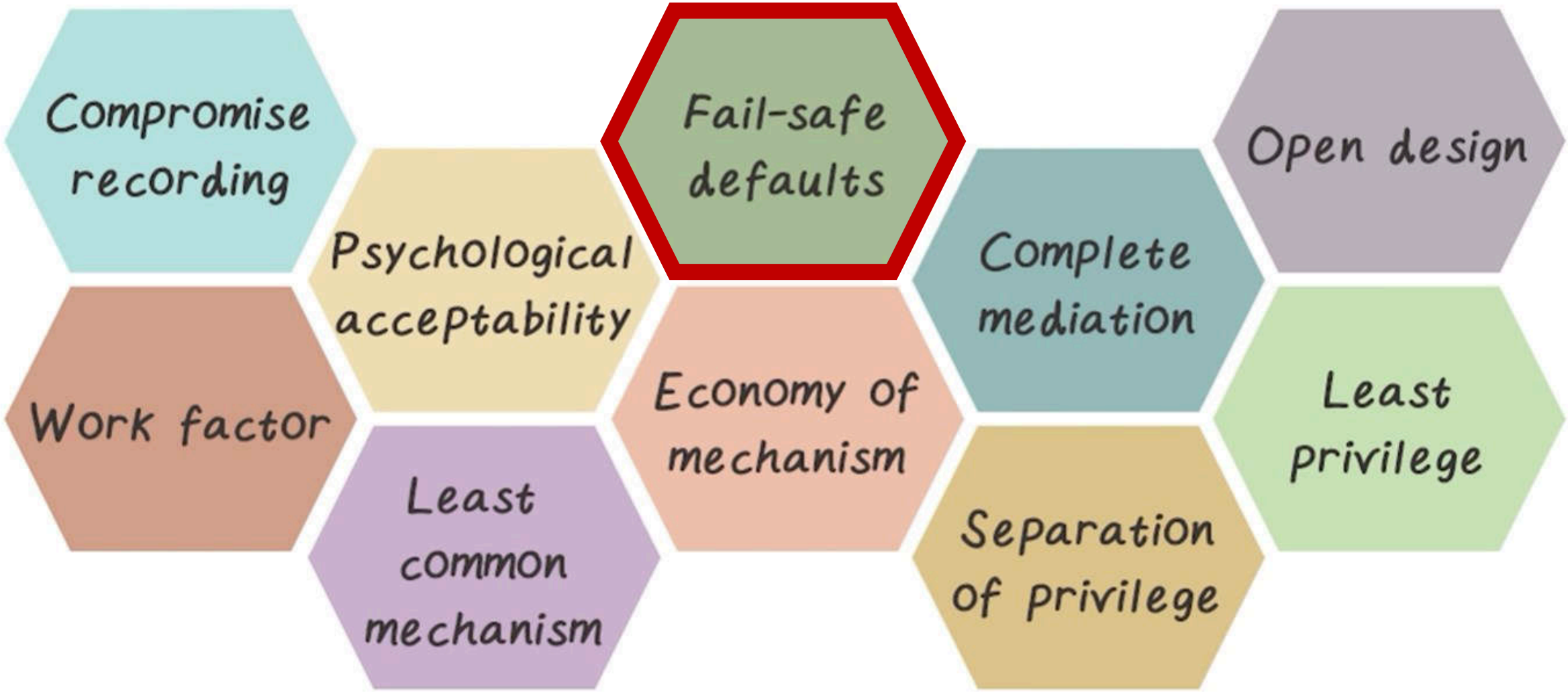


Ten Principals of Security

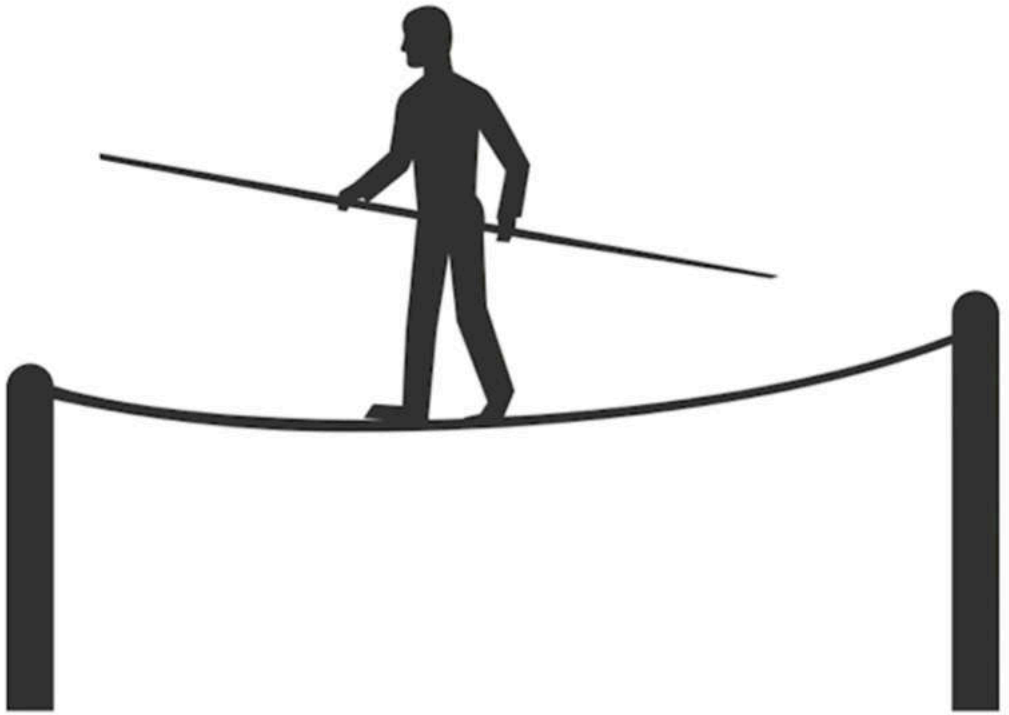




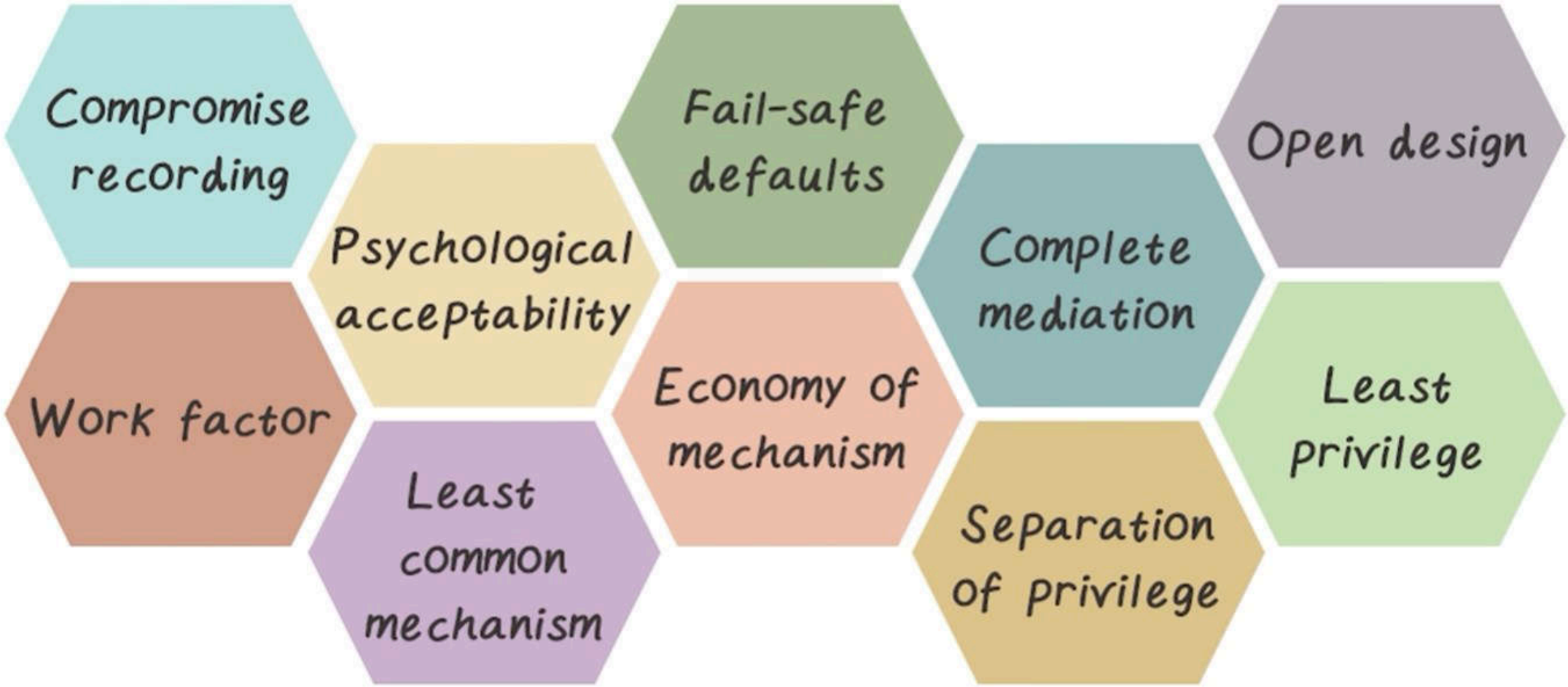
Ten Principals of Security



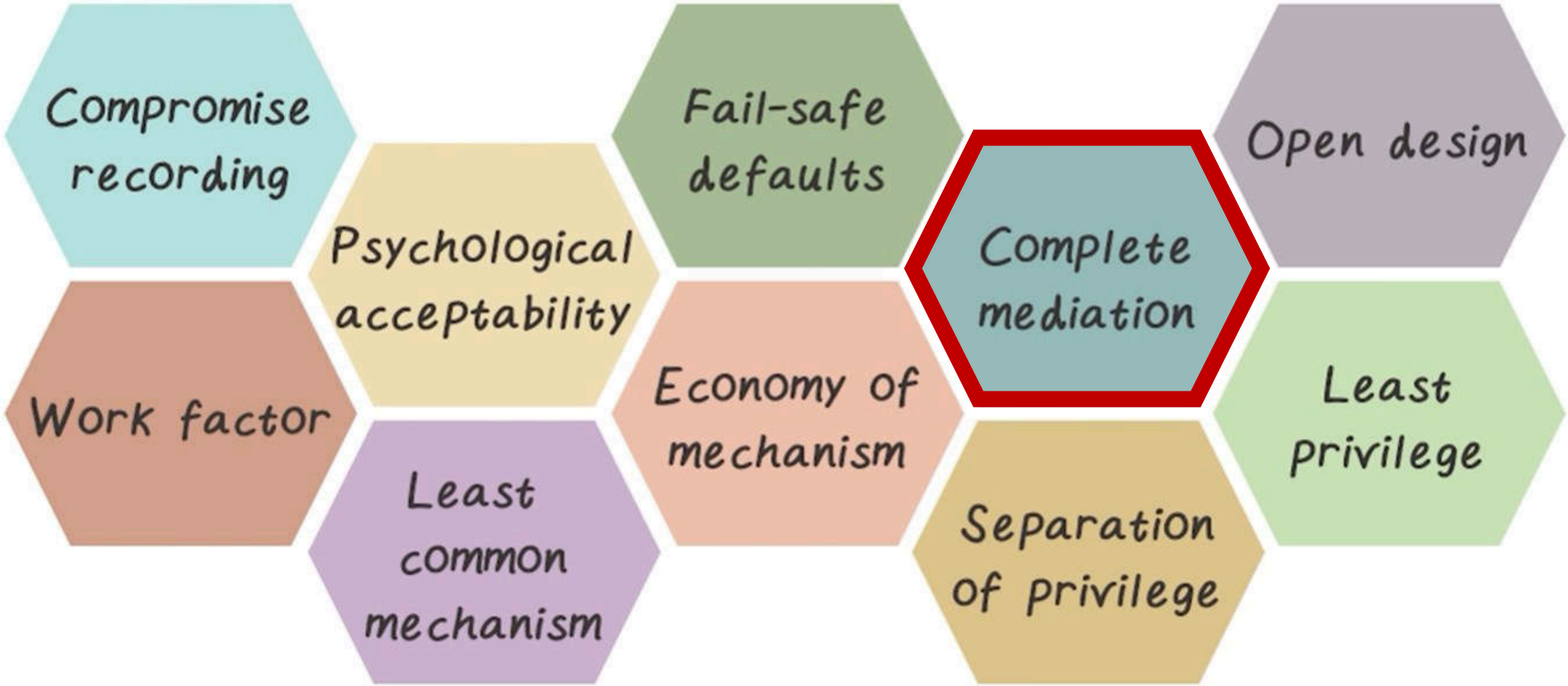
Ten Principals of Security



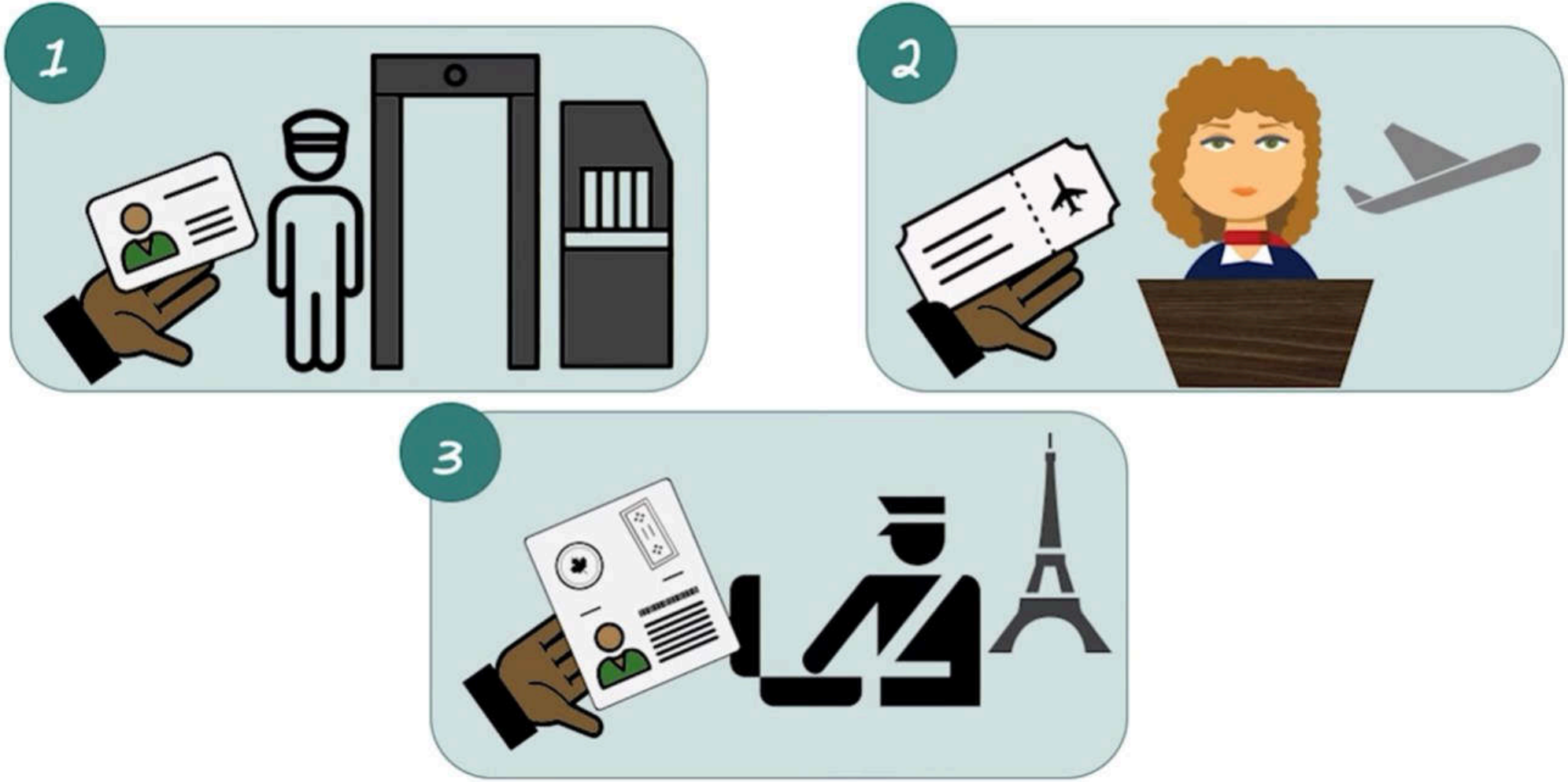
Ten Principals of Security



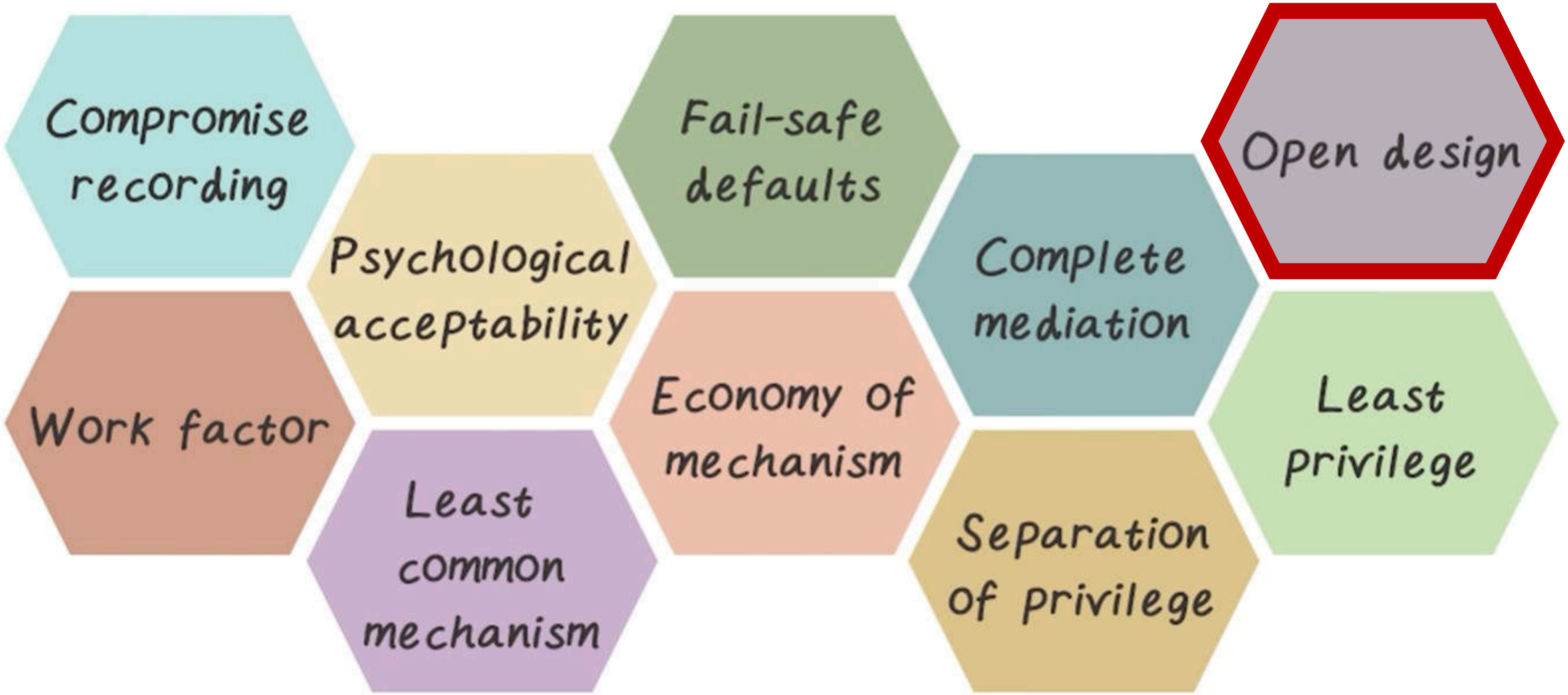
Ten Principals of Security



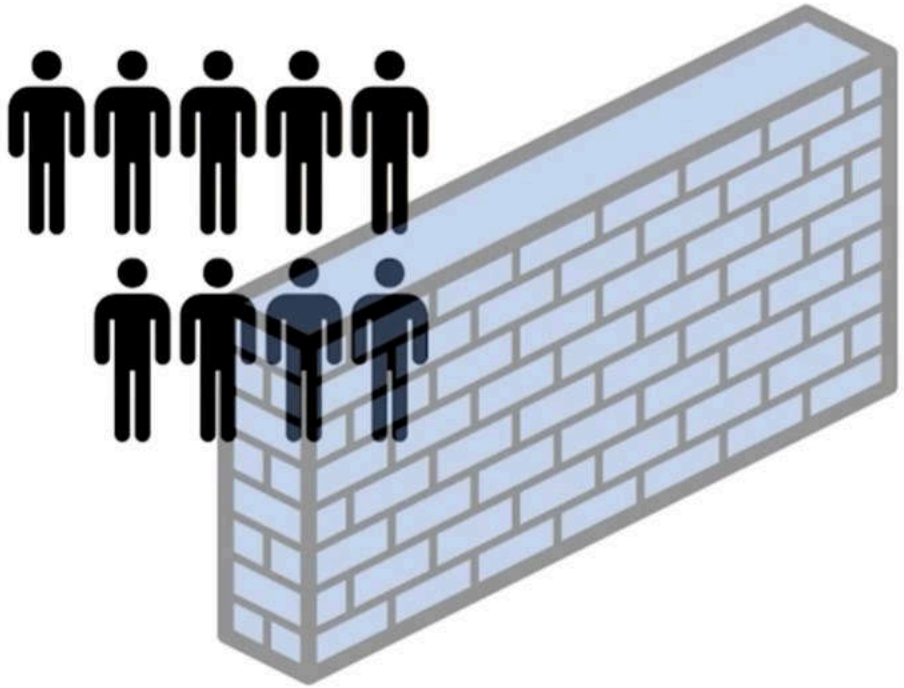
Ten Principals of Security

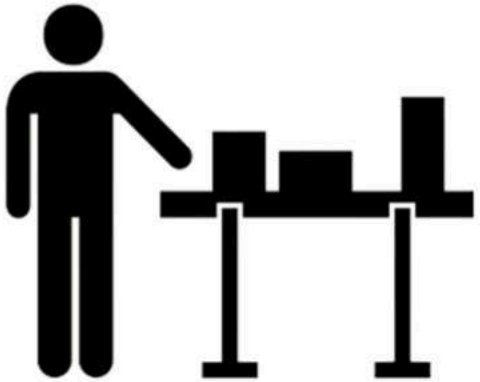


Ten Principals of Security

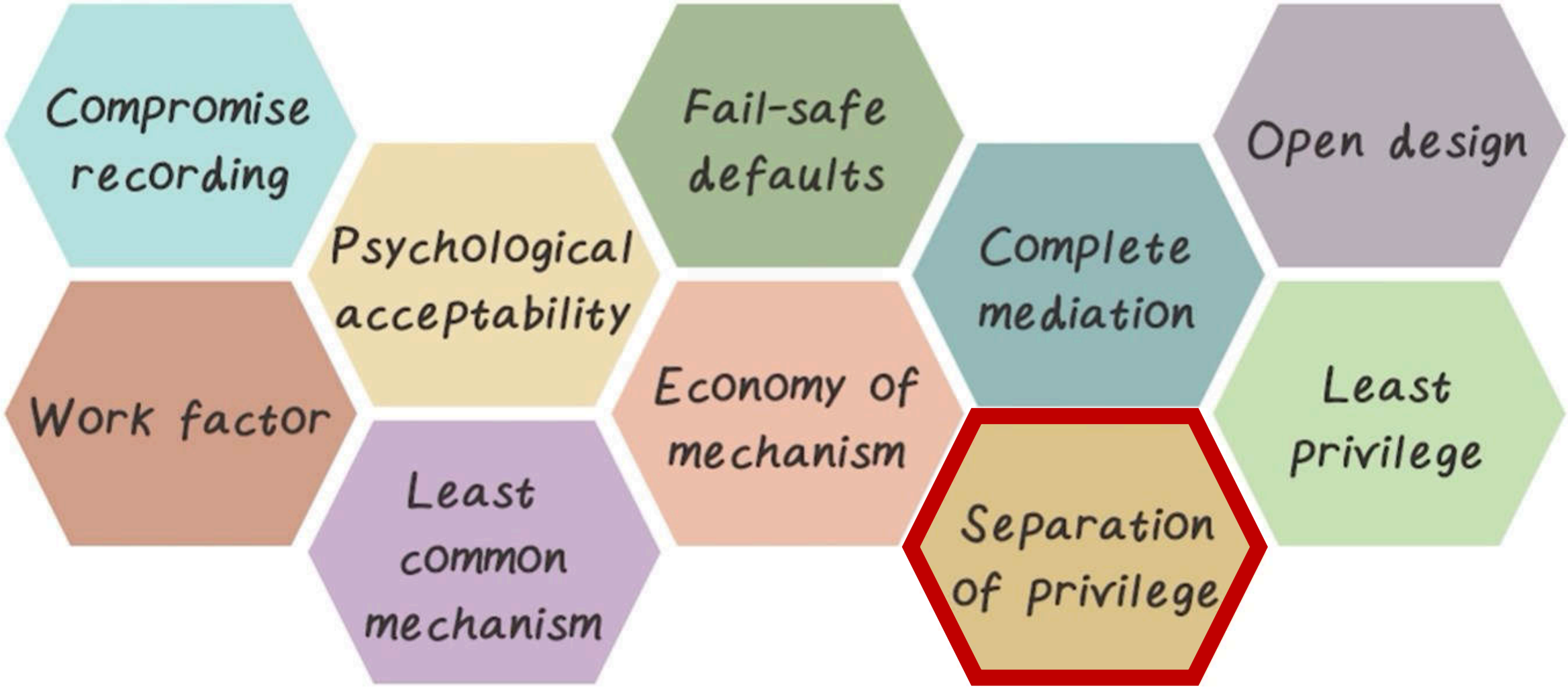


Ten Principals of Security

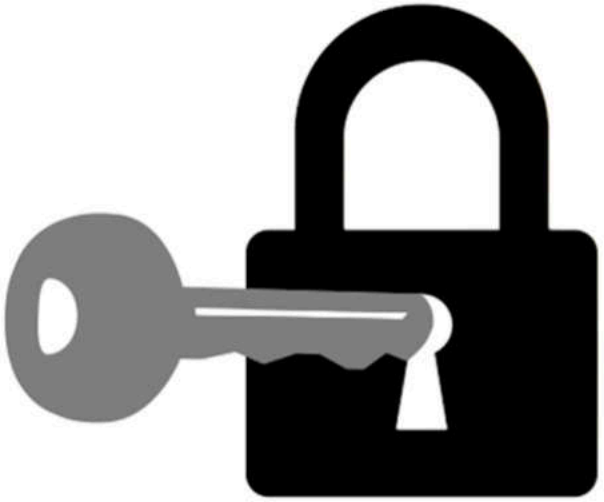




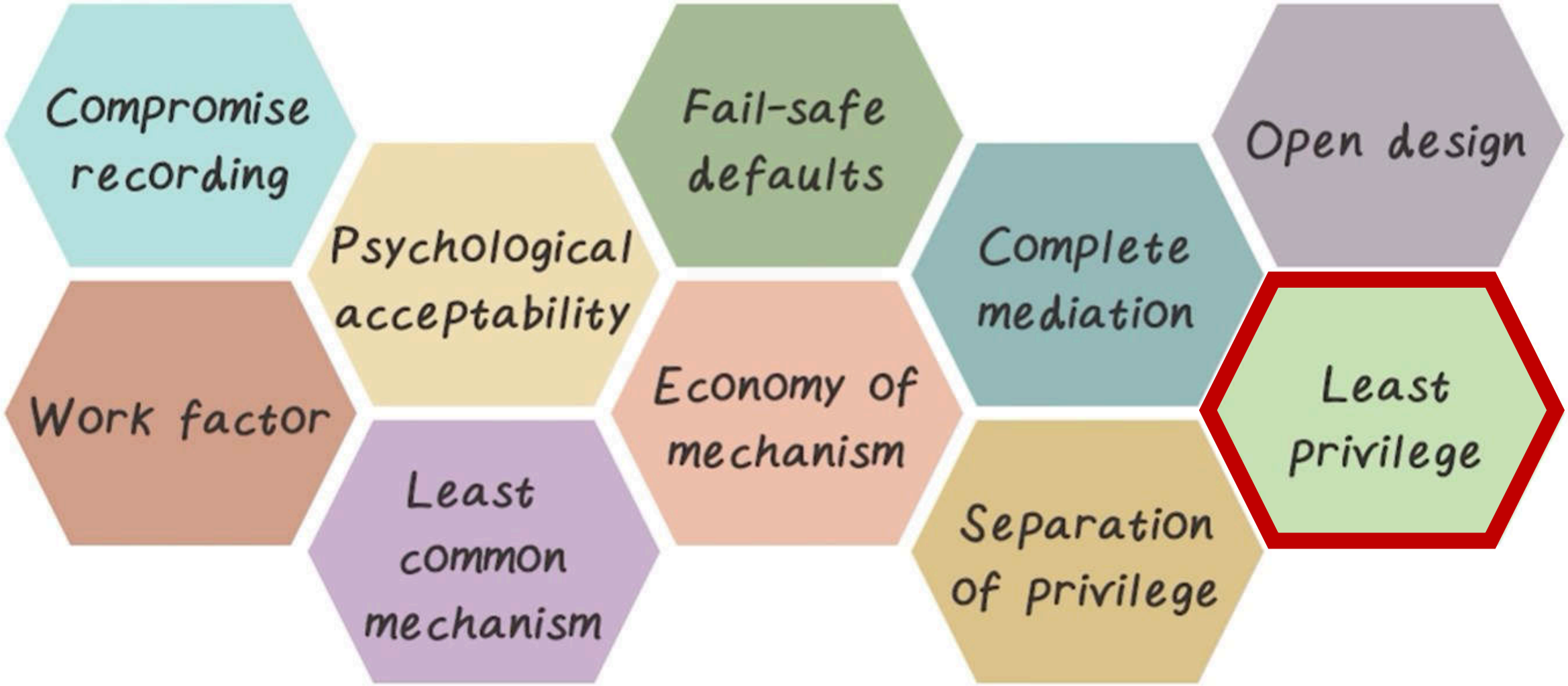
Ten Principals of Security



Ten Principals of Security

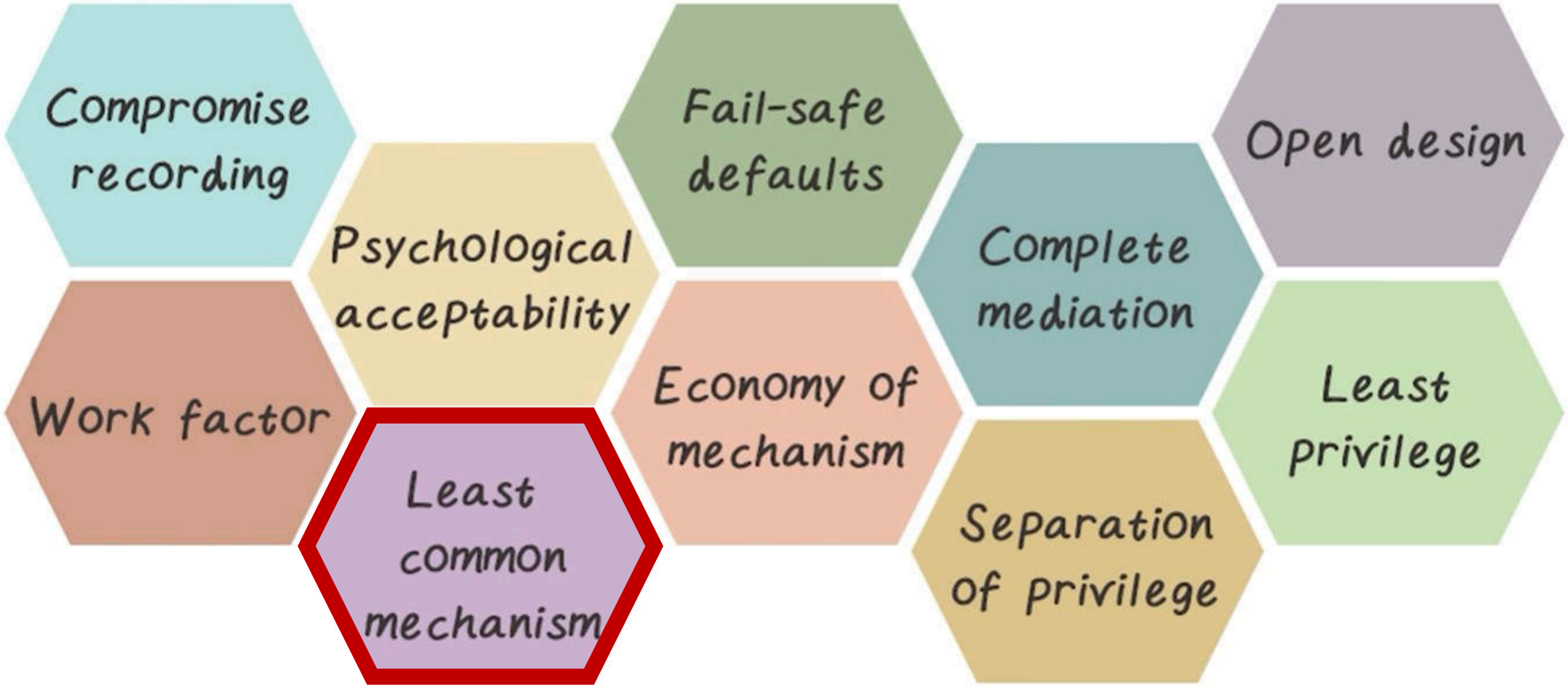


Ten Principals of Security

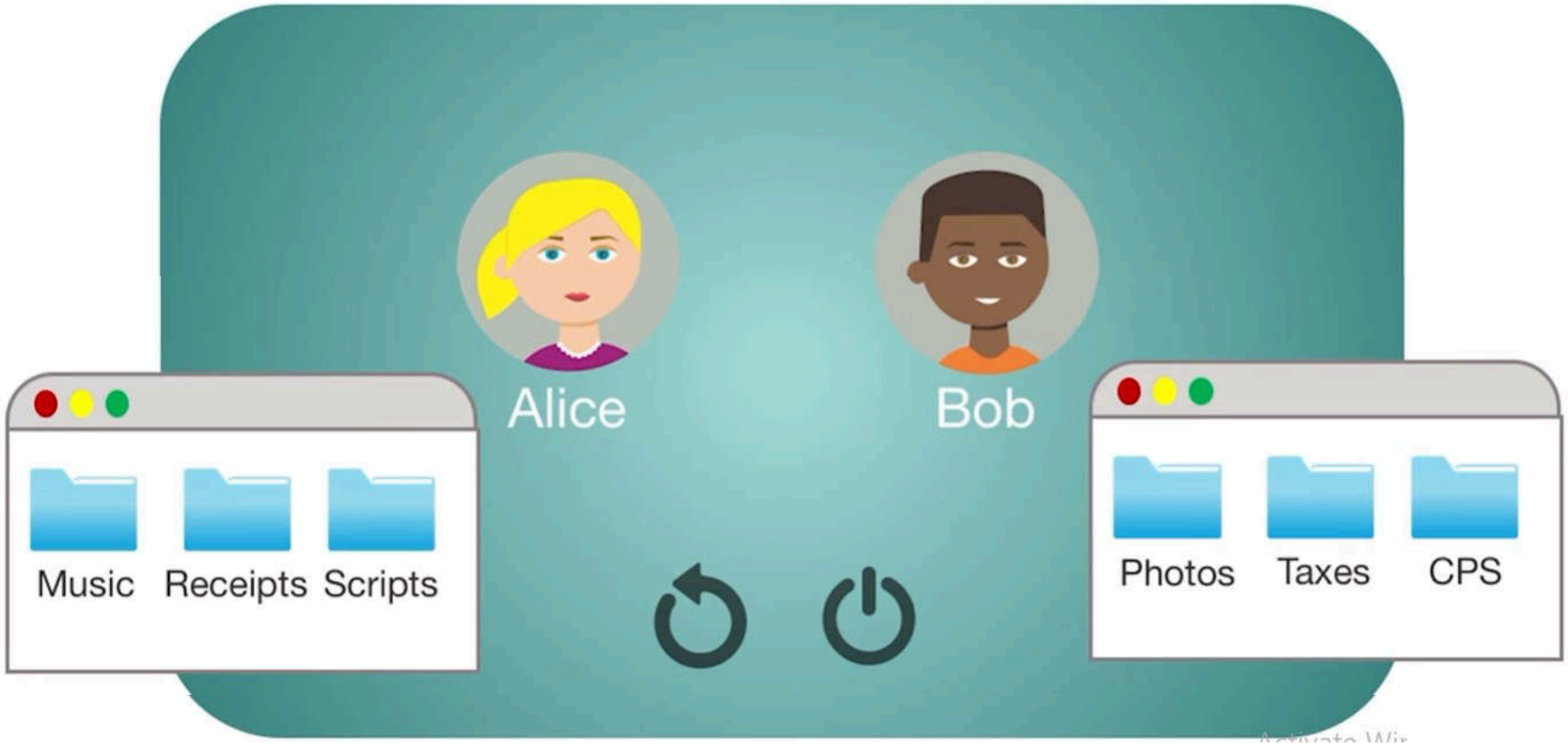


Ten Principals of Security

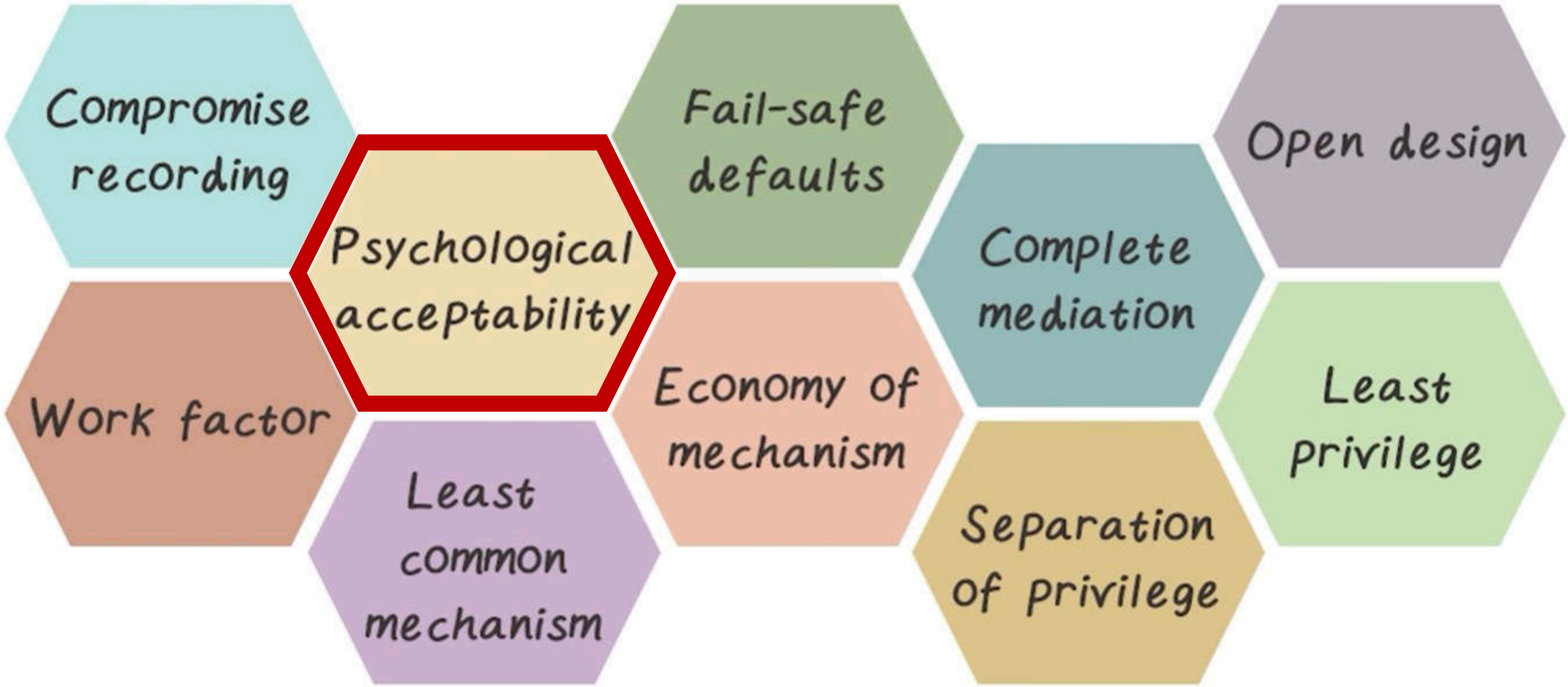
Ten Principals of Security



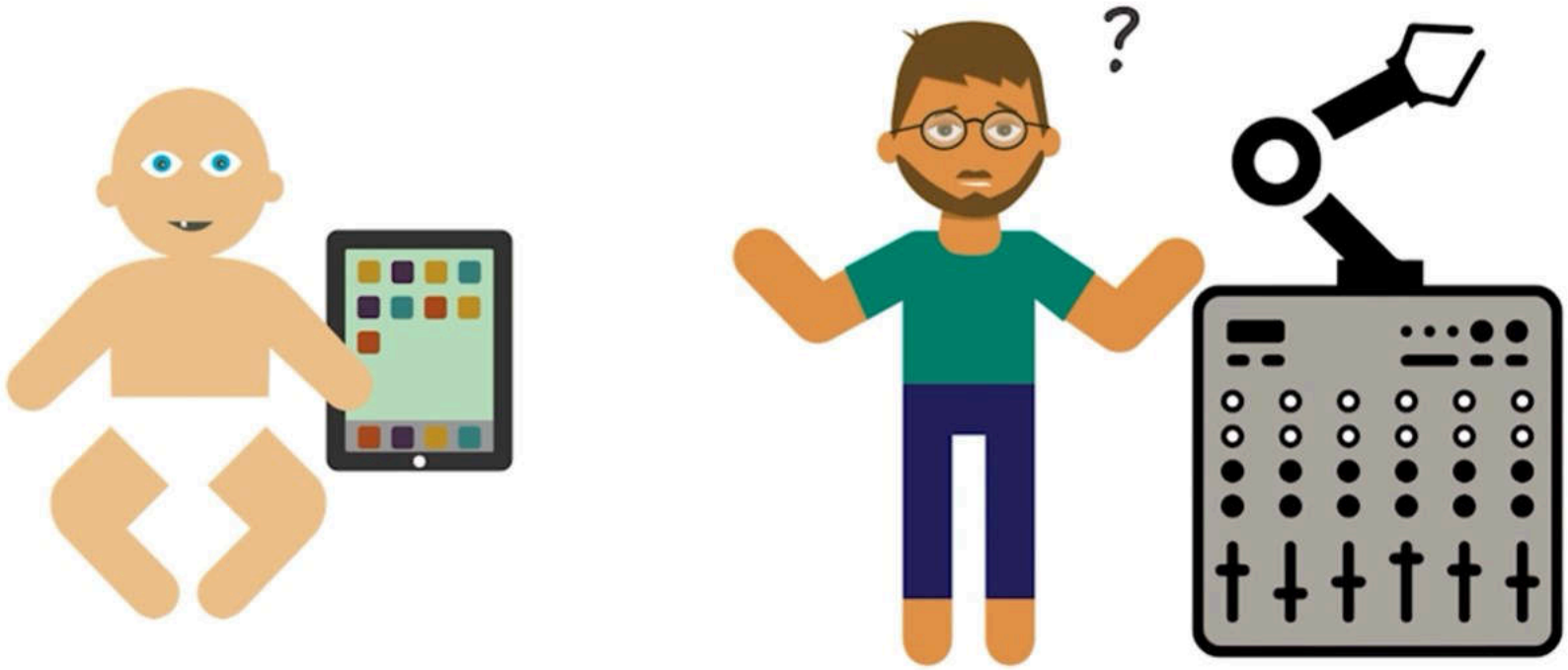
Ten Principals of Security



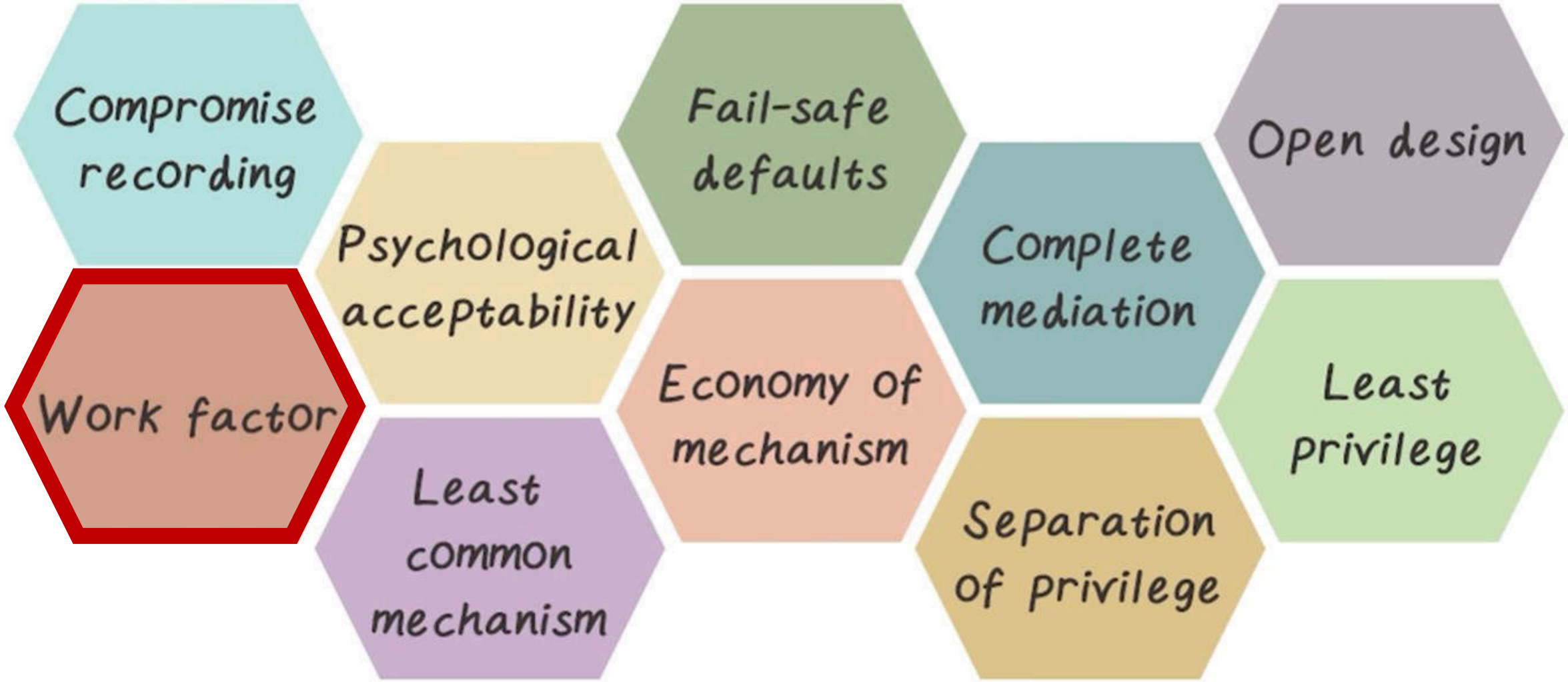
Ten Principals of Security



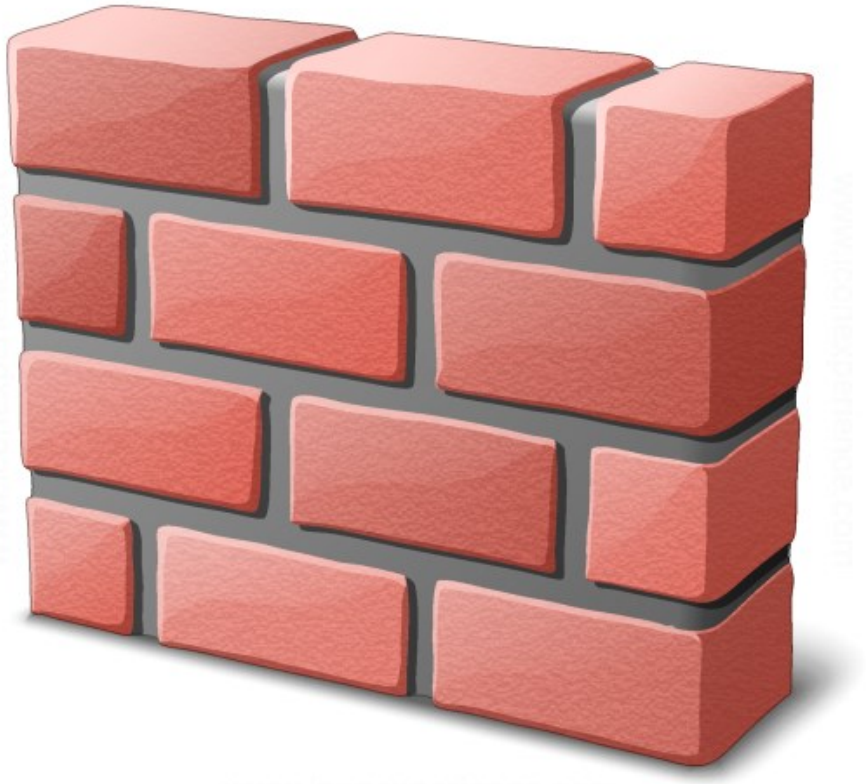
Ten Principals of Security



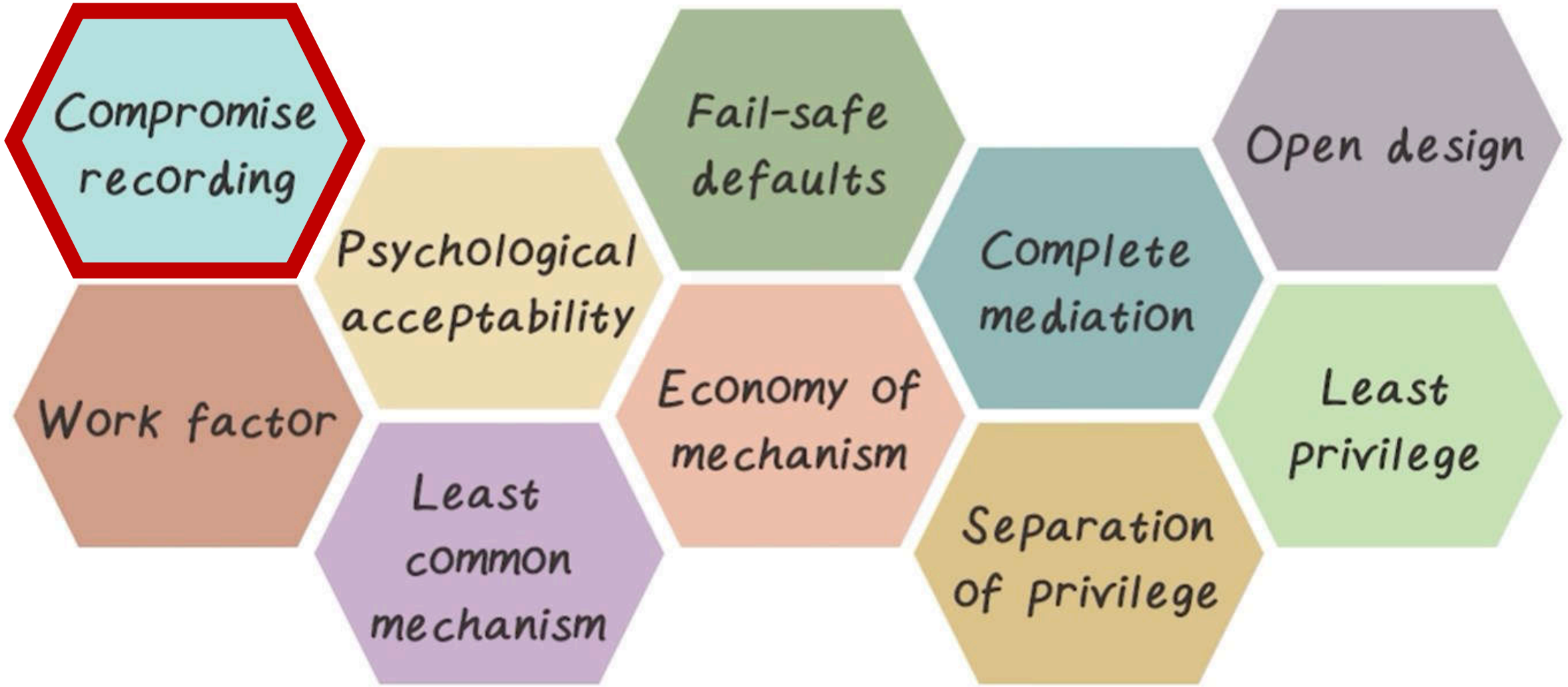
Ten Principals of Security



Ten Principals of Security



Ten Principals of Security



Ten Principals of Security

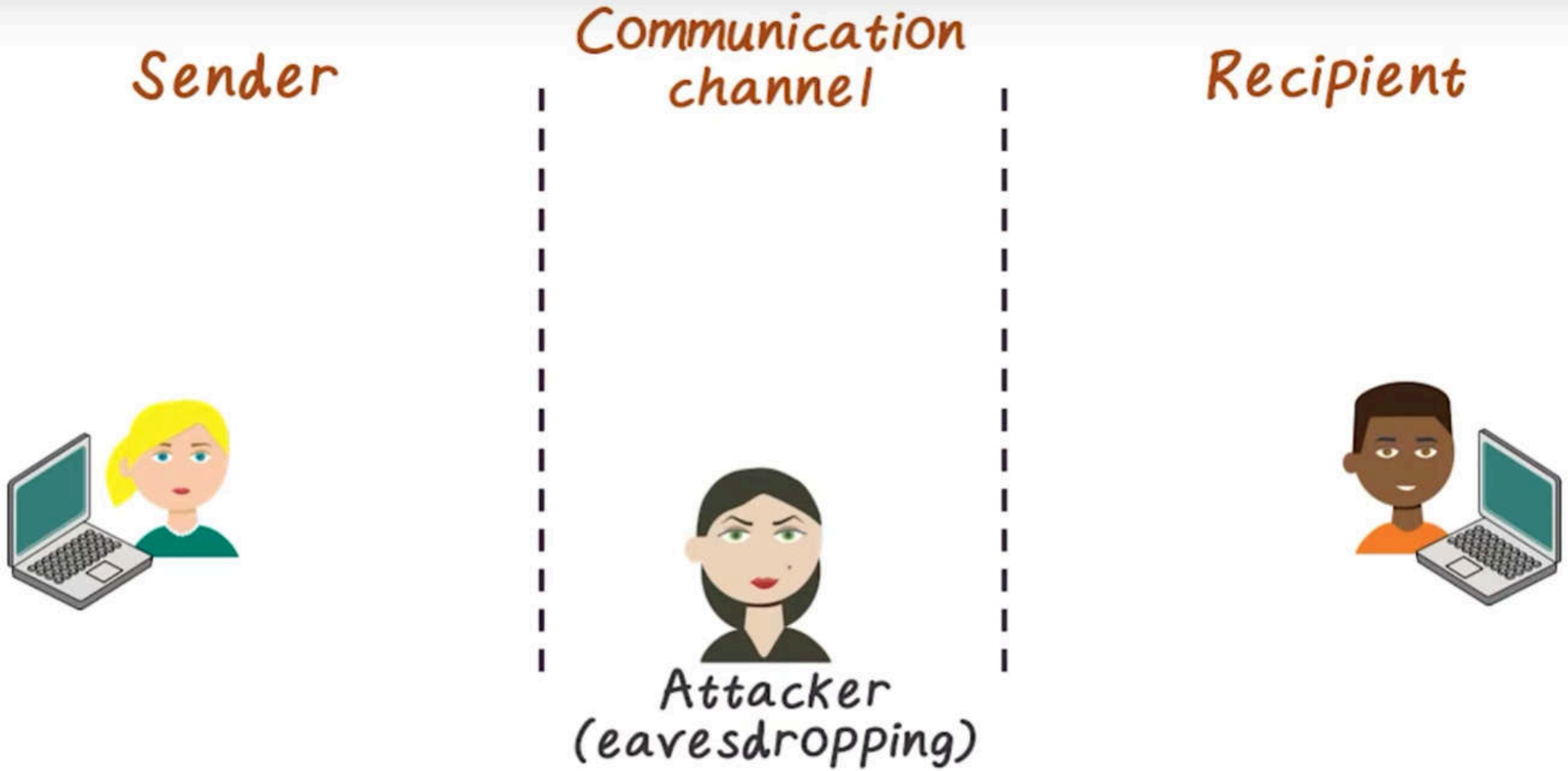
Cryptographic Concepts

Sender

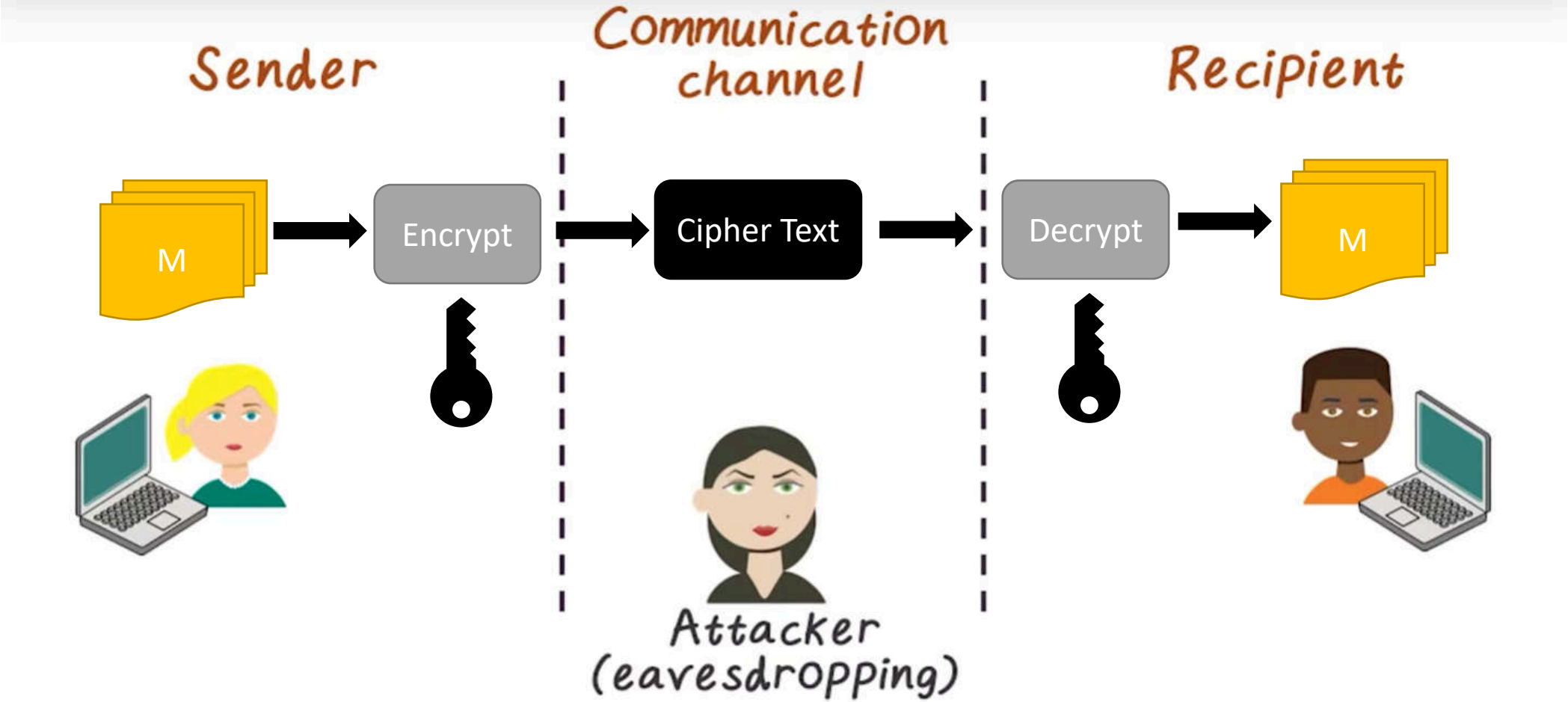
Communication channel

Recipient

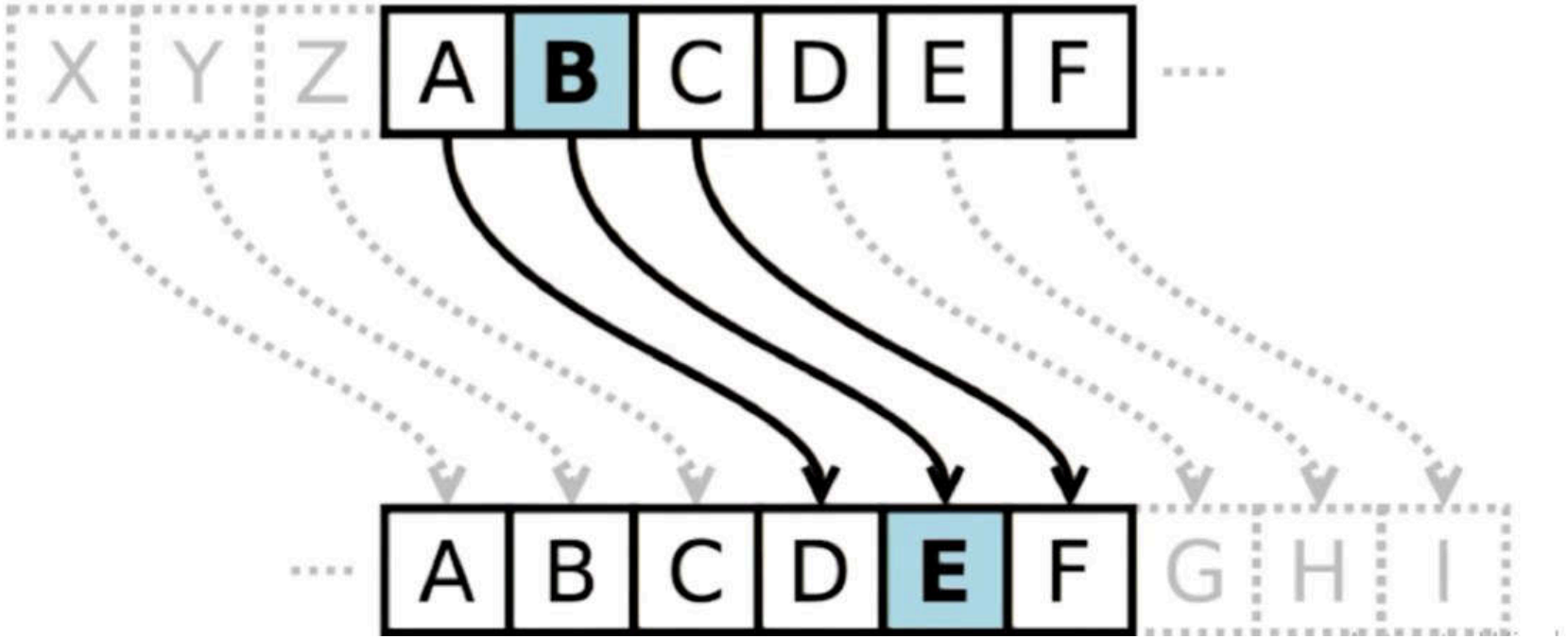
Cryptographic Concepts



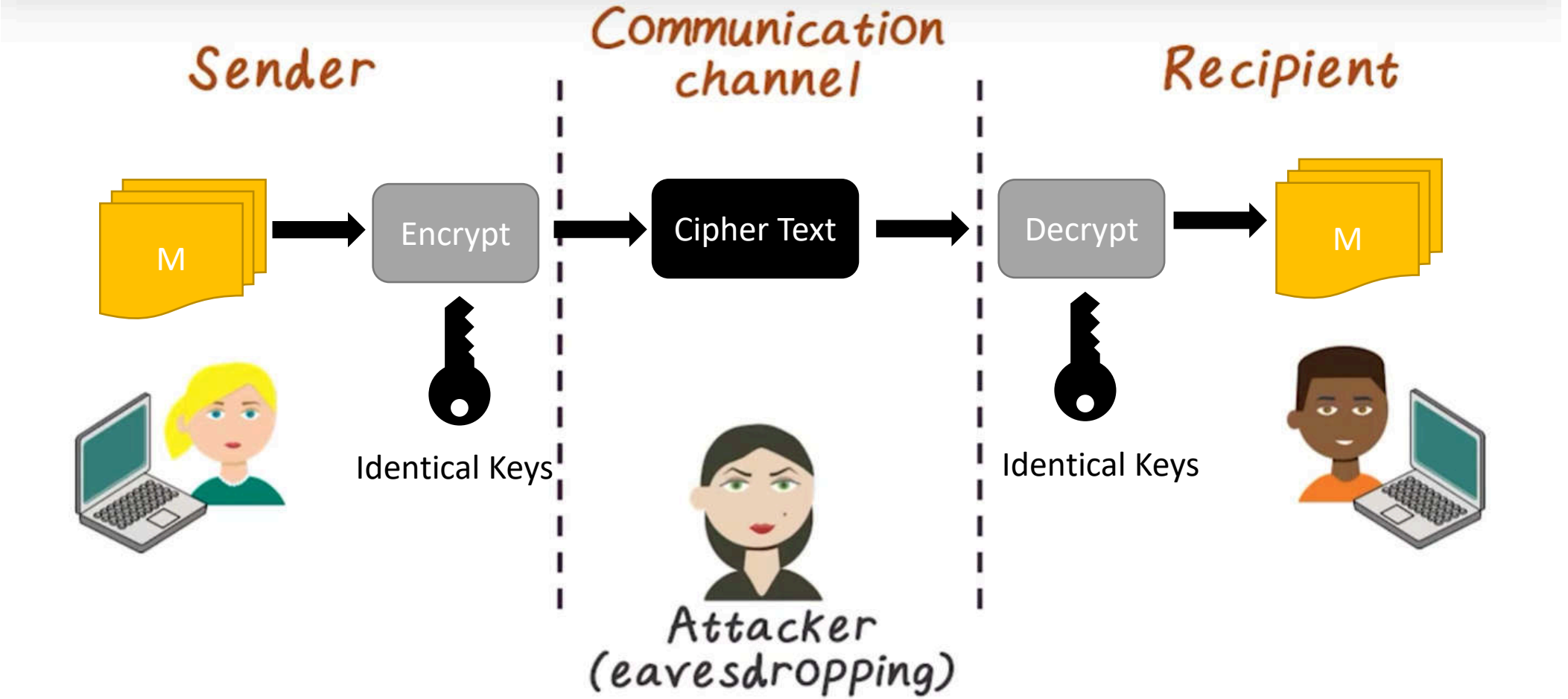
Cryptographic Concepts



Ceaser Cypher

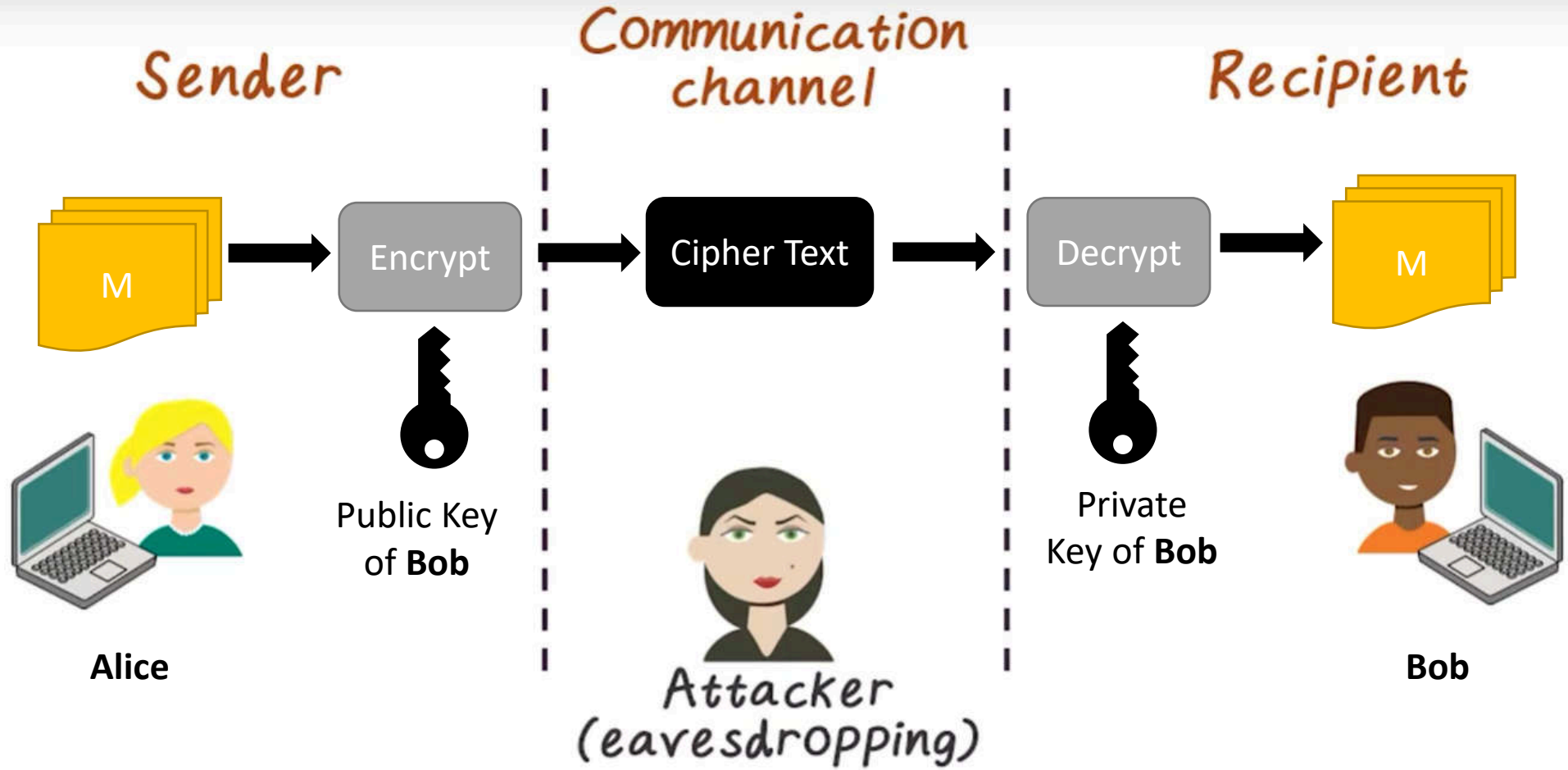


Symmetric Cryptosystem



Symmetric Cryptosystem

Asymmetric Cryptosystem (Public Key Cryptosystem)



Thanks a lot

If you are taking a Nap, **wake up**.....Lecture Over