UNIVERSITÉ Concordia UNIVERSITY

Supply Chain Security in IoT

Under the Supervision of Prof. Suryadipta Majumdar

Bharathwaj S (40267496) || **Chris V** (40232485) || **Harleen K** (40232489) || **Moazam A** (40298779) **||** **Mohik J** (40224737) || **Mukul P** (40257131) || **Nusrat Jahan Kashfia** (40260286) || **Sabrina S** (40266939) || **Chakradhar Reddy** (40207537)

Stage I: Survey

A Survey on Supply Chain Security

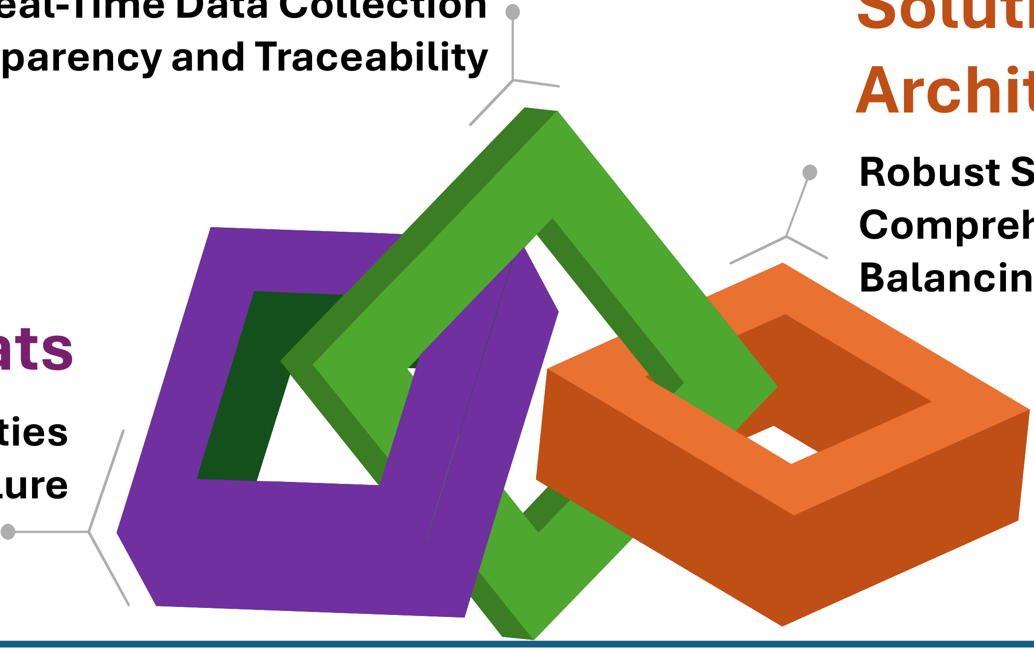
Hassija, Vikas & Chamola, Vinay & Gupta, Vatsal & Jain, Sarthak & Guizani, Nadra. (2020)

Application Areas

Supply chain digitalization
Real-Time Data Collection
Enhanced Transparency and Traceability

Solution Architectures

Robust Security Measures
Comprehensive Security Strategies
Balancing Benefits and Risks



Security Threats

Security Vulnerabilities
Single Points of Failure

Hassija, Vikas & Chamola, Vinay & Gupta, Vatsal & Jain, Sarthak & Guizani, Nadra. (2020). A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures. IEEE Internet of Things Journal. PP. 10.1109/JIOT.2020.3025775.

ReSC-2

An RFID-enabled system specifically designed for securing IoT devices in a supply chain, ensuring that they are not tampered with, counterfeited, or mishandled as they move from manufacturer to end-user.

How Does It Work?

Binding Tags with Control Chips

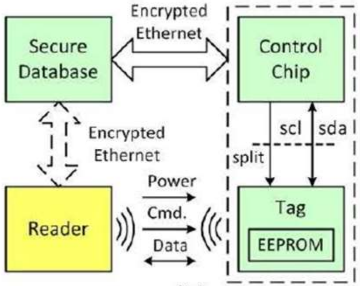
Mutual Authentication

Tag Traceability

The RFID tag contains a unique identity (tag ID), which is paired with the control chip's identity (CC ID). This pairing is stored in a centralized database, ensuring that the tag and chip remain linked throughout the device's lifecycle.

Only authorized RFID readers can interact with the tags. Each reader generates a signature based on its private key and the tag's identity, which is then validated by the centralized database.

Each reader's signature includes a timestamp and an index indicating its position in the supply chain. This information is encrypted and stored in the tag's memory.



Hardware Architecture

Security Evaluation

Cloning Attacks: ReSC-2 binds each tag to a unique control chip identity, making it impossible to create a valid clone without the corresponding chip.

Eavesdropping: AES encryption ensures that even if the communication is intercepted, the data cannot be understood or used by attackers.

Man-in-the-Middle Attacks: ReSC-2 mitigates this by using session keys and random numbers for each communication session, ensuring that altered communications are detected and rejected.

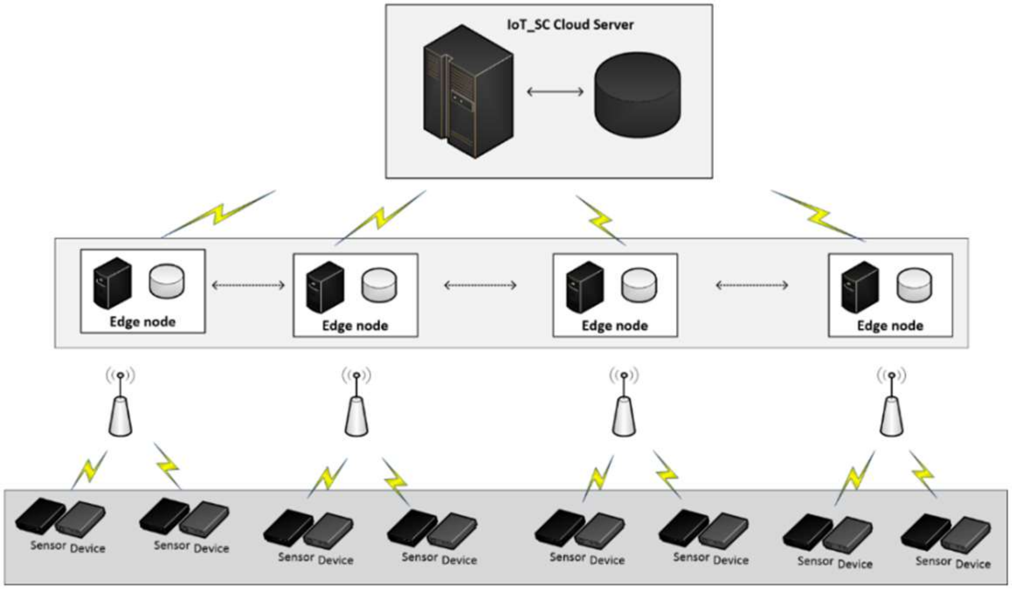
Tampering and Physical Attacks: Tag traceability and the binding of tags to control chips make it difficult to tamper with devices without detection. Any changes in the tag trace or the control chip identity will be flagged during the final verification process.

K. Yang, D. Forte, and M. M. Tehranipoor, “Protecting endpoint devices in IoT supply chain,” *IEEE Xplore*, Nov. 01, 2015. https://ieeexplore.ieee.org/abstract/document/7372591

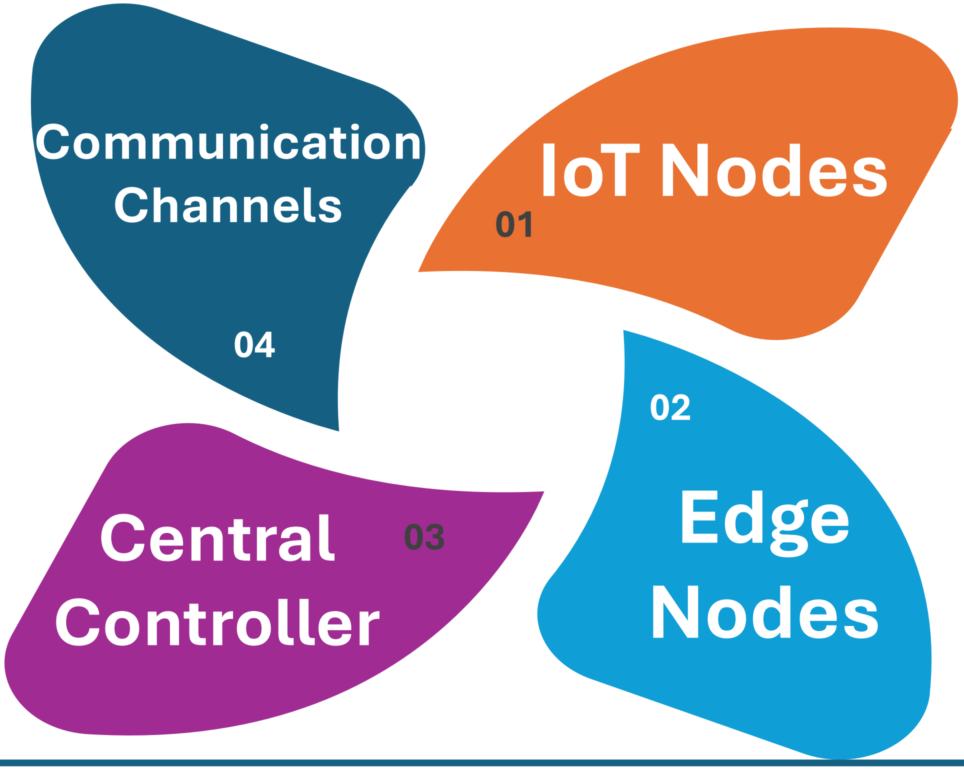
Intuitive Development to Examine Collaborative IoT Supply Chain System Underlying Privacy and Security Levels and Perspective Powering through Proactive Blockchain

Shahzad, Aamir & Zhang, Kaiwen & Gherbi, Abdelouahed. (2020).

IoT-SC System Architecture



Major Components



01 IoT Nodes

02 Edge Nodes

03 Central Controller

04 Communication Channels

Shahzad, Aamir & Zhang, Kaiwen & Gherbi, Abdelouahed. (2020). Intuitive Development to Examine Collaborative IoT Supply Chain System Underlying Privacy and Security Levels and Perspective Powering through Proactive Blockchain. Sensors. 20. 3760. 10.3390/s20133760.

Intuitive Development to Examine Collaborative IoT Supply Chain System Underlying Privacy and Security Levels and Perspective Powering through Proactive Blockchain

Shahzad, Aamir & Zhang, Kaiwen & Gherbi, Abdelouahed. (2020).

Privacy

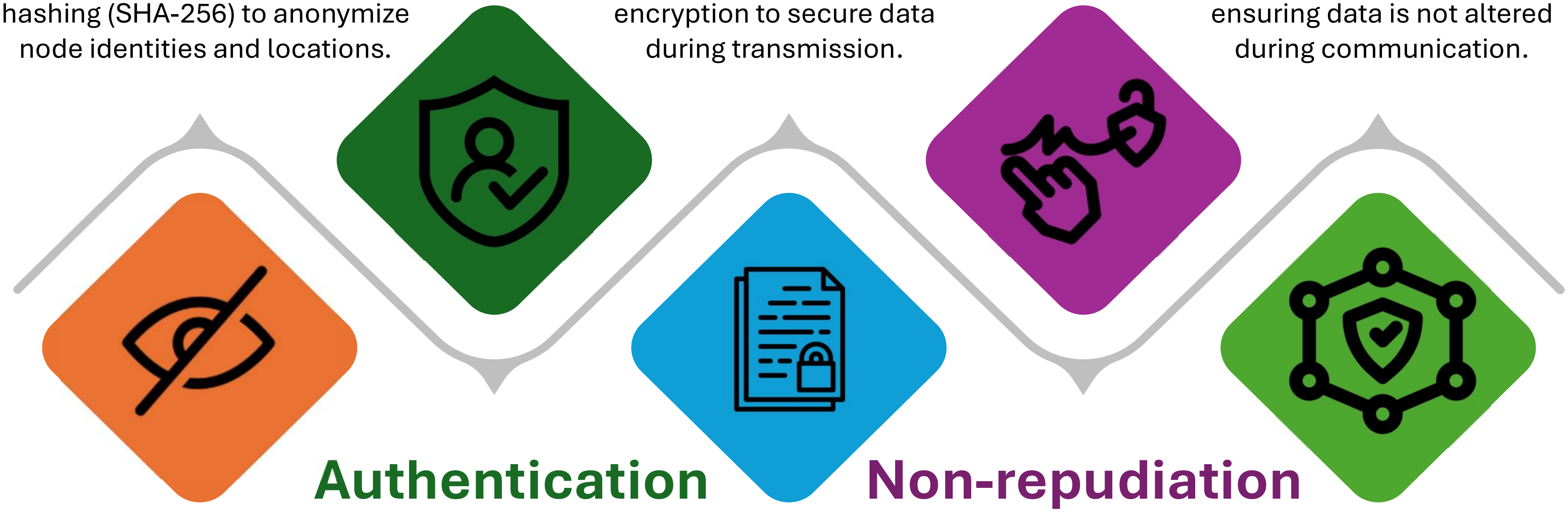
Achieved through cryptographic hashing (SHA-256) to anonymize node identities and locations.

Confidentiality

Ensured by using AES encryption to secure data during transmission.

Integrity

Verified through hashing, ensuring data is not altered during communication.



Authentication

Managed by using MAC (Message Authentication Codes) and unique shared keys.

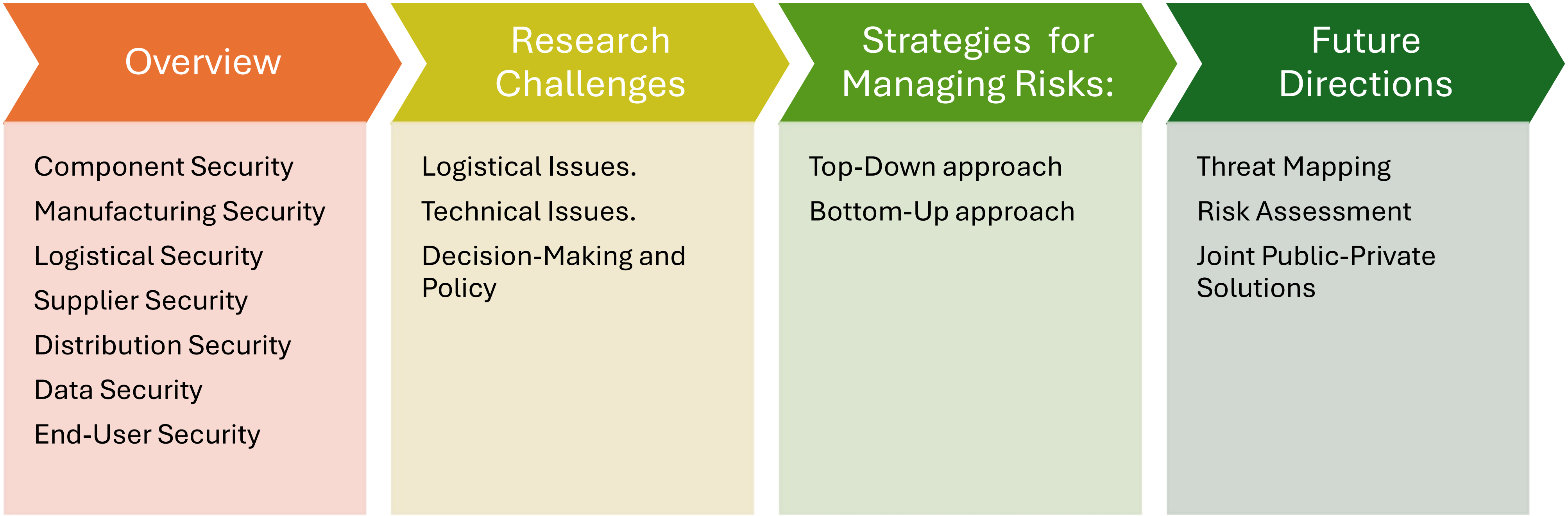
Non-repudiation

Implemented with RSA digital signatures, preventing any entity from denying its actions.

Shahzad, Aamir & Zhang, Kaiwen & Gherbi, Abdelouahed. (2020). Intuitive Development to Examine Collaborative IoT Supply Chain System Underlying Privacy and Security Levels and Perspective Powering through Proactive Blockchain. Sensors. 20. 3760. 10.3390/s20133760.

IoT Supply Chain Security: Overview, Challenges, and the Road Ahead

Farooq, Junaid & Zhu, Quanyan. (2019)



Overview

- Component Security
- Manufacturing Security
- Logistical Security
- Supplier Security
- Distribution Security
- Data Security
- End-User Security

Research Challenges

- Logistical Issues.
- Technical Issues.
- Decision-Making and Policy

Strategies for Managing Risks:

- Top-Down approach
- Bottom-Up approach

Future Directions

- Threat Mapping
- Risk Assessment
- Joint Public-Private Solutions

Farooq, Junaid & Zhu, Quanyan. (2019). IoT Supply Chain Security: Overview, Challenges, and the Road Ahead. 10.13140/RG.2.2.12780.51840.

Stage II: SoK

Attack Landscape

A supply chain attack is a combination of at least two attacks. The first attack is on a supplier that is then used to attack the target to gain access to its assets. The target can be the final customer or another supplier. For an attack to be classified as a supply chain one, both the supplier and the customer must be targets.

Direct Attacks

- Hacking Attacks
- Denial of service
- Passwords for financial gains
- Industrial espionage
- Compromises to intellectual property

Indirect Attacks

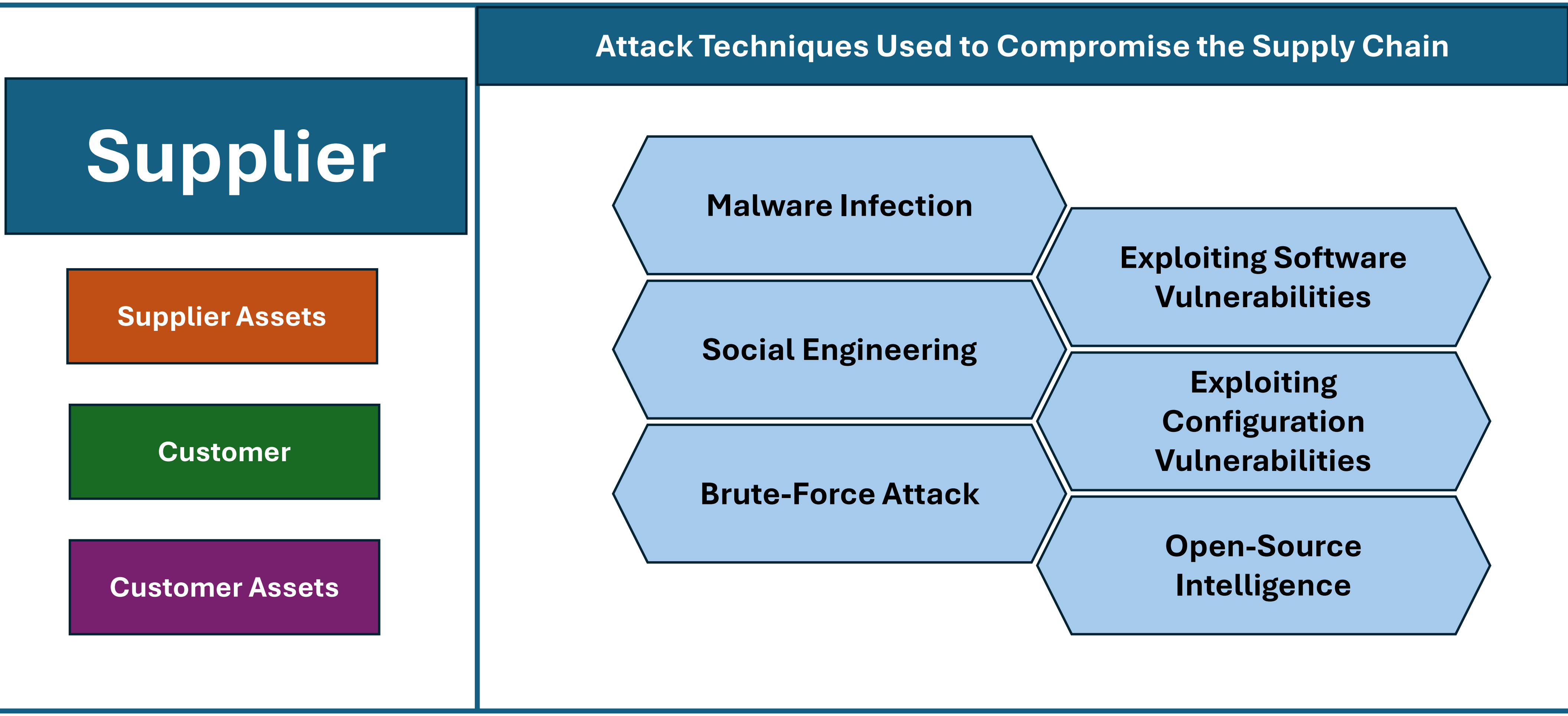
In indirect attacks, the attacker's layout "bait" enables them to access the target system.

- Viruses
- Spoofing attacks
- Counterfeit products
- Worms and trojans
- Soft-and hardware malicious codes

If employees accept the bait by visiting a website or downloading software, the attacker gains access to the system.

Olav Lysne. 2018. The Huawei and Snowden Questions Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment? Springer Cham. https://doi.org/10.1007/978-3-319-74950- 1

Taxonomy of Supply Chain Attacks



Supplier

Supplier Assets

Customer

Customer Assets

Attack Techniques Used to Compromise the Supply Chain

Malware Infection

Social Engineering

Brute-Force Attack

Exploiting Software Vulnerabilities

Exploiting Configuration Vulnerabilities

Open-Source Intelligence

ENISA. 2021. Threat Landscape for Supply Chain Attacks. Report. ENISA, Athens, Greece. https://www.enisa.europa.eu/publications/threat-landscape-for-supplychain-attacks

Taxonomy of Supply Chain Attacks

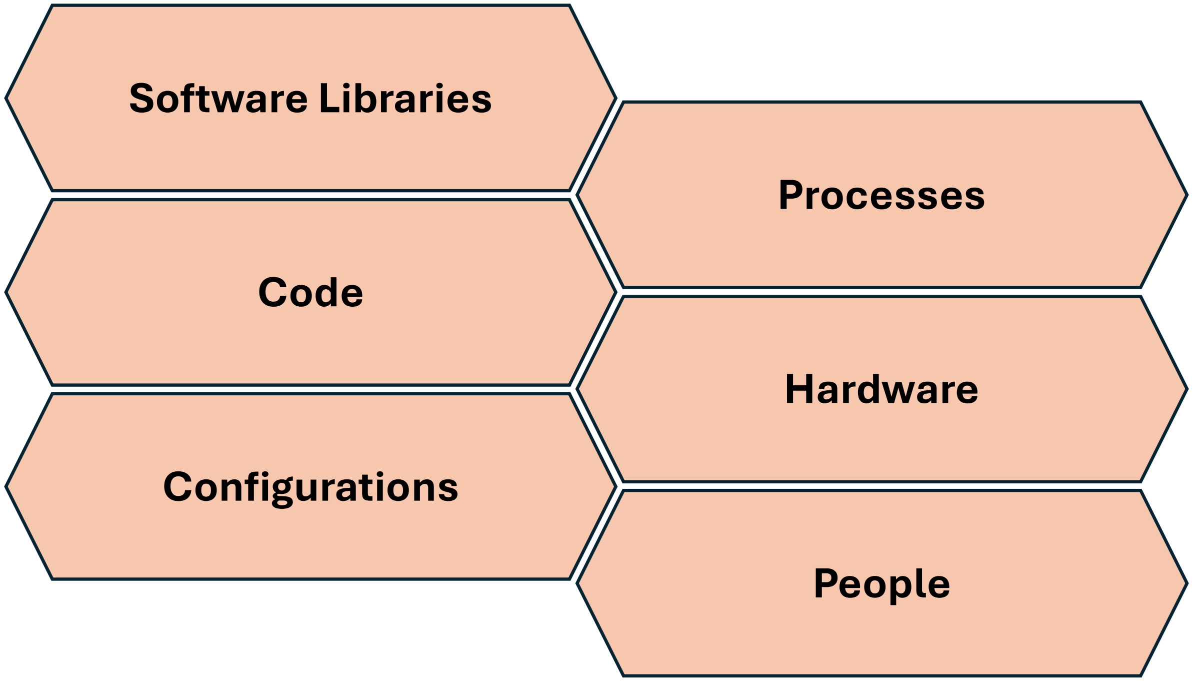
Supplier

Supplier Assets

Customer

Customer Assets

Supplier Assets Targeted by the Supply Chain Attack



Software Libraries

Code

Configurations

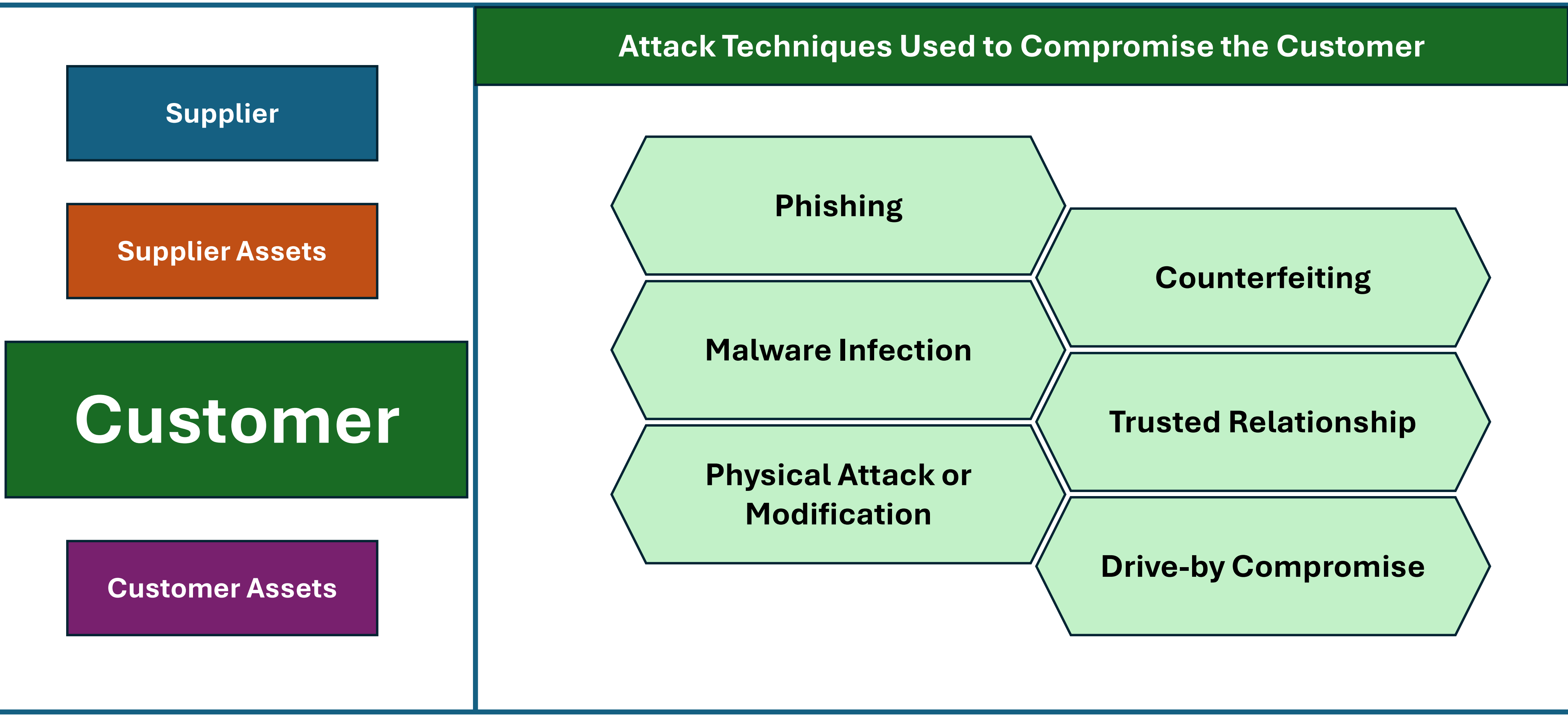
Processes

Hardware

People

ENISA. 2021. Threat Landscape for Supply Chain Attacks. Report. ENISA, Athens, Greece. https://www.enisa.europa.eu/publications/threat-landscape-for-supplychain-attacks

Taxonomy of Supply Chain Attacks



Supplier

Supplier Assets

Customer

Customer Assets

Attack Techniques Used to Compromise the Customer

Phishing

Counterfeiting

Malware Infection

Trusted Relationship

Physical Attack or Modification

Drive-by Compromise

ENISA. 2021. Threat Landscape for Supply Chain Attacks. Report. ENISA, Athens, Greece. https://www.enisa.europa.eu/publications/threat-landscape-for-supplychain-attacks

Taxonomy of Supply Chain Attacks

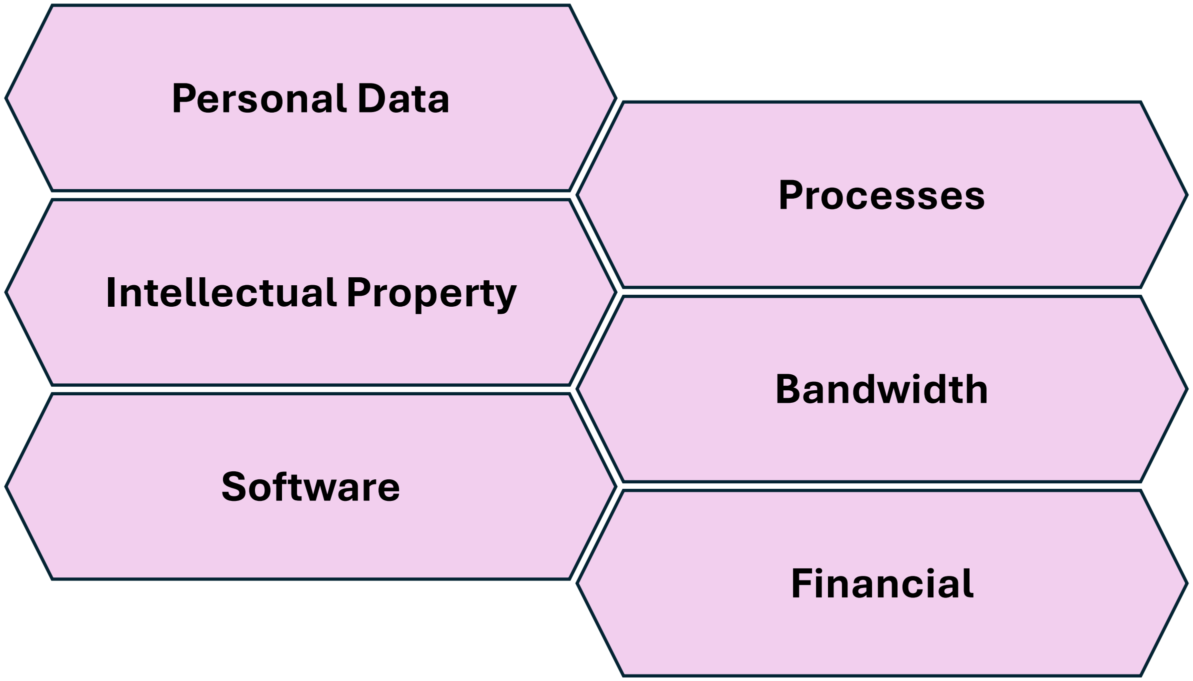
Supplier

Supplier Assets

Customer Assets

Customer Assets

Customer Assets Targeted by the Supply Chain Attack



Personal Data

Processes

Intellectual Property

Bandwidth

Software

Financial

ENISA. 2021. Threat Landscape for Supply Chain Attacks. Report. ENISA, Athens, Greece. https://www.enisa.europa.eu/publications/threat-landscape-for-supplychain-attacks

Managing Supply Chain Risks

Technical

Personnel

Procedural

However, a supply chain attack uses legitimate, trusted processes to gain full access to organizations' data by targeting the vendor's software source code, updates or build processes. As a result, many authors argue that such technical countermeasures only provide a partial solution

[illegible] form the most fundamental layer of protection

They specify system accessibility and are designed to make aggression less attractive to attackers

Includes firewalls and passwords (access control) or the diversification of software and hardware

Managing Supply Chain Risks

Technical

Personnel

Procedural

Risk awareness initiatives and training are among the most cited countermeasures in the literature.

Low-security awareness among employees has been consistently identified as the number one barrier to IT security's success.

In cyberspace, employees are a significant failure point. This is often neglected.

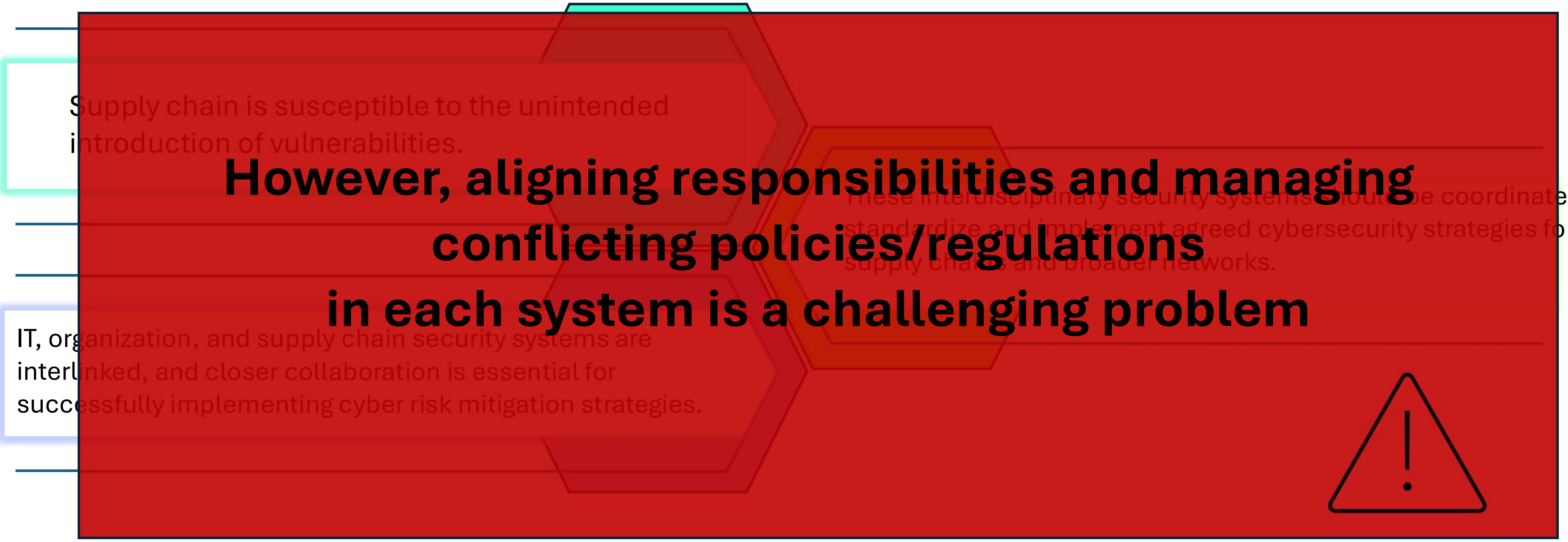
But supply chain security and the means and tools to support it are not explicitly included in cybersecurity curricula.

Managing Supply Chain Risks

Technical

Personnel

Procedural



Supply chain is susceptible to the unintended introduction of vulnerabilities.

IT, organization, and supply chain security systems are interlinked, and closer collaboration is essential for successfully implementing cyber risk mitigation strategies.

These interdisciplinary security systems should be coordinated to standardize and implement agreed cybersecurity strategies for supply chains and broader networks.

However, aligning responsibilities and managing conflicting policies/regulations in each system is a challenging problem

RAIN RFID Security

What is it?

Radio Identification Industry Alliance

Ultra High Frequency Tags

Industry Standard

But what about *cloud?*

Security Analyses

Kill Feature

8 Character Pin

Authentication Feature

Short-Range Mode

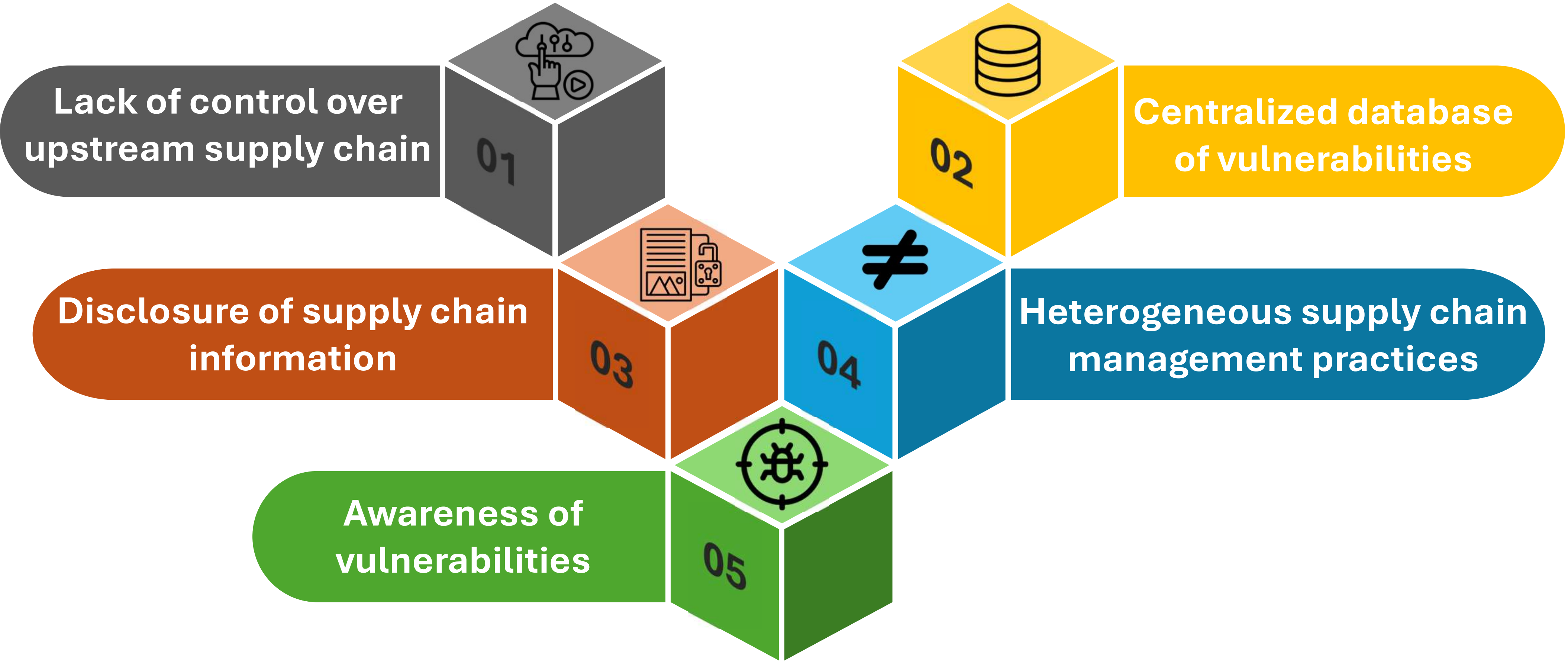
Encryption:

- **XOR**
- **AES128**
- **Present80**
- **CryptoGPS**

Khalid, Ahmad & Conchon, Emmanuel & Peyrard, Fabrice. (2016). Evaluation of RAIN RFID authentication schemes. 1-8. 10.1109/SSIC.2016.7571807.

Robshaw, M.J.B., & Williamson, T. (2015). RAIN RFID and the Internet of Things: Industry Snapshot and Security Needs. Impinj. NIST Lightweight Cryptography Workshop 2015, 1-27

Challenges



01 Lack of control over upstream supply chain

02 Centralized database of vulnerabilities

03 Disclosure of supply chain information

04 Heterogeneous supply chain management practices

05 Awareness of vulnerabilities

Omitola, Tope & Wills, Gary. (2018). Towards Mapping the Security Challenges of the Internet of Things (IoT) Supply Chain. Procedia Computer Science. 126. 441-450. 10.1016/j.procs.2018.07.278.

Future Research

❑ More research is needed to design risk assessment approaches tailored to the specificities of the digital supply chain

- particularly in critical infrastructure environments
- identification of 0-day vulnerabilities
- continuous, dynamic assessment of the associated risk
- forecasting of possible cascading effects across infrastructure sector

❑ Further research is needed to provide infrastructures for sharing data and information

- this will allow the secure identification of actors and products as well as the privacy of actors and will facilitate the automatic analysis of shared elements.

❑ Research is needed to develop automated mechanisms for the analysis of standard requirements and for the continuous monitoring for compliance with standards.

❑ Need to consider how business continuity can be ensured in the face of a successful digital supply chain attack.

❑ Need to design and develop training and education programs on managing supply chain cybersecurity risks

References

Nozari, Hamed & Fallah, Mohammad & Szmelter-Jarosz, Agnieszka & Krzemiński, Maciej. (2021). Analysis of Security Criteria for IoT-Based Supply Chain: A Case Study of FMCG Industries. Central European Management Journal. 29. 10.7206/cemj.2658-0845.63.

Shahzad, Aamir & Zhang, Kaiwen & Gherbi, Abdelouahed. (2020). Intuitive Development to Examine Collaborative IoT Supply Chain System Underlying Privacy and Security Levels and Perspective Powering through Proactive Blockchain. Sensors. 20. 3760. 10.3390/s20133760.

Abdel-Basset, Mohamed & Mohamed, Mai. (2018). Internet of Things and its Impact on supply chain: A framework for building smart, secure and efficient systems. Future Generation Computer Systems. 86. 10.1016/j.future.2018.04.051.

Zhou, Wei & Piramuthu, Selwyn. (2018). IoT security perspective of a flexible healthcare supply chain. Information Technology and Management. 19. 10.1007/s10799-017-0279-7.

Omitola, Tope & Wills, Gary. (2018). Towards Mapping the Security Challenges of the Internet of Things (IoT) Supply Chain. Procedia Computer Science. 126. 441-450. 10.1016/j.procs.2018.07.278.

Yang, Kun & Forte, Domenic & Tehranipoor, Mark. (2015). Protecting endpoint devices in IoT supply chain. 351-356. 10.1109/ICCAD.2015.7372591.

Al-Talib, Moayad & Melhem, Wasen & Anosike, Anthony & Garza-Reyes, Jose Arturo & Nadeem, Simon & Kumar, Anil. (2020). Achieving resilience in the supply chain by applying IoT technology. Procedia CIRP. 91. 10.1016/j.procir.2020.02.231.

Hiromoto, Robert & Haney, Michael & Vakanski, Aleksandar. (2017). A secure architecture for IoT with supply chain risk management. 431-435. 10.1109/IDAACS.2017.8095118.

Hassija, Vikas & Chamola, Vinay & Gupta, Vatsal & Jain, Sarthak & Guizani, Nadra. (2020). A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures. IEEE Internet of Things Journal. PP. 10.1109/JIOT.2020.3025775.

Hasan, A S M Touhidul & Sabah, Shabnam & Haque, Rakib Ul & Daria, Apubra & Rasool, Dr & Jiang, Qingshan. (2022). Towards Convergence of IoT and Blockchain for Secure Supply Chain Transaction. Symmetry. 14. 10.3390/sym14010064.

Kieras, Timothy & Farooq, Junaid & Zhu, Quanyan. (2021). I-SCRAM: A Framework for IoT Supply Chain Risk Analysis and Mitigation Decisions. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3058338.

Kieras, Timothy & Farooq, Junaid & Zhu, Quanyan. (2020). RIoTS: Risk Analysis of IoT Supply Chain Threats. 1-6. 10.1109/WF-IoT48130.2020.9221323.

Khalid, Ahmad & Conchon, Emmanuel & Peyrard, Fabrice. (2016). Evaluation of RAIN RFID authentication schemes. 1-8. 10.1109/SSIC.2016.7571807.

Robshaw, M.J.B., & Williamson, T. (2015). RAIN RFID and the Internet of Things: Industry Snapshot and Security Needs. Impinj. NIST Lightweight Cryptography Workshop 2015, 1-27

Farooq, Junaid & Zhu, Quanyan. (2019). IoT Supply Chain Security: Overview, Challenges, and the Road Ahead. 10.13140/RG.2.2.12780.51840.

Thank You!!