Subverting Counter Mode Encryption for Hidden Communication in High-Security Infrastructures

Exploiting the AES GCM Authentication Tag for Hidden Communications

Alexander Hartl [1], **Joachim Fabini [1]**, Christoph Roschger [2],
Peter Eder-Neuhauser [3], Marco Petrovic [3], Roman Tobler [3], Tanja Zseby [1]

IRTF CFRG Meeting | IETF113, 24.03.2022

[1] TU Wien
[2] TGM - Vienna Institute of Technology
[3] Wiener Netze GmbH

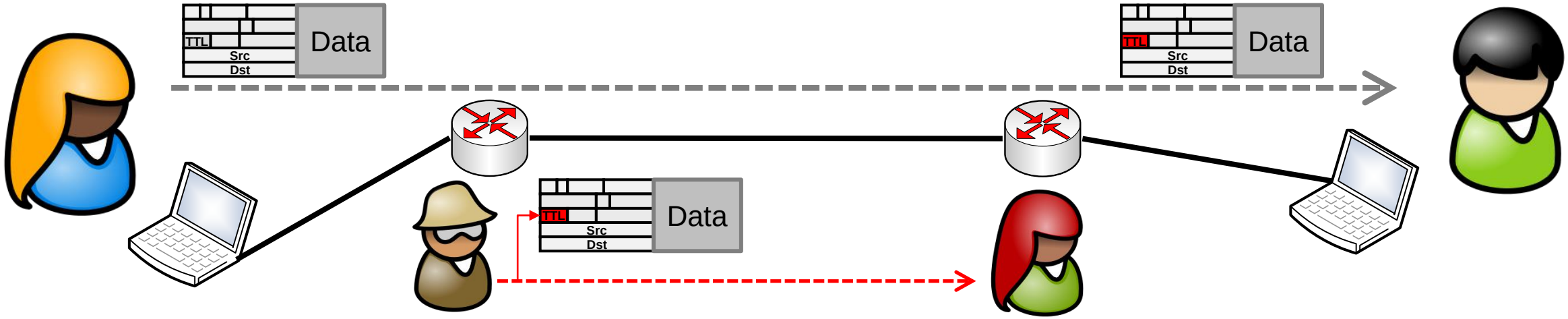
Bundesministerium
Landwirtschaft, Regionen
und Tourismus

KIRAS
Sicherheitsforschung

FFG
Forschung wirkt.

Introduction

- Modern malware prefers **hidden communication** (steganography)
  - **Misuse legitimate, existing network communication** (of potentially benign parties)
  - **Covert** communication: mutable protocol fields and headers at various layers, packet timing, …
    - Network layer: IP TTL, flags, options, inter-arrival-time, …
  - **Subliminal** communication: random numbers, cryptographical nonces, etc.

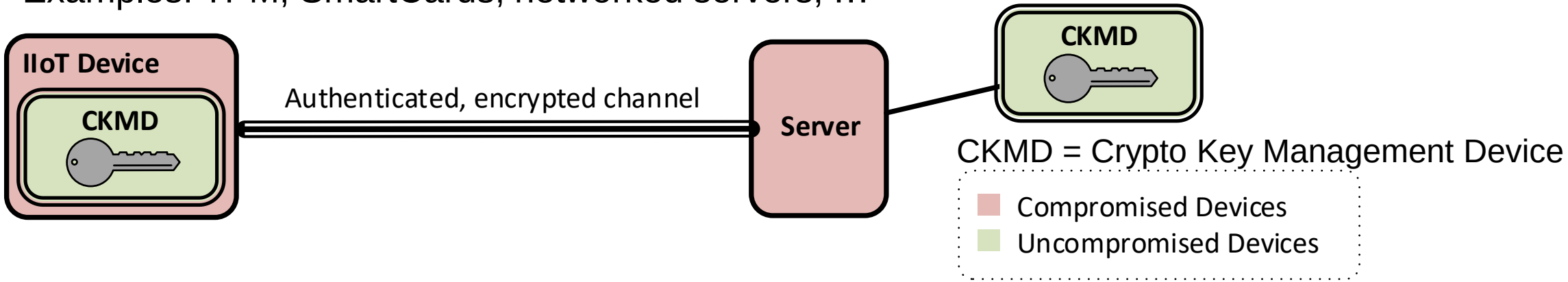


Hardening Systems in Critical Infrastructures

Assumption: **any system is vulnerable**

- Complexity of today‘s software is no longer manageable: **Who discovers vulnerabilities? When?**

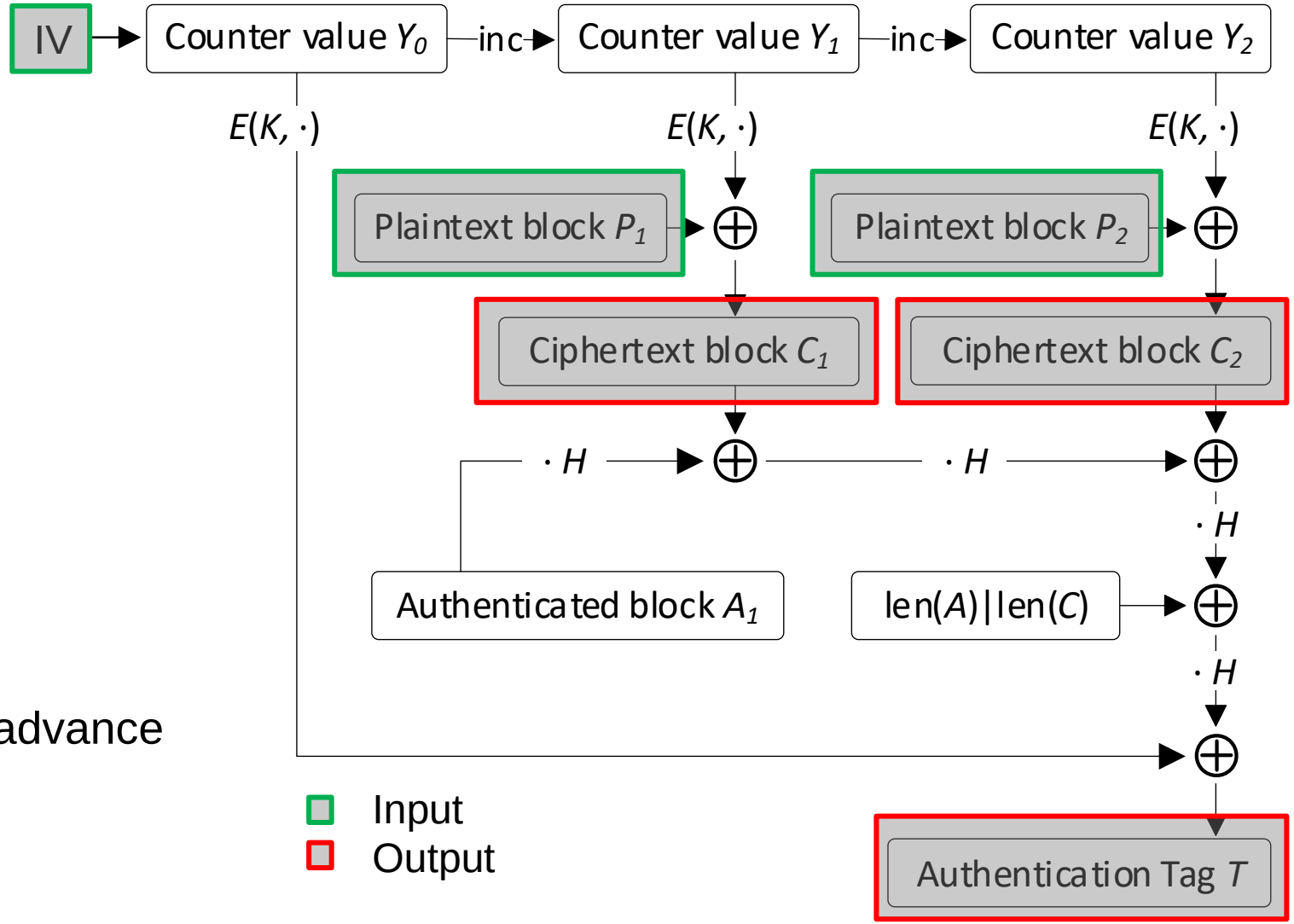
- **Protect crypto key access** through hardware devices
  - **Access only through well-defined APIs only**: encrypt, decrypt
  - Benefit: cryptographic keys can‘t be leaked (even on compromise of the system)
  - Examples: TPM, SmartCards, networked servers, …



- Compromised devices
  - **Research Question: Can malware exploit cryptography for hidden communications in hardened systems?**

Galois/Counter Mode (GCM)

- AES-GCM widely deployed
  - TLS 1.2, 1.3
  - SSH
  - IPsec
  - MACsec
- Attractive properties
  - Fast and parallelizable
  - Provable security and provable multi-user security
  - Key stream pre-computable in advance
  - Free of patents



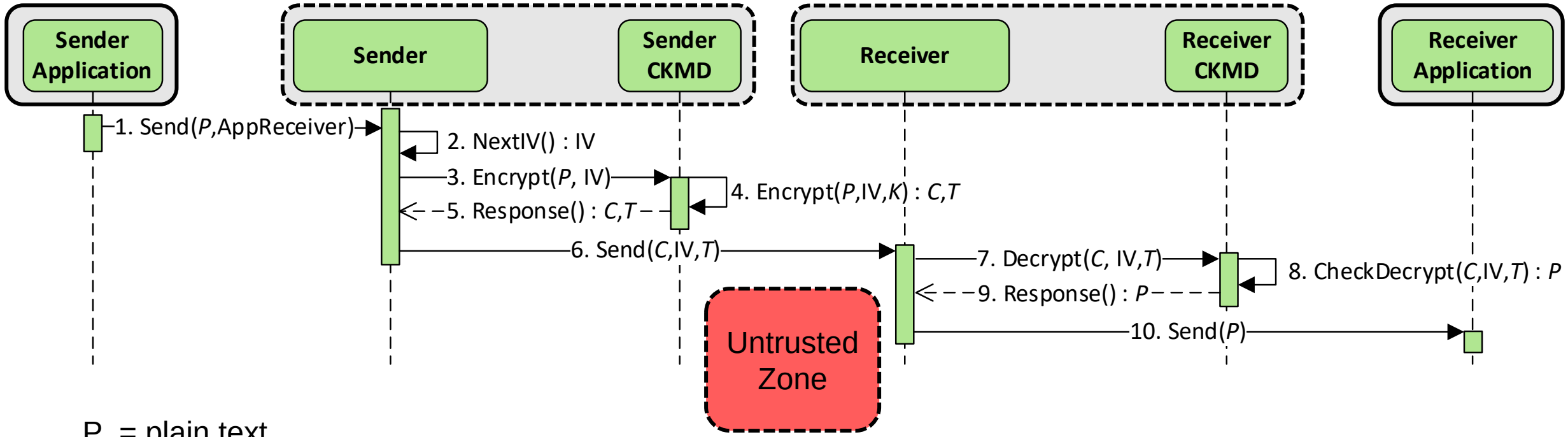
Initialization Vector (IV) Selection Methods

- **Random**
  - No state-keeping necessary
- **Deterministic (Counting IVs)**
  - Not just a probabilistic statement of IV reuse
  - Avoid having to transmit IV
  - Has been argued to limit facilities for hidden communication

- When using a CKMD, state-keeping is difficult (cost, robustness, …)

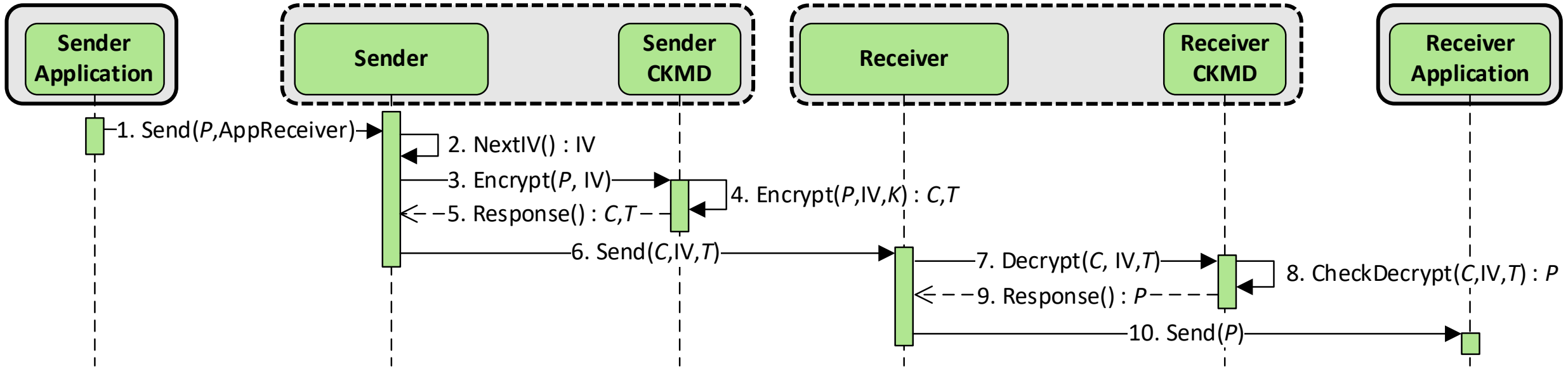
  → Deterministic IVs are likely **managed by the requesting device**

Legitimate Device Communication



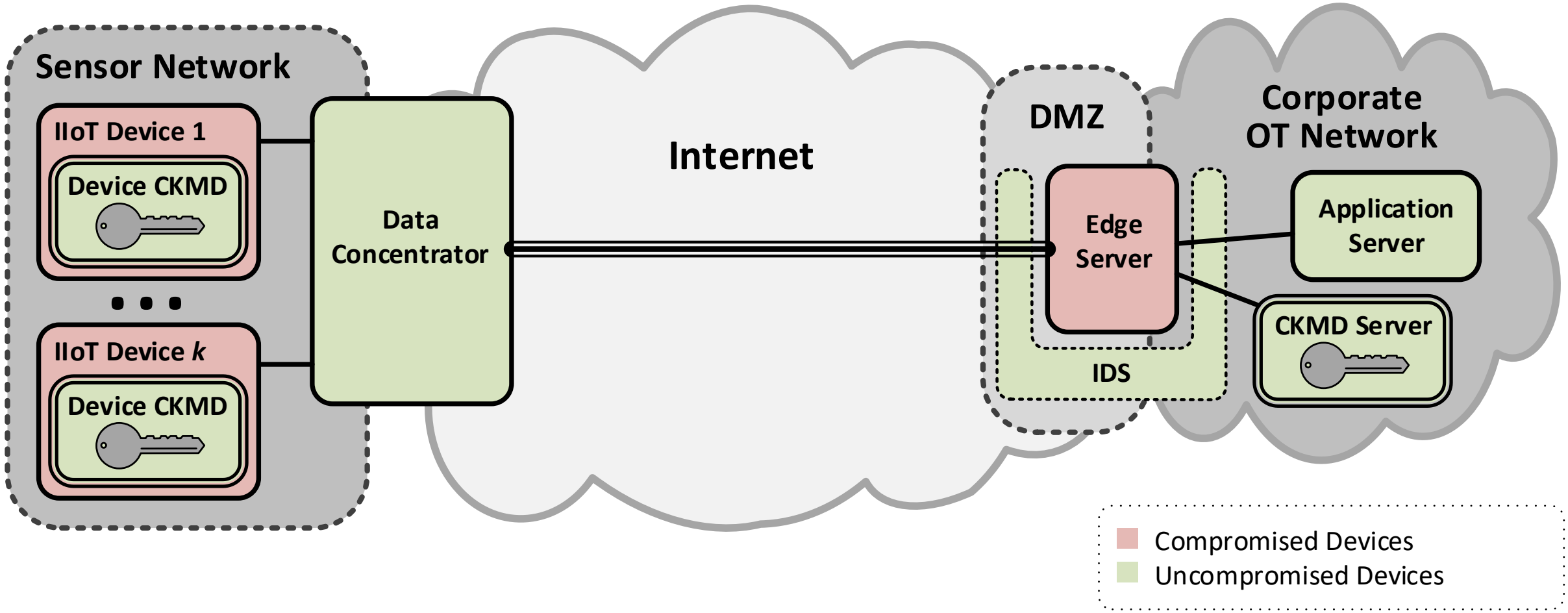
P = plain text
C = cipher text
IV = initialization vector
T = authentication tag

Legitimate Device Communication

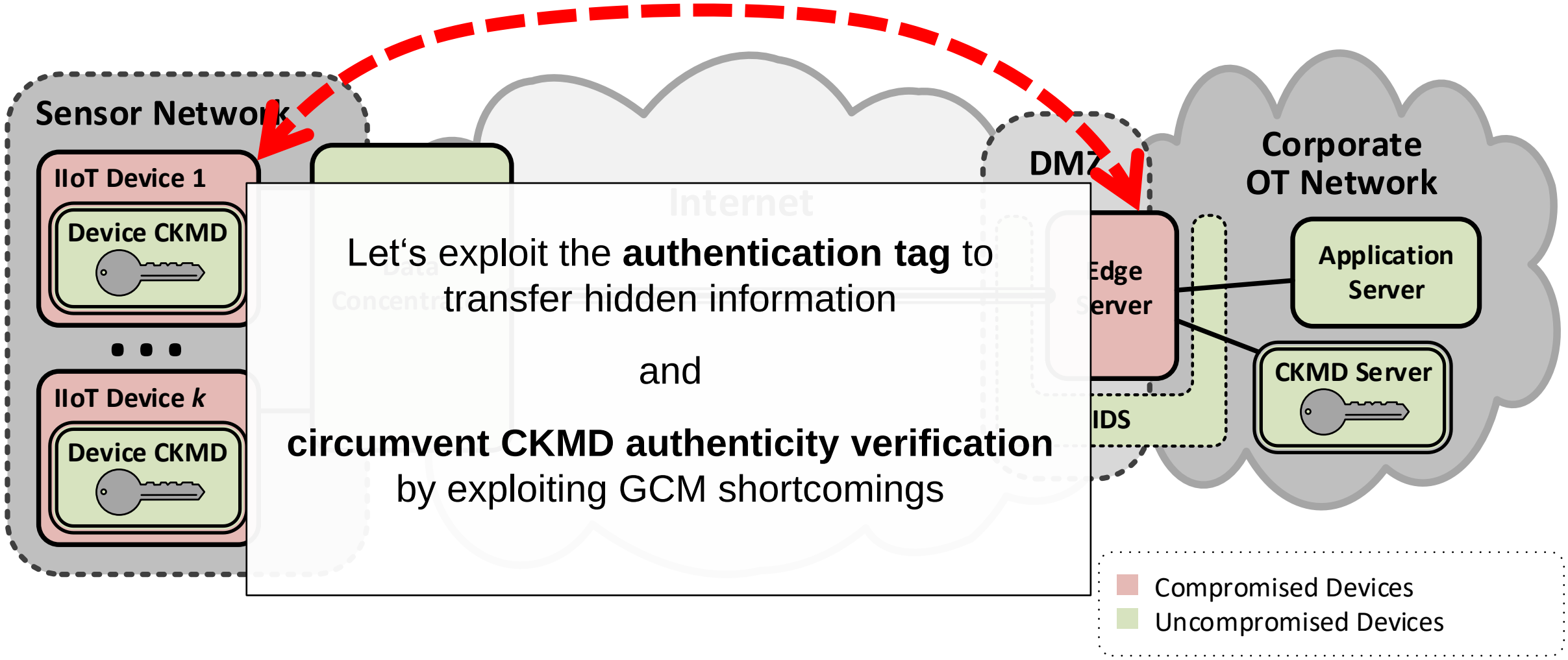


- **Observation:** GCM works similar to stream ciphers
  → **we can decrypt by encrypting with same IV** !
  → **we can decrypt circumventing authenticity verification**
- Also encryption can be attacked by requesting encryption with same IV
- Similar problems exist also for other counter encryption modes

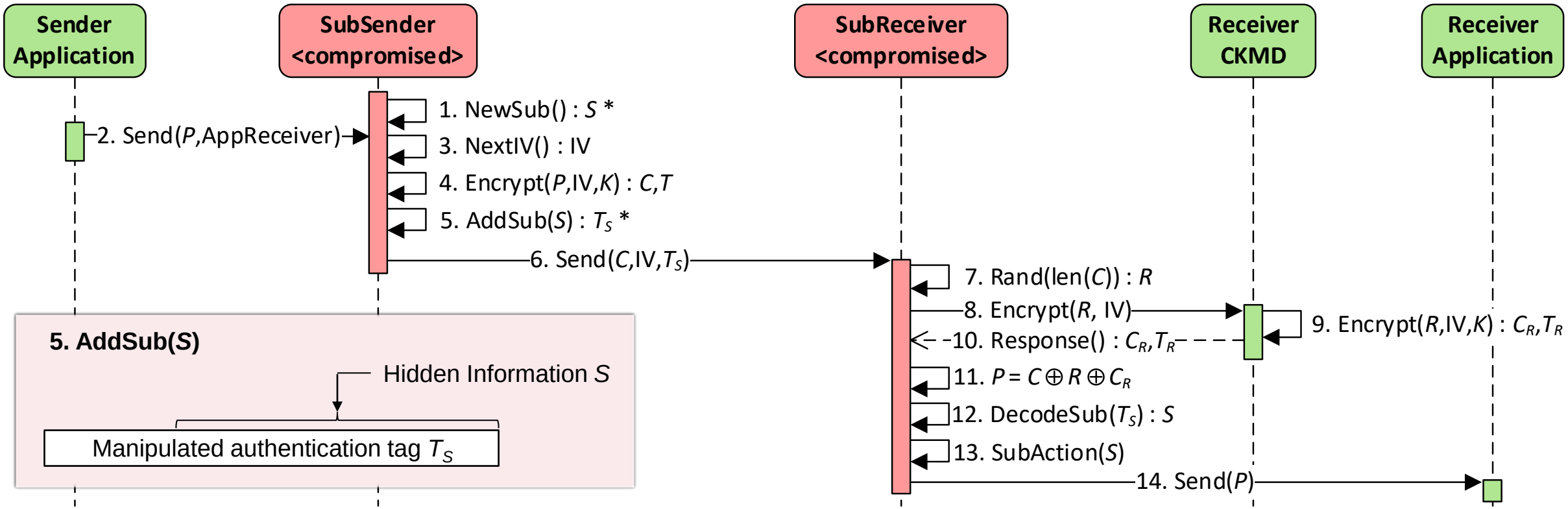
Example: An IIoT Infrastructure



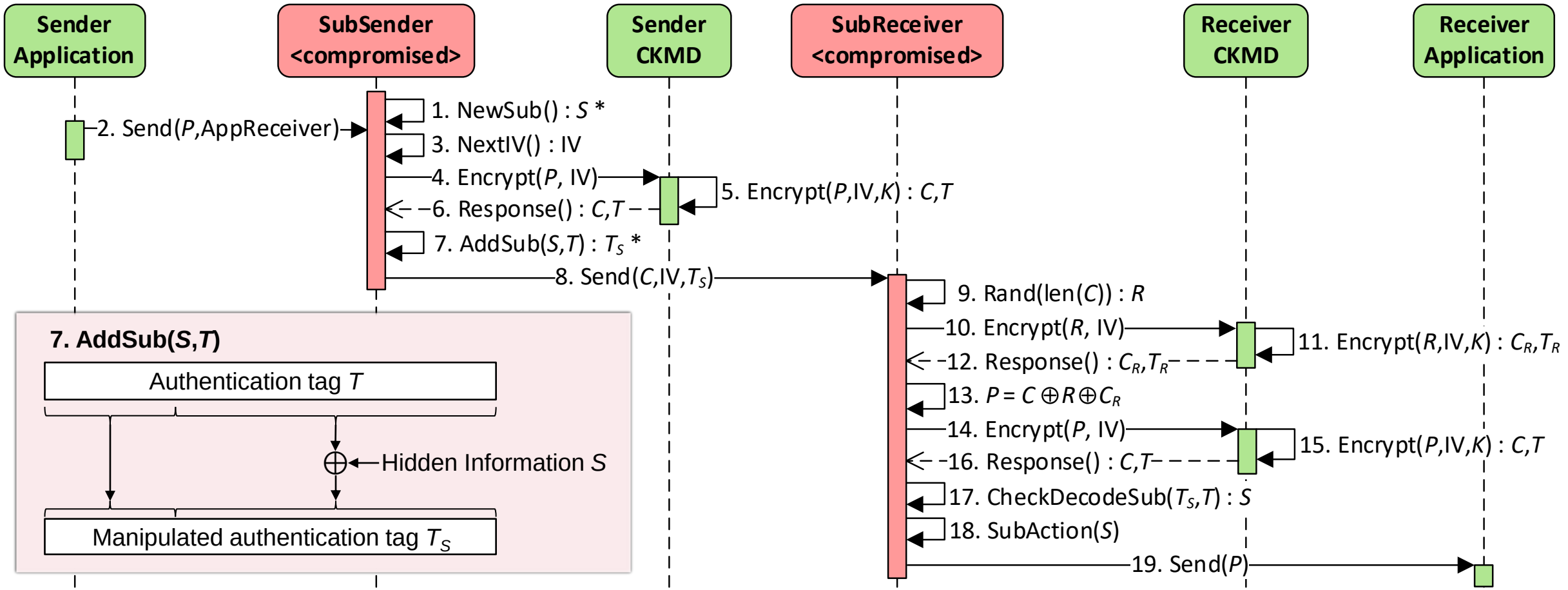
Example: An IIoT Infrastructure



A Simple Subliminal Channel

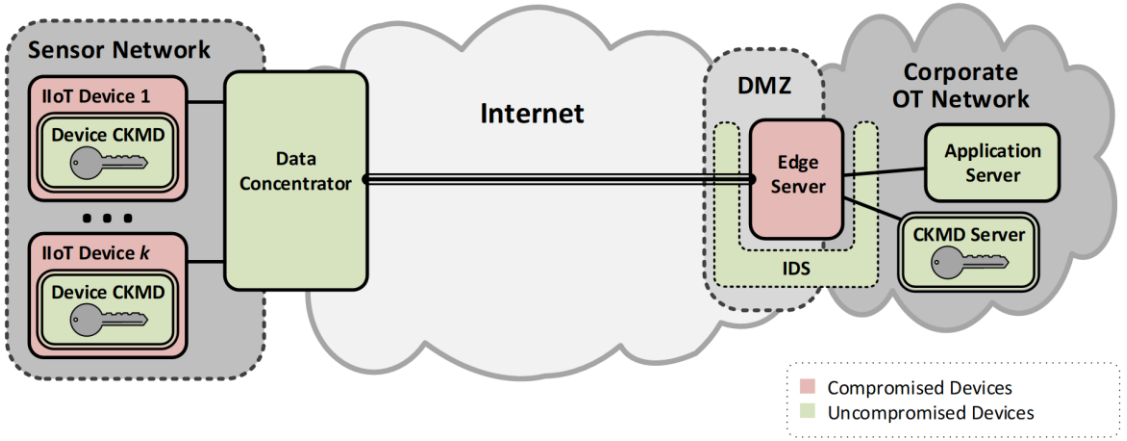


An Advanced Subliminal Channel



Properties of the Subliminal Channel

- **Deployment**
  - Agnostic to protocol semantics
  - Cannot be destroyed by intermediate nodes
- **Detection**: Without secret key
  - the subliminal channel can not be revealed
  - hidden information cannot be decoded - even if the subliminal channel is known
- **Capacity**
  - Depends on message rate → usually high, since MACs are transmitted frequently
- **Location** of sender of hidden information
  - Anywhere on communication path, where he can manipulate the message



Mitigations

- Different operational mode for block cipher
  - **(AES-)GCM-SIV**
  - CBC with HMAC
  - ...
- Generate IVs on CKMD
  → Might lead to random IVs: risk of CKMD-originated subliminal channel

If compatibility with existing systems is required:

- Use distinct keys for each direction (forward, reverse)
- On the CKMD, preconfigure part of IV to unique value for each device

Conclusions

- **Combining CKMDs with GCM encryption (or similar modes) can show security shortcomings**
  - Despite non-compromised CKMDs, the authentication tag can be abused for hidden information
  - → subliminal channel with very attractive properties
  - Challenge particularly for systems with high security demands, e.g., in an IIoT infrastructure
- Best remedies: **Use GCM-SIV** or generate IVs on the CKMD
- Paper download: https://dl.acm.org/doi/10.1145/3465481.3470082
  - A. Hartl, J. Fabini, C. Roschger, P. Eder Neuhauser, M. Petrovic, R. Tobler, and T. Zseby: “Subverting Counter Mode Encryption for Hidden Communication in High Security Infrastructures Infrastructures”. In The 16th International Conference on Availability, Reliability and Security (ARES 2021). Association for Computing Machinery, New York, NY, USA, Article 78, 1–11. DOI:https://doi.org/10.1145/3465481.3470082
  - Ask for a pre-published version

This work was supported by the project MALware cOmmunication in cRitical Infrastructures (MALORI), funded by the Austrian security research program KIRAS of the Federal Ministry for Agriculture, Regions and Tourism (BMLRT) under grant no. 873511.

MALORI Project: MALware cOmmunication in cRitical Infrastructures

- https://www.kiras.at/en/financed-proposals/detail/malori

- **Consortium:** academia, operators of critical infrastructures, security software company, public agency
- **Goal:** Analyze potential for hidden malware communication in CI
  - Covert and subliminal communication
  - Identify exploits, detection, and defense options

- **Time frame:** 1/2020 – 06/2022
  - Funded research, KIRAS Programme, Austrian Research Agency (FFG)

- Contact: Joachim Fabini (mailto:Joachim.Fabini@tuwien.ac.at)