Network Steganography

Kevin Lamshöft
Jonas Hielscher
Otto-von-Guericke-University Magdeburg
Advanced Mulitmedia and Security Lab

The Prisoner’s Problem

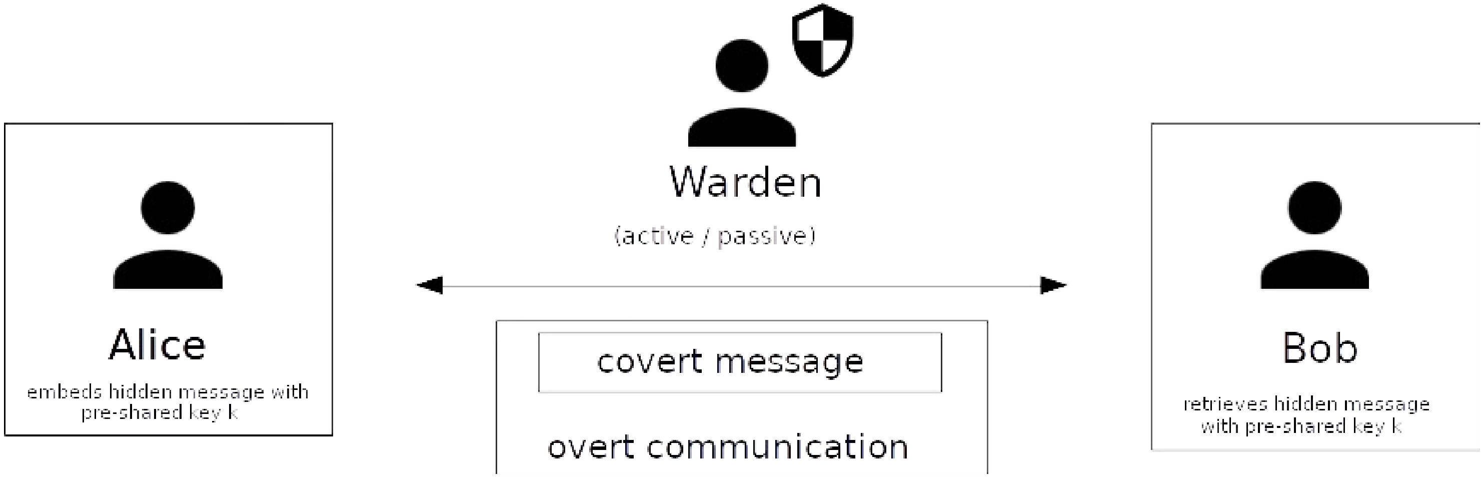

Warden
(active / passive)
Alice
embeds hidden message with pre-shared key k
covert message
overt communication
Bob
retrieves hidden message with pre-shared key k

Figure 1: The Prisoners’ Problem as described by G.J. Simmons [Sim83] and A.D. Ker [Ker16].

here: covert channel := hidden channel

[Sim83] G.J. Simmons, The Prisoners’ Problem and the subliminal channel. In: Chaum D. (eds) Advances in Cryptology. Springer, Boston, MA, https://doi.org/10.1007/978-1-4684-4730-9_5
[Ker16] Andrew D. Ker, Information Hiding – Lecture Notes, Department of Computer Science, Oxford University, 2016, http://www.cs.ox.ac.uk/andrew.ker/docs/informationhiding-lecture-notes-ht2016.pdf

Folie aus:
[LD20] Kevin Lamshöft, Jana Dittmann, “Assessment of Hidden Channel Attacks: Targetting Modbus/TCP”, 21st IFAC World Congress, Germany, July 12-17, 2020

Steganographic communication scenario

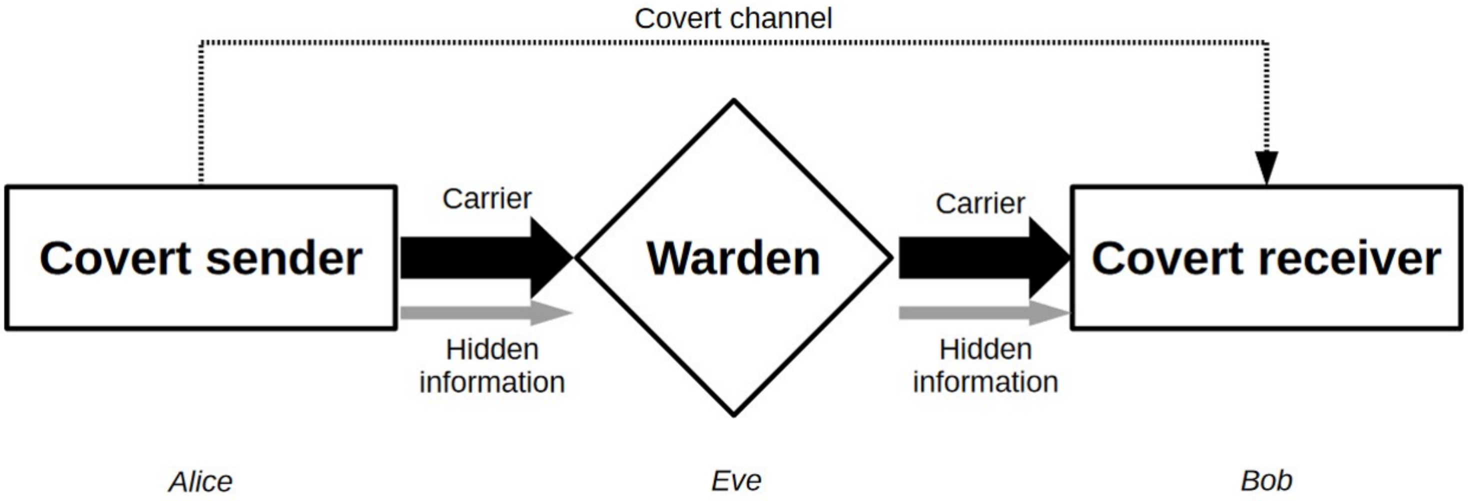


Fig. 1: The default steganographic scenario, with a sender, receiver and Warden. Based on [1].

[1] Sebastian Zander, Grenville Armitage, and Philip Branch. Covert channels in the IP time to live field. 2006.

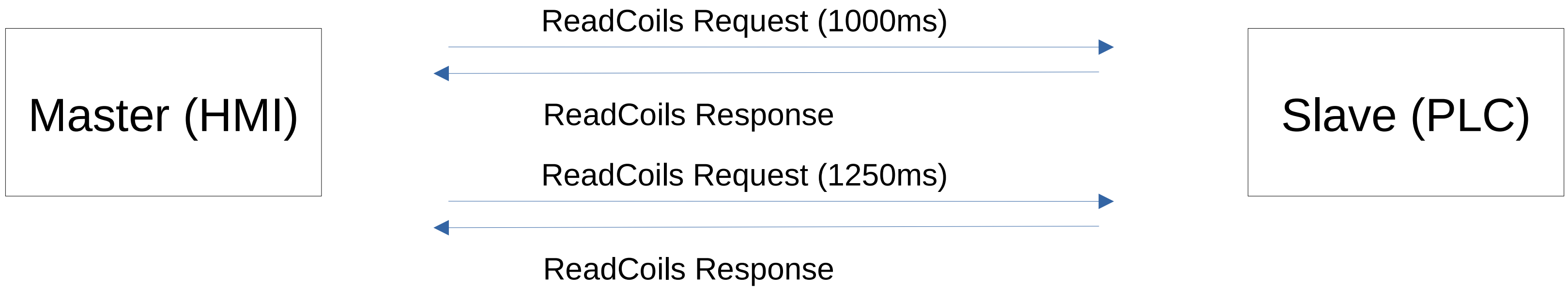
Terminology

History

In classical steganography hidden data are stored in media, for example images.

[1] Steffen Wendzel. NETWORK INFORMATION HIDING: A COURSE ON STEGANOGRAPHY AND COVERT CHANNELS. https://github.com/cdpxe/Network-Covert-Channels-A-University-level-Course/ [November 03. 2020]

Examples for Network Steganography: Interpacket Times



Master (HMI)

ReadCoils Request (1000ms)

ReadCoils Response

ReadCoils Request (1250ms)

ReadCoils Response

Slave (PLC)

Time in ms	0	500	1000	1500	2000	2250	2500	2750	3250	• 3750
Message Type	Read Coils	Write Coils	Read Coils	Write Coils	-	Read Coils (+250ms)	• -	Write Coils (+250ms)	Read Coils (+250ms)	Write Coils (+250ms)
Hidden Message (bit)	-	-	-	-	-	0	-	1	0	• 1

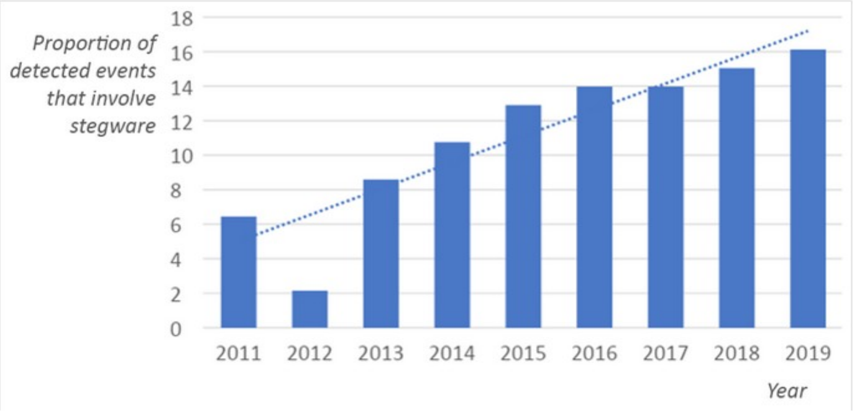
Folie aus:
[LD20] Kevin Lamshöft, Jana Dittmann, “Assessment of Hidden Channel Attacks: Targetting Modbus/TCP”, 21st IFAC World Congress, Germany, July 12-17, 2020

Goals of Steganography

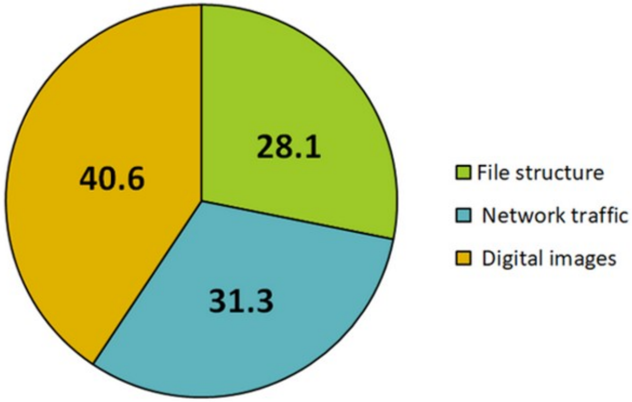
- Main Goal: Hidden communication
  - Enabling stealthy
    - Infiltration of networks and systems
    - Exfiltration of data
    - Command and Control Channnels

- Scenarios
  - APTs
  - Malware
  - Nation-State actors
  - Citizens / Journalists

A Threat?



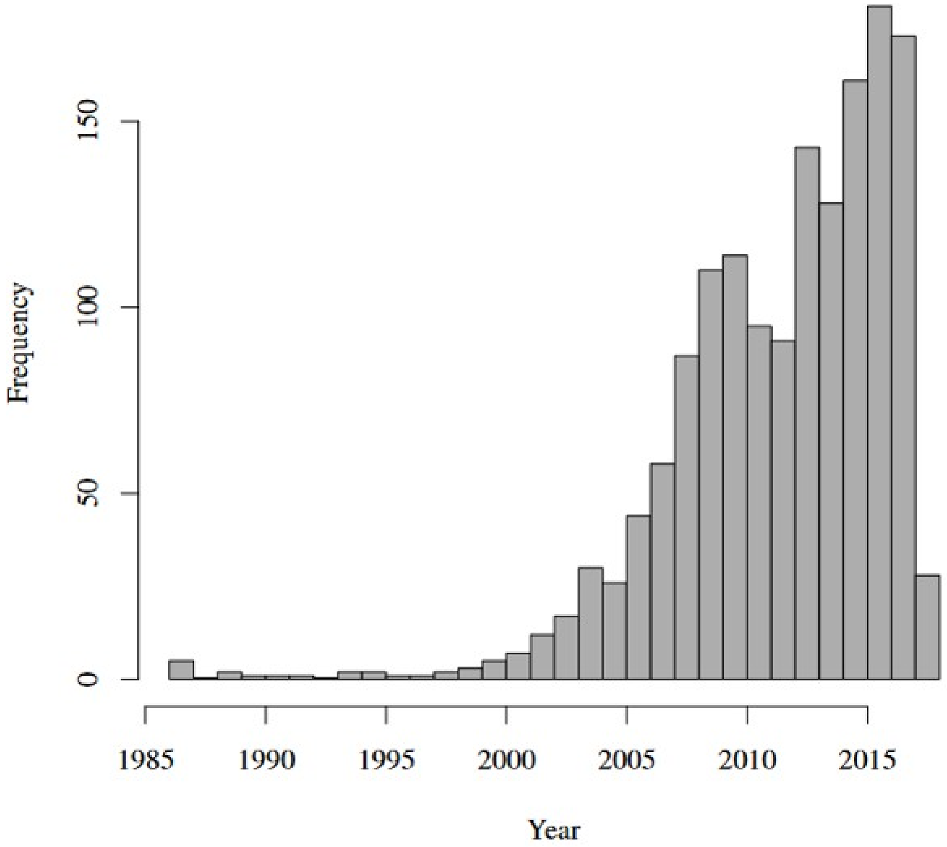
Number of detected Malware events with steganographic capabilities. Screenshot from [1].



Distribution of different hiding techniques in those events. Screenshot from [1].

[1] SIMARGL. Stegware – the latest trend in cybercrime. February 2019. https://simargl.eu/blog/technical/stegware-the-latest-trend-in-cybercrime.

A Threat?



Number of publications in the field of Covert Channel/ Steganography over the last decades. Screenshot from [1].

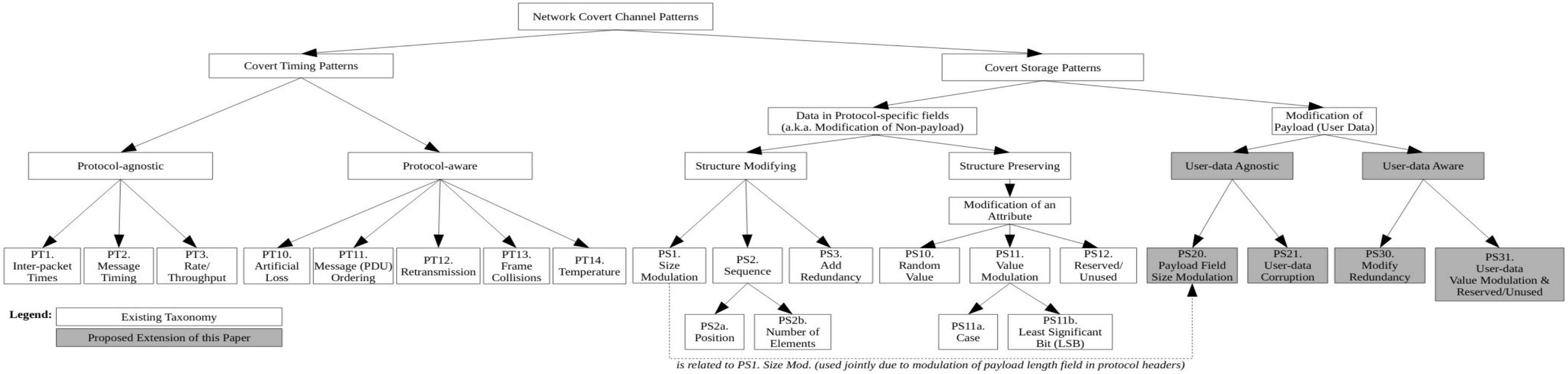
[1] Steffen Wendzel. Get Me Cited, Scotty! Analysis of Citations in Covert Channel/ Steganography Research. In Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018, New York, NY, USA, 2018. Association for Computing Machinery.

A Threat?

- Example Malware from [1]
  - Okrum and Ketrican: C&C communications are hidden in HTTP traffic
  - DarkHydrus: it uses DNS tunneling to transfer information, which is a technique observed in the past also in Morto and Feederbot malware
  - Steganography in contemporary cyberattacks: a general review including Backdoor.Win32.Denis hiding data in a DNS tunnel for C&C communications
  - NanoLocker: the ransomware hide data in ICMP packets

[1] lucacav. steg-in-the-wild. https://github.com/lucacav/steg-in-the-wild [November 03. 2020]

Pattern-based Taxonomy for Network Covert Channels



Network Covert Channel Patterns

Covert Timing Patterns

Covert Storage Patterns

Protocol-agnostic

Protocol-aware

Data in Protocol-specific fields (a.k.a. Modification of Non-payload)

Modification of Payload (User Data)

Structure Modifying

Structure Preserving

User-data Agnostic

User-data Aware

Modification of an Attribute

PT1. Inter-packet Times

PT2. Message Timing

PT3. Rate/ Throughput

PT10. Artificial Loss

PT11. Message (PDU) Ordering

PT12. Retransmission

PT13. Frame Collisions

PT14. Temperature

PS1. Size Modulation

PS2. Sequence

PS3. Add Redundancy

PS10. Random Value

PS11. Value Modulation

PS12. Reserved/ Unused

PS20. Payload Field Size Modulation

PS21. User-data Corruption

PS30. Modify Redundancy

PS31. User-data Value Modulation & Reserved/Unused

PS2a. Position

PS2b. Number of Elements

PS11a. Case

PS11b. Least Significant Bit (LSB)

Legend: Existing Taxonomy

Proposed Extension of this Paper

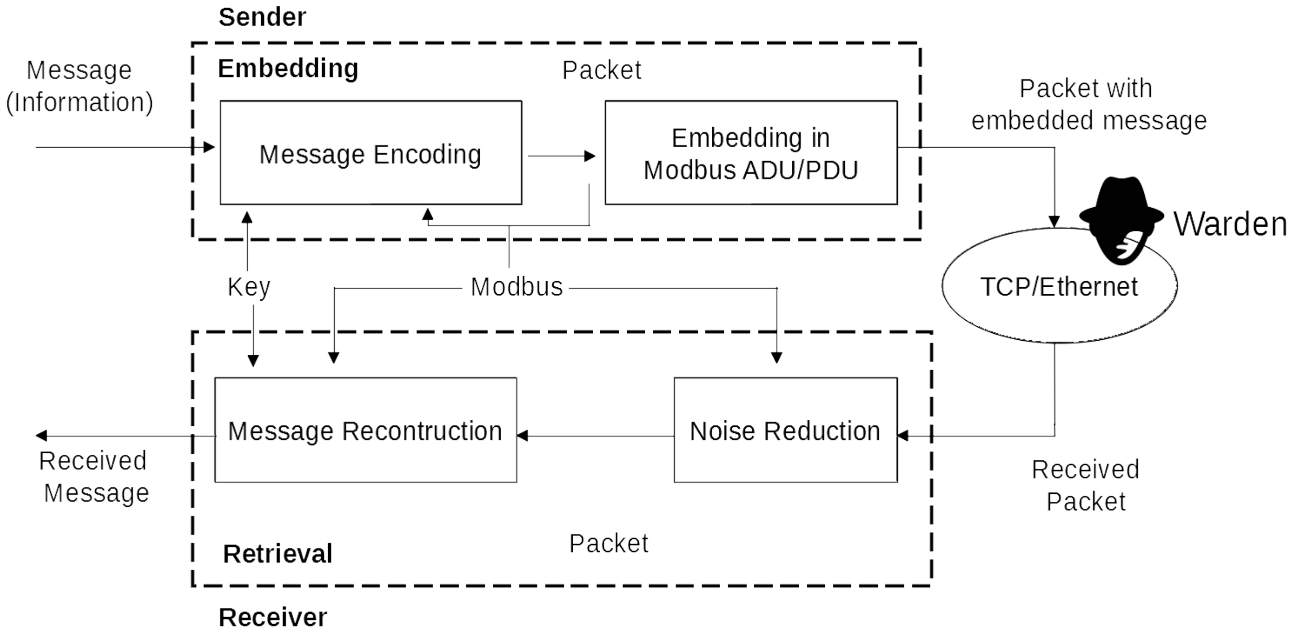
is related to PS1. Size Mod. (used jointly due to modulation of payload length field in protocol headers)

Figure 2: Extended Taxonomy for Classifcation of Network Convet Channel Patters [MWC18]

[MWC18] Wojciech Mazurczyk, Steffen Wendzel, and Krzysztof Cabaj. 2018. Towards Deriving Insights into Data Hiding Methods Using Pattern-based Approach. In Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018). Association for Computing Machinery, New York, NY, USA, Article 10, 1–10. DOI:https://doi.org/10.1145/3230833.3233261

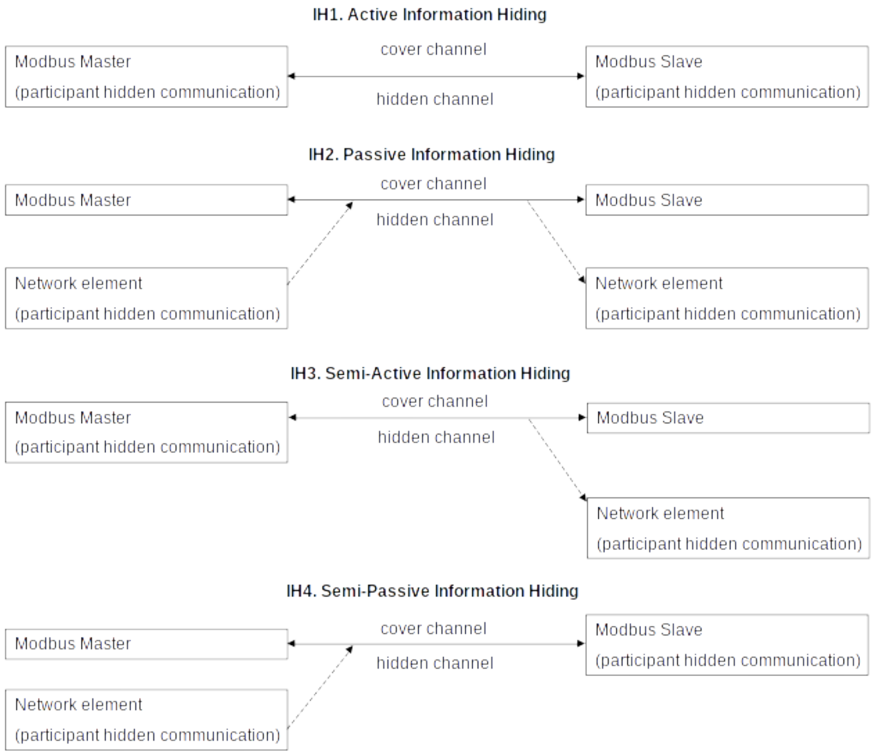
Folie aus:
[LD20] Kevin Lamshöft, Jana Dittmann, “Assessment of Hidden Channel Attacks: Targetting Modbus/TCP”, 21st IFAC World Congress, Germany, July 12-17, 2020

Embedding & Retrieval (at the example of Modbus/TCP)



Folie aus:
[LD20] Kevin Lamshöft, Jana Dittmann, “Assessment of Hidden Channel Attacks: Targetting Modbus/TCP”, 21st IFAC World Congress, Germany, July 12-17, 2020

Active / Passive / Hybrid Information



IH1. Active Information Hiding

Modbus Master (participant hidden communication) ↔ cover channel / hidden channel ↔ Modbus Slave (participant hidden communication)

IH2. Passive Information Hiding

Modbus Master ↔ cover channel / hidden channel ↔ Modbus Slave

Network element (participant hidden communication)

Network element (participant hidden communication)

IH3. Semi-Active Information Hiding

Modbus Master (participant hidden communication) ↔ cover channel / hidden channel ↔ Modbus Slave

Network element (participant hidden communication)

IH4. Semi-Passive Information Hiding

Modbus Master ↔ cover channel / hidden channel ↔ Modbus Slave (participant hidden communication)

Network element (participant hidden communication)

Our extension and application to Modbus/TCP of the active/passive information hiding differentiation as published by Dittmann et al. [DHH05].

[DHH05] J. Dittmann, D. Hesse, R. Hillert, Steganography and steganalysis in voice-over ip scenarios: operational aspects and first experiences with a new steganalysis tool set. In Security, Steganography, and Watermarking of Multimedia Contents VII, volume 5681, 607–618. International Society for Optics and Photonics.

Plausibility and Compliance

- Plausability of a Covert Channel:
  - Condition 1: Protocol-Compliance
    - orginal recipient receives, accepts and processes the modified packet or flow (protocol is not broken)
  - Condition 2: Warden Compliance
    - Three levels of compliance:
      - (L1) warden has no knowledge or suspicion of the existance
      - (L2) warden suspects a hidden message but can not access it
      - (L3) warden can identify and access hidden message, but can not reconstruct the plain text

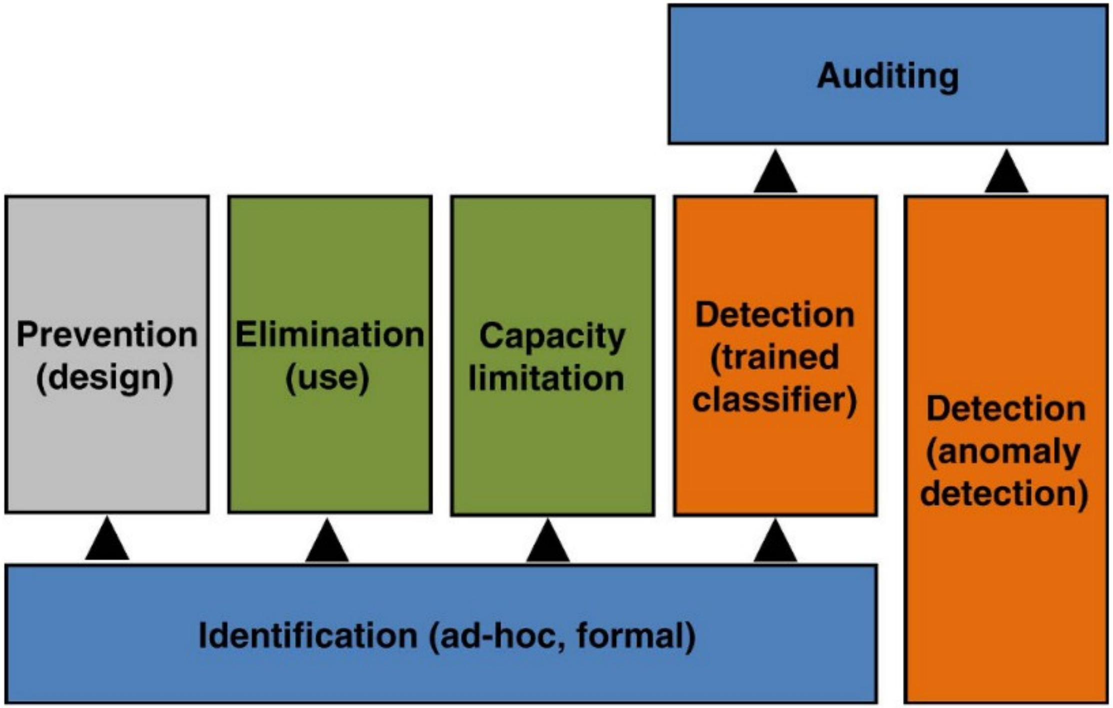
Active/ Passive Warden

- Passive Warden: Just observing and auditing the channel.

  - Goal 1: Detect the presence of the channel.
  - Goal 2: Understand how the channel works.
  - Goal 3: Read the communication content

- Active Warden: Interrupting the covert communication
  - Suppression
  - Removal

Countermeasure Overview

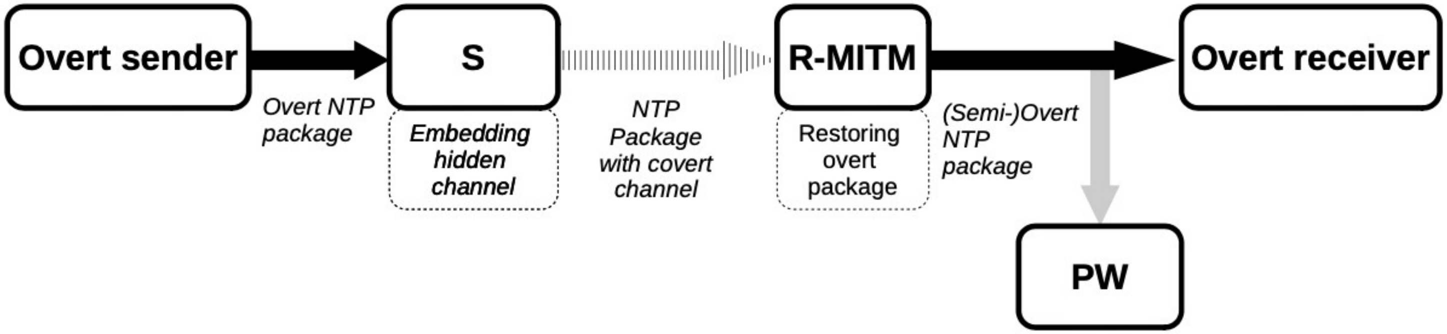

Auditing
Prevention (design)
Elimination (use)
Capacity limitation
Detection (trained classifier)
Detection (anomaly detection)
Identification (ad-hoc, formal)

Different types of countermeasures, described by [1]

[1] *Wojciech Mazurczyk, Steffen Wendzel, Sebastian Zander, Amir Houmansadr, andKrzysztof Szczypiorski. Background Concepts, Definitions, and Classification inInformation Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures, John Wiley & Sons, Ltd,2016.*

Reversible Channels

- Idea: Remove the covert channel (restore the overt network traffic), before it reaches a warden.



A Sender (S) is embedding a hidden information into over traffic. A receiver (R-MITM) first reads the covert information, and then restores the overt traffic, before the a warden (PW) and the Overt Receiver receive the traffic. Example based on [1] and NTP.

[1] Jonas Hielscher. In search of lost time: Covert Channels and Security Layer Bypass with the Network Time Protocol. Master Thesis. 2020. Otto-von-Guericke-University Magdeburg.

Further Literature