Steganography Ante Portas –
Key Aspects in A Nutshell

Steffen Wendzel

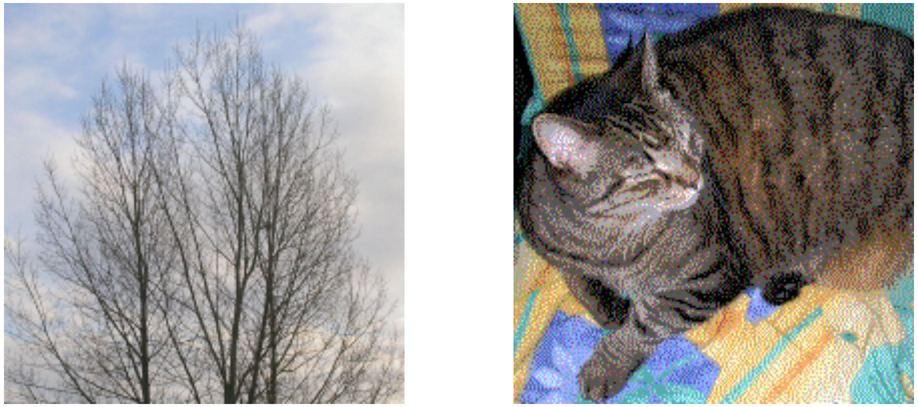
http://www.wendzel.de

Hack-in-the-Box

Amsterdam, Apr-12-2018

Information Hiding

What is „Information Hiding“? Two different examples:



All figures taken from Wikipedia articles on ‘Steganography‘ and ‘Watermarking‘

Steganography (digital):

hiding $something in $something_else

Steganography (digital):

hiding code in $something_else
images
text
music
videos
raw data
…

Steganography (digital):

hiding

- code
- images
- text
- music
- videos
- raw data
- …

in

- HTML
- text
- Javascript
- audio files
- network flows
- executables
- filesystem metadata
- blockchains
- cyber-physical systems

Steganography (digital):

hiding

code
images
text
music
videos
raw data
…

in

HTML
text
Javascript
audio files
network flows
executables
filesystem metadata
blockchains
cyber-physical systems

Basic Mimicry System

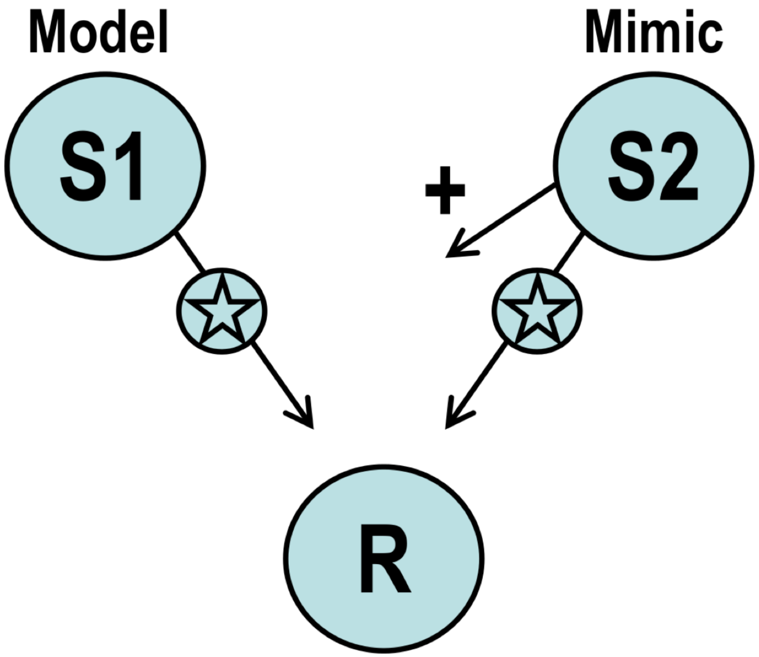


Fig. Basic mimicry system (Vane-Wright, 1976); graphic from (Mazurczyk et al., 2016)

History of Information Hiding

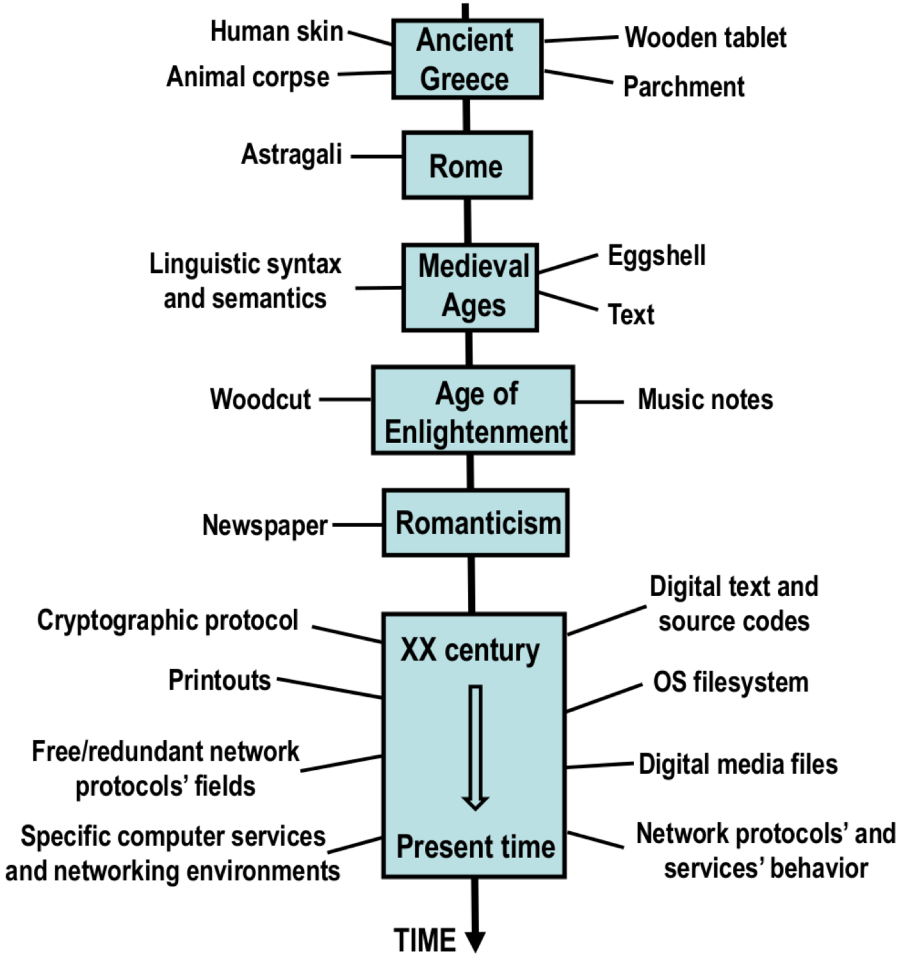


Fig. Information Hiding Methods During Time (Mazurczyk et al., 2016)

History of Information Hiding

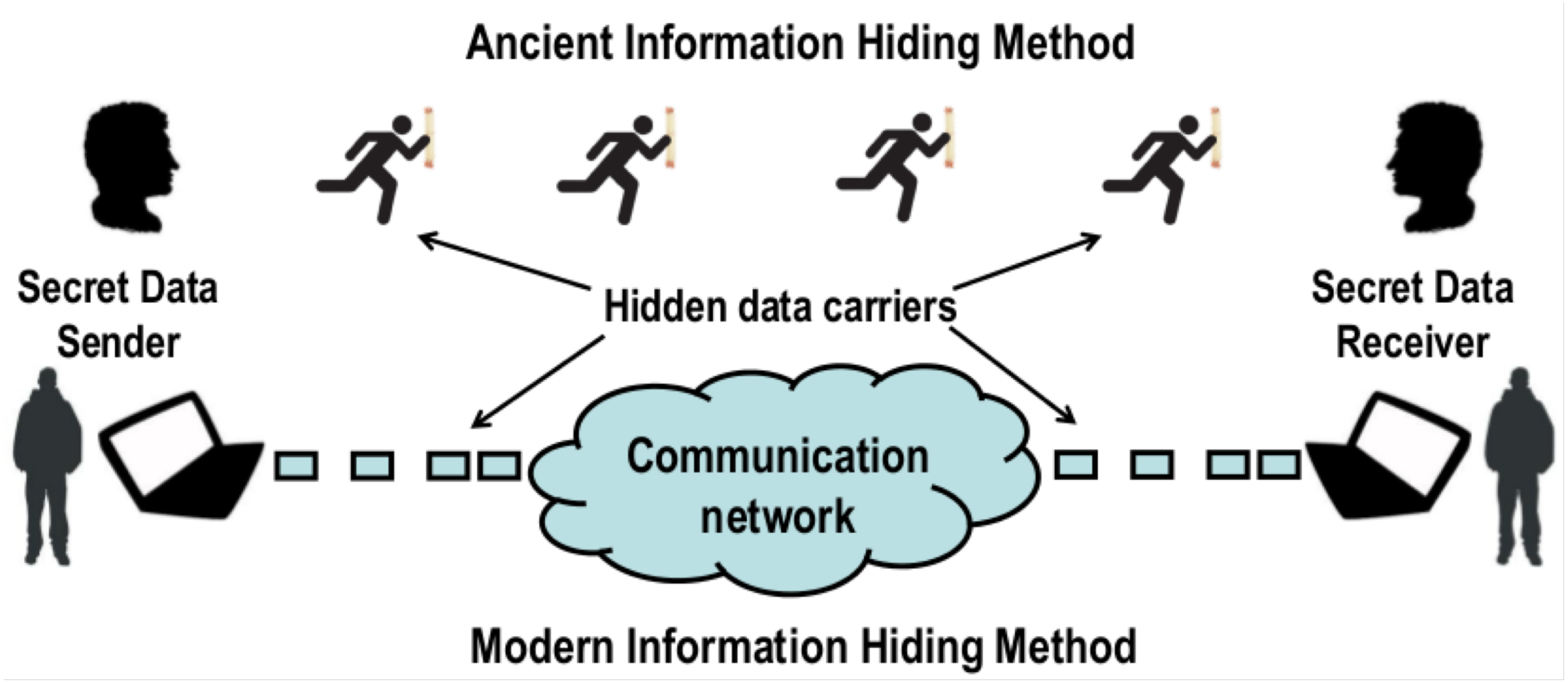


Fig. Difference between Ancient and Modern IH Methods (Mazurczyk et al., 2016)

Basic Taxonomy

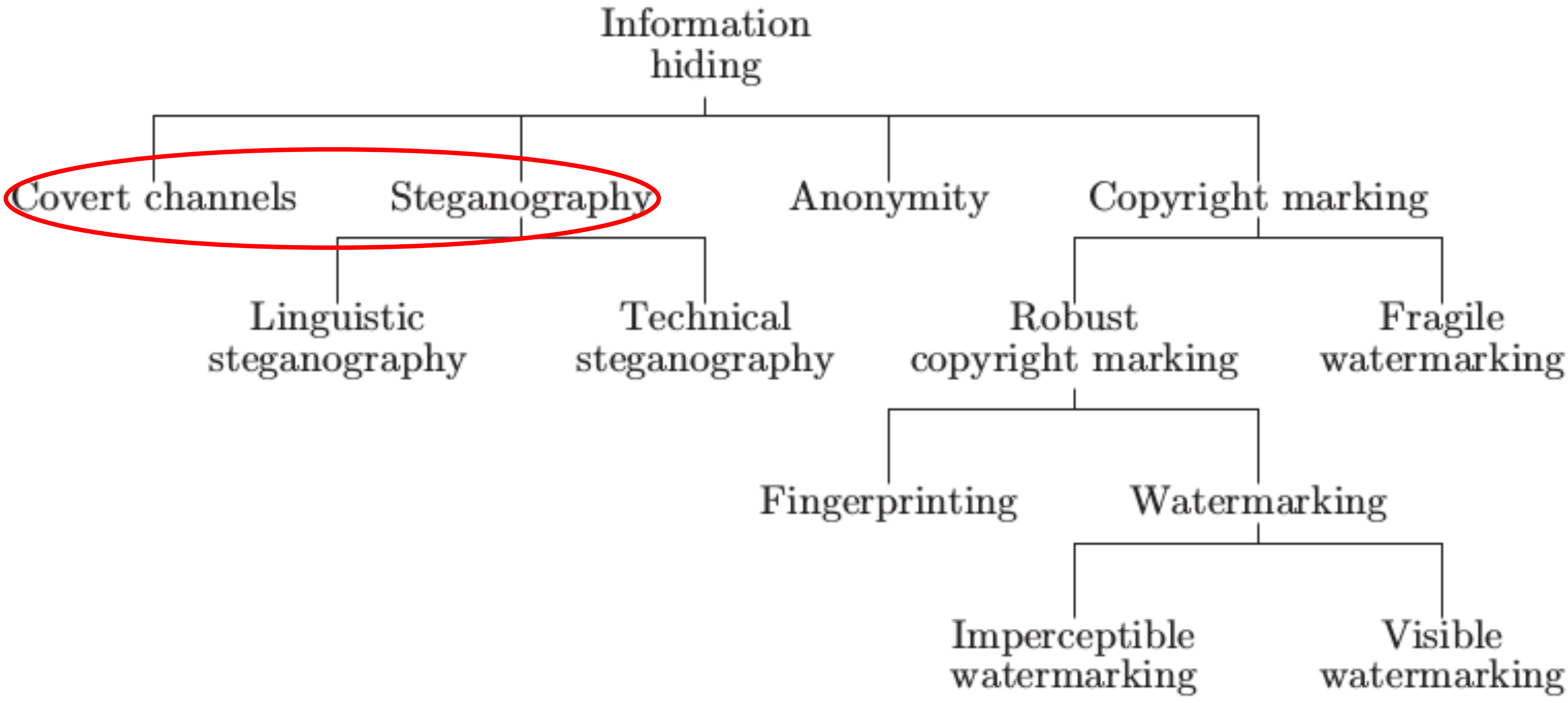
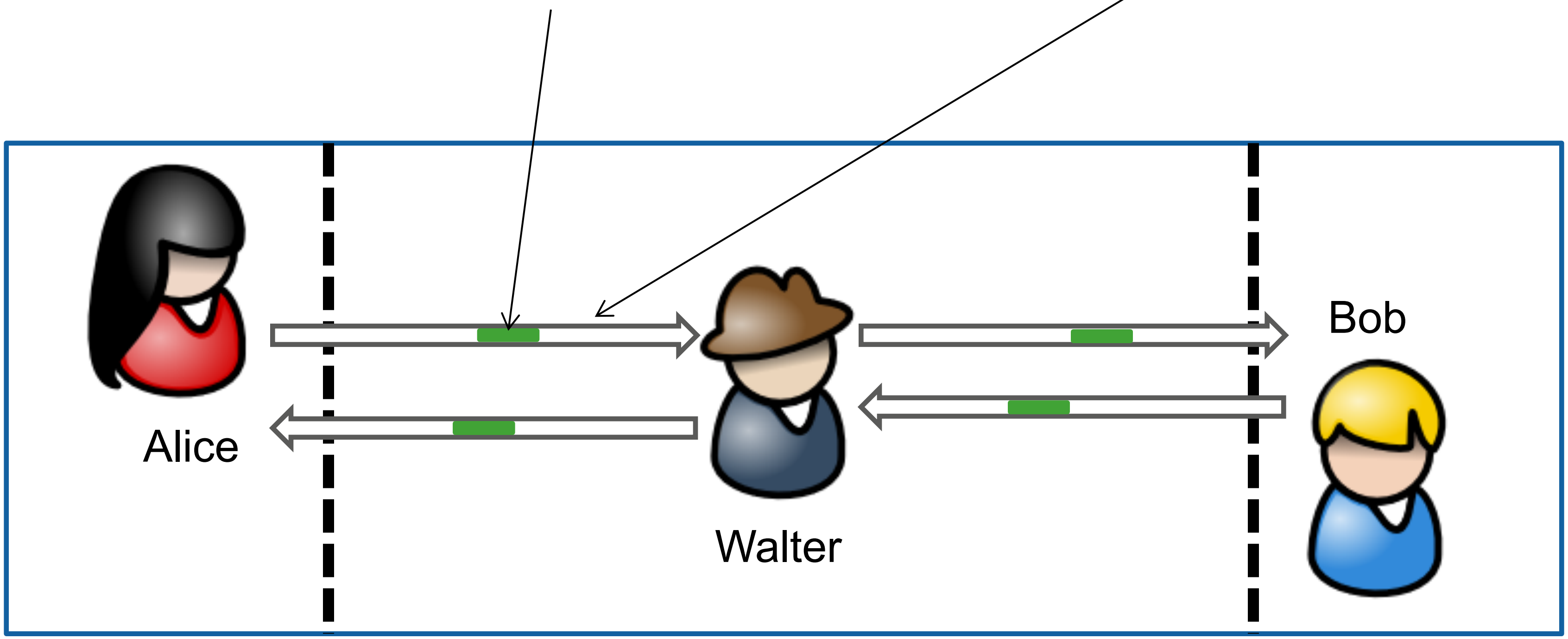


Fig. Classification of Information Hiding Techniques (Petitcolas et al., 1999)

Terminology

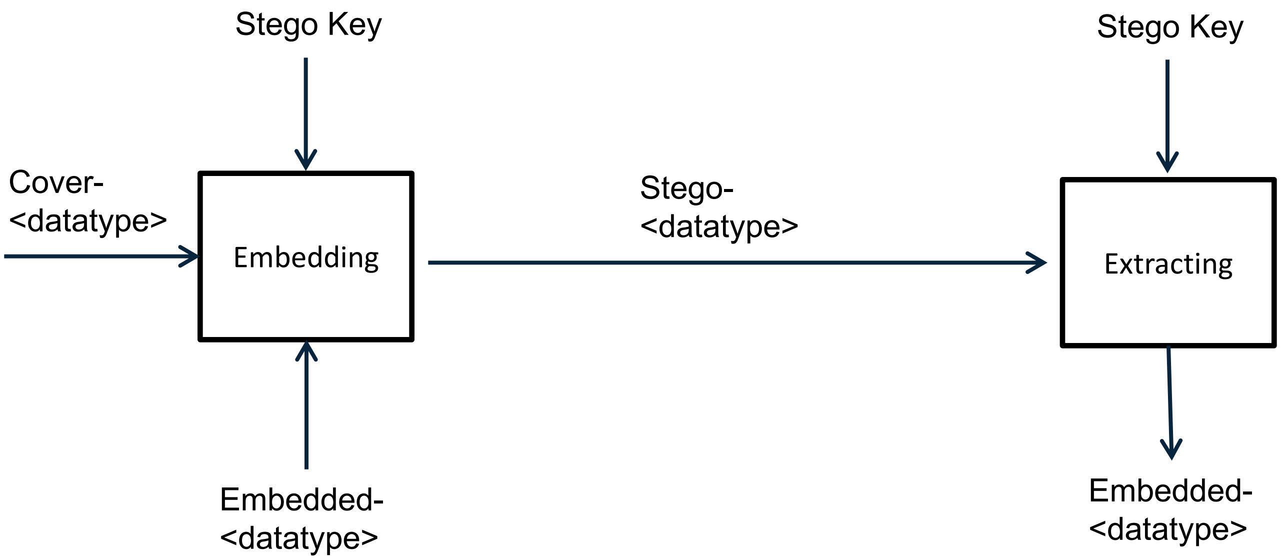
- Covert Channel (Lampson, 1973): *“…not intended for information transfer at all”*
  - A covert channel without intention is a **side channel**
  - DoD defined it differently: CCs break a security policy (usually in MLS) (DoD, 1985).

- Steganography (Fridrich, 2010):
  - “Steganography can be informally defined as the practice of undetectably communicating a **message** **(a.k.a. steganogram)** in a **cover object**.“



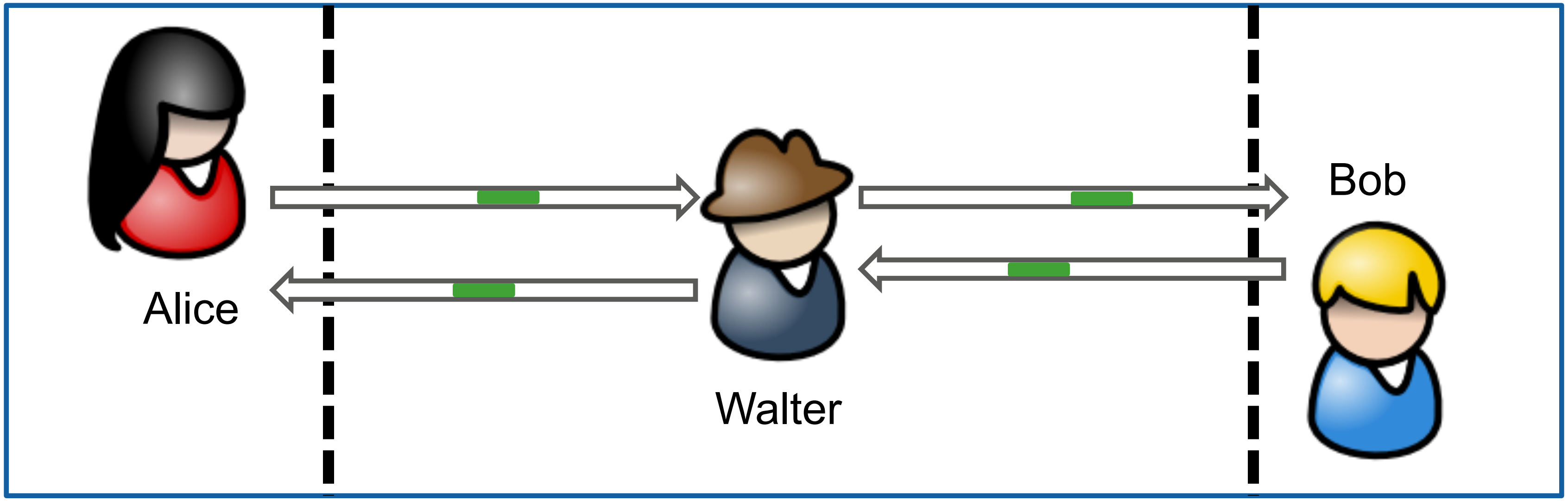
Terminology

- Steganography (Fridrich, 2010):
  - “Steganography can be informally defined as the practice of undetectably communicating a **message** **(a.k.a. steganogram)** in a **cover object**.“
- Terminology based on (Pfitzmann, 1996):



Definition

- Walter is referred to as a **warden**. He performs a so-called **steganalysis**.
- A warden can be
  - Passive
    - tries to detect the presence (and content) of a hidden message in a cover object and tries to determine who is involved in the steganographic communication
  - Active
    - Modifies the cover object (e.g. removes or replaces steganogram)
  - Malicious
    - Can introduce own messages to fool involved participants (e.g. message spoofing)



Is it applied in practice?

Yes, especially for hiding C&C communications, e.g. Fakem RAT / Carbanak / Anunak.

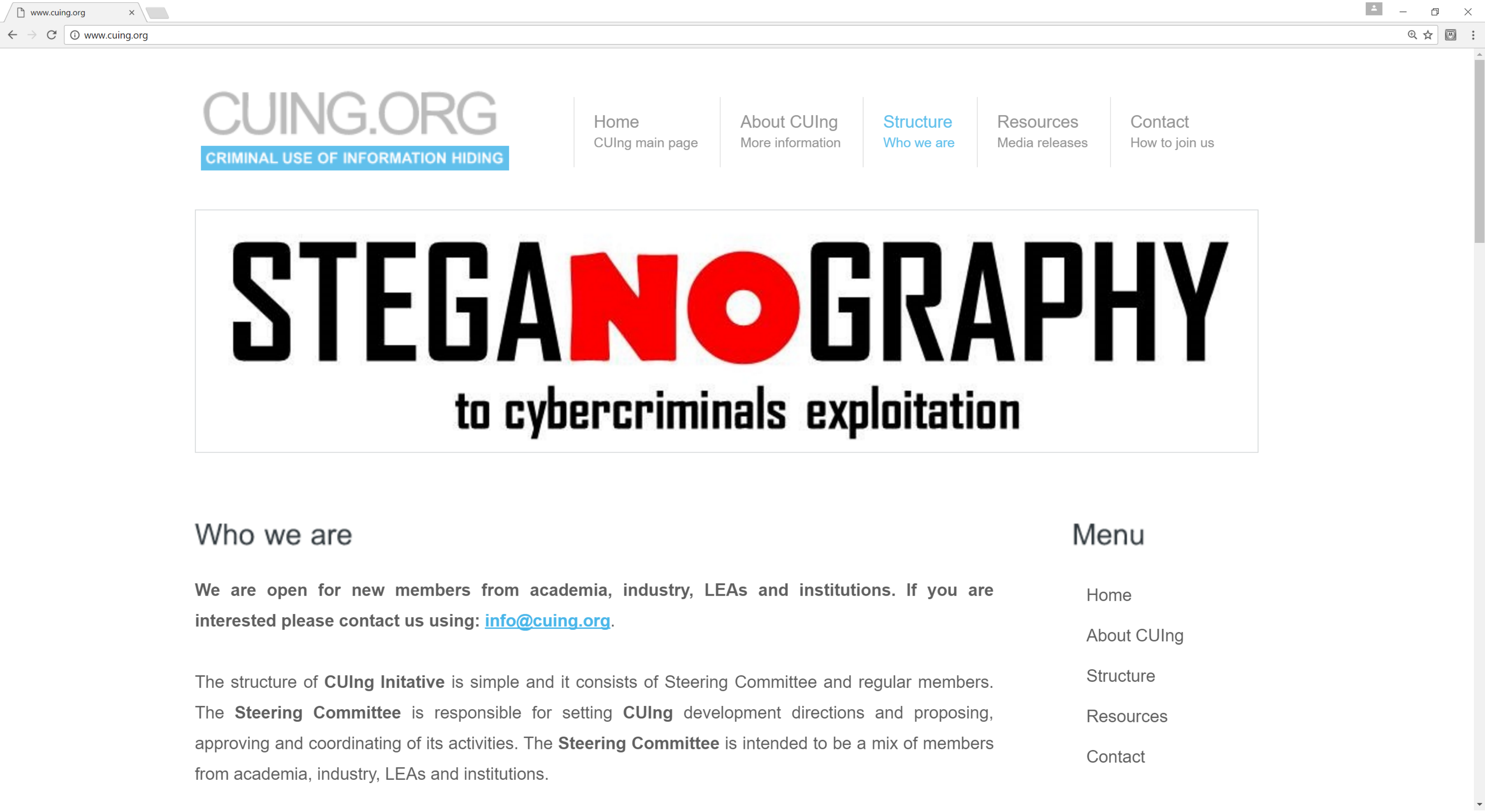
Letting malware traffic appear as MSN or Yahoo! Messenger traffic, hiding traffic in SSH connections.

Hiding data in Javascript, HTML, text, digital images or – recently – blockchain.

Want to know more?

Summary#1 / Summary#2

Is it applied in practice?



Who we are

We are open for new members from academia, industry, LEAs and institutions. If you are interested please contact us using: info@cuing.org.

The structure of **CUIng Initative** is simple and it consists of Steering Committee and regular members. The **Steering Committee** is responsible for setting **CUIng** development directions and proposing, approving and coordinating of its activities. The **Steering Committee** is intended to be a mix of members from academia, industry, LEAs and institutions.

Some potential scenarios

- Advanced Persistent Threats (APT): large-scale sophisticated data leakage, applying techniques such as `spear phishing’
- Criminals: sharing of illegal information or material, such as child porn. [For the latter, there are – unfortunately – multiple known cases of stego application!]
- Malware: e.g. stealthy botnet C&C channels
- Military/secret service: Industrial espionage, stealthy communication
- Citizens: censorship circumvention
- Journalists: freedom of speech -> expression of opinions in networks with censorship

NETWORK INFORMATION HIDING

Definition

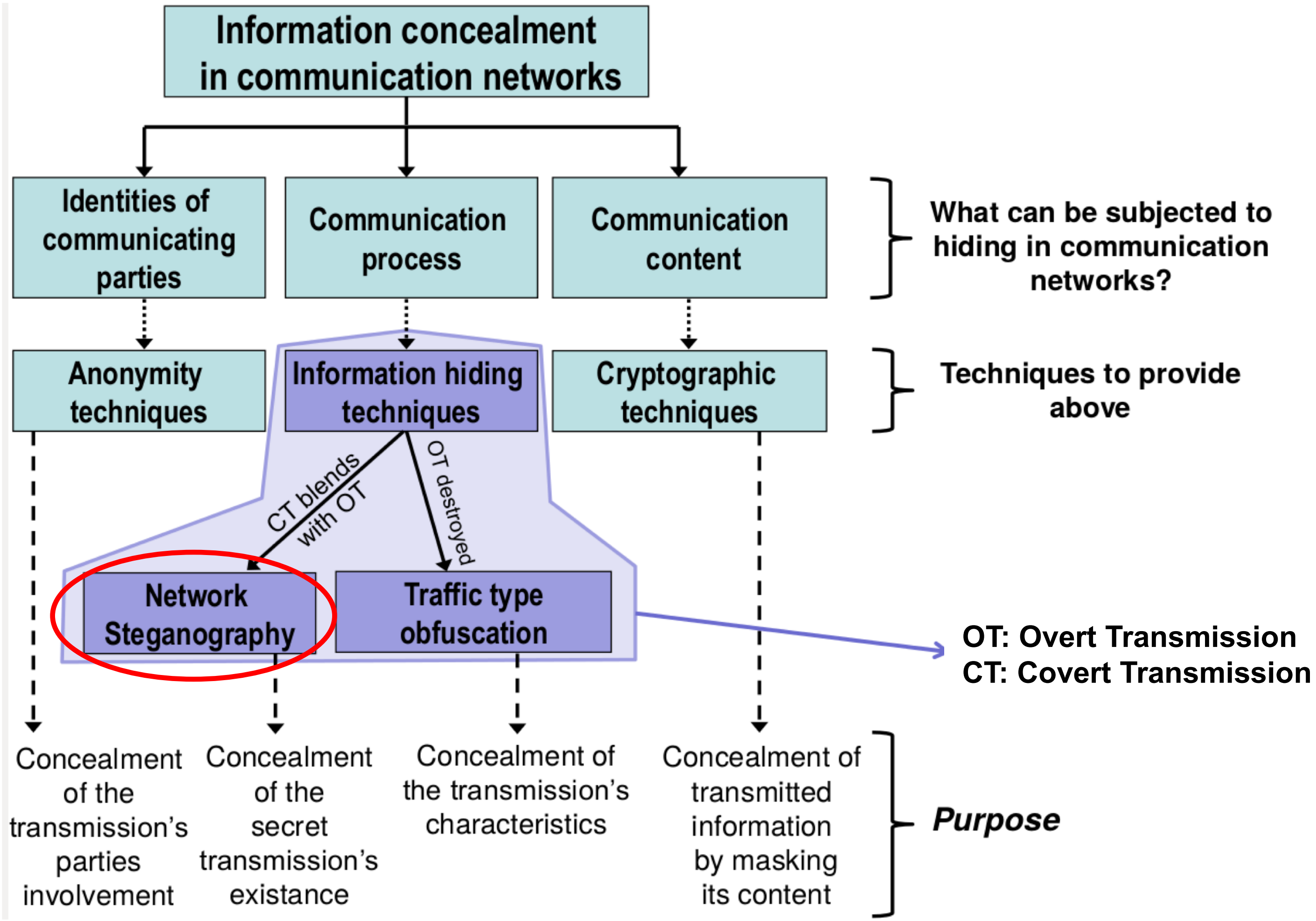

Information concealment in communication networks
Identities of communicating parties
Communication process
Communication content
What can be subjected to hiding in communication networks?
Anonymity techniques
Information hiding techniques
Cryptographic techniques
Techniques to provide above
CT blends with OT
OT destroyed
Network Steganography
Traffic type obfuscation
OT: Overt Transmission
CT: Covert Transmission
Concealment of the transmission's parties involvement
Concealment of the secret transmission's existance
Concealment of the transmission's characteristics
Concealment of transmitted information by masking its content
Purpose

Fig. Classification of Information Hiding Techniques (Mazurczyk et al., 2016)

HIDING PATTERNS

Why Patterns?

- One can either study a few hundred hiding techniques for network covert channels … or simply their general ideas.
  - Because of massive redundancy and similarities in known hiding techniques.

- **We analyzed tons of hiding methods published since 1987.**

Result: a few patterns can describe them all!

Patterns in Network Information Hiding

Patterns were set in relation to other patterns to introduce a **new taxonomy** of patterns. The 109 hiding techniques could be described by only 11 patterns.

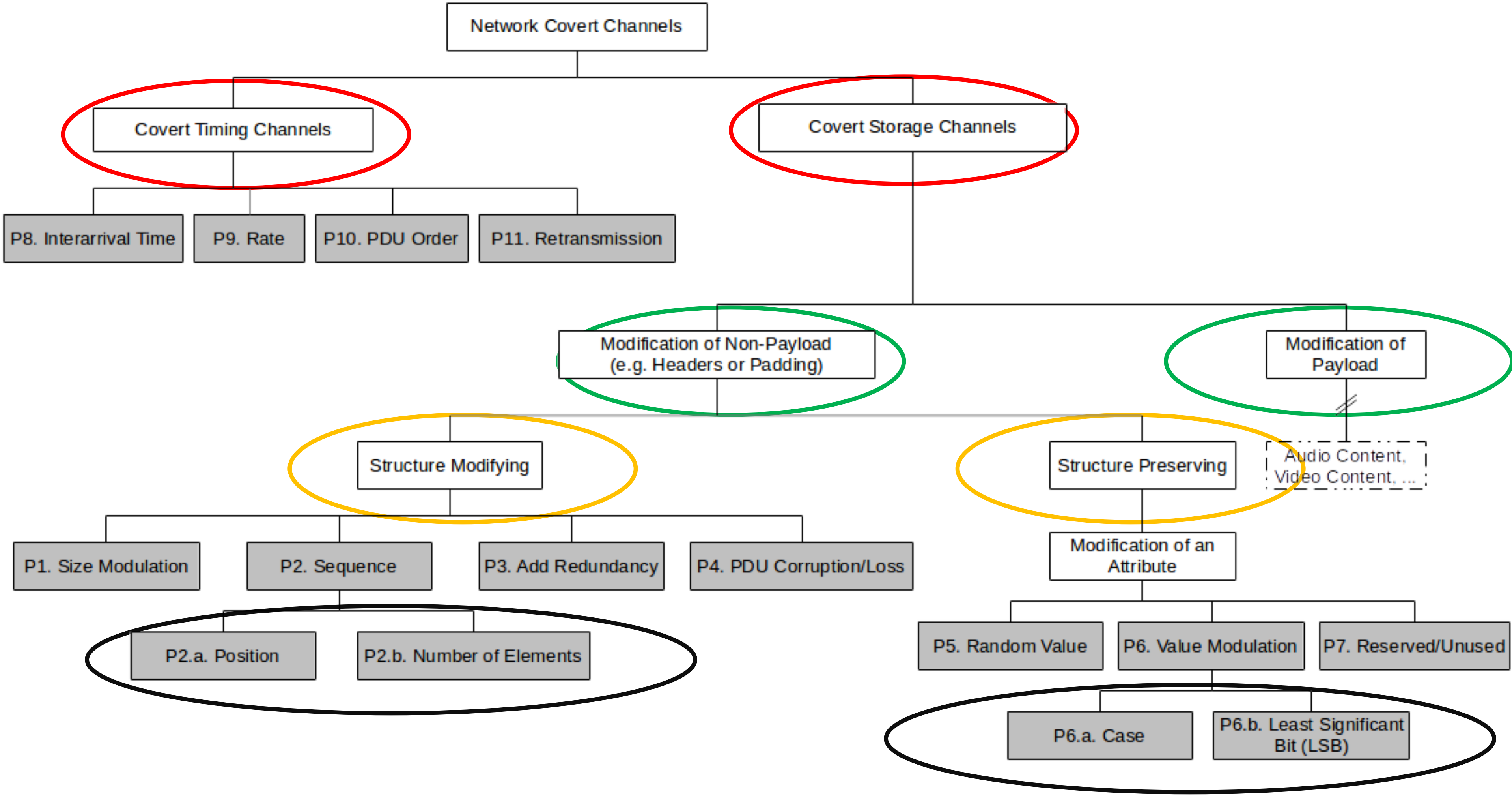


Image source: (Wendzel et al., 2015)

P1. Size Modulation Pattern

- The overt channel uses the size of a header element or of a PDU* to encode the hidden message.

- Examples:
  - Modulation of data block length in LAN frames
  - Modulation of IP fragment sizes

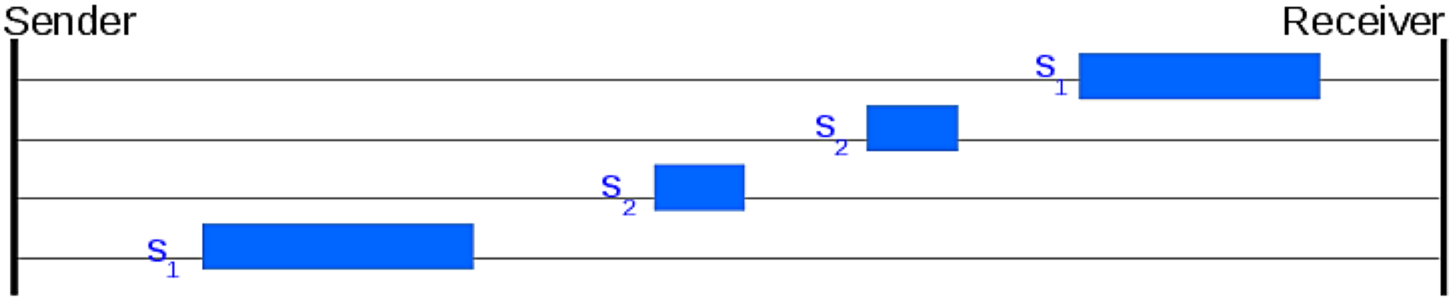


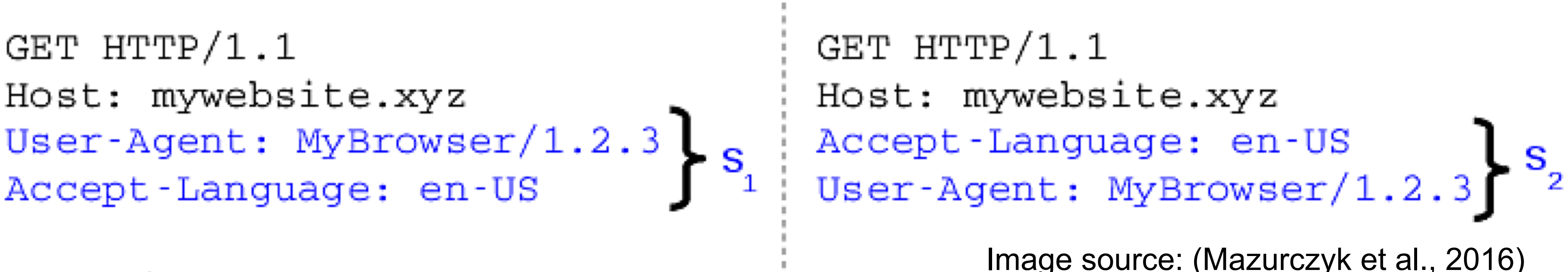
Image source: (Mazurczyk et al., 2016)

**protocol data unit*

P2. Sequence Pattern

- The covert channel alters the sequence of header/PDU elements to encode hidden information.

- Examples:
  - Sequence of DHCP options
  - Sequence of FTP commands
  - Sequence of HTTP header fields



```
GET HTTP/1.1
Host: mywebsite.xyz
User-Agent: MyBrowser/1.2.3
Accept-Language: en-US
```

```
GET HTTP/1.1
Host: mywebsite.xyz
Accept-Language: en-US
User-Agent: MyBrowser/1.2.3
```

Image source: (Mazurczyk et al., 2016)

- Sub-patterns:
  - P2.a. Position Pattern (e.g. pos. of IPv4 option *x* in list of options)
  - P2.b. Number of Elements Pattern (e.g. # of IPv4 options)

P3. Add Redundancy Pattern

- The covert channel creates new space within a given header element or within a PDU to hide data in it.

- Examples:
  - Extend HTTP headers with additional fields or extend values of existing fields
  - Create a new IPv6 destination option with embedded hidden data
  - Manipulate \`pointer‘ and \`length‘ values for IPv4 record route option to create space for data hiding

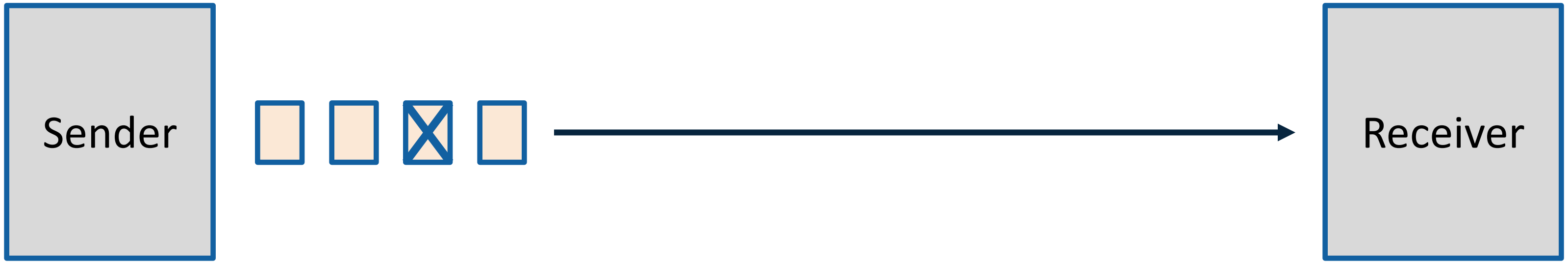
```
GET / HTTP/1.0          GET / HTTP/1.0
                        User-Agent: Mozilla/4.0
```

P4. PDU Corruption

- The covert channel generates corrupted PDUs that contain hidden data or actively utilizes packet loss to signal hidden information.

- Examples:
  - Transfer corrupted frames in IEEE 802.11
  - MitM drops selected packets exchanged between two VPN sites to introduce covert information.

E.g., sending a number of packets in which corrupted packets indicate hidden data:



P5. Random Values

- The covert channel embeds hidden data in a header element containing a (pseudo) random value.

- Examples:
  - Utilize IPv4 identifier field
  - Utilize the first ISN of a TCP connection (cf. previous lecture on IH)
  - Utilize DHCP *xid* field

P6. Value Modulation Pattern

- The covert channel selects one of *n* values a header element can contain to encode a hidden message.

- Examples:
  - Send a frame to one of *n* available Ethernet addresses in a LAN
  - Encode information by the possible Time-to-live (TTL) values in IPv4 or in the Hop Limit values in IPv6
  - Select one of *n* possible BACnet message types

```
USeR-AGEnT: MyBrowser/1.2.3          User-AGENT: MyBrowser/1.2.3
0010 00010                           0111 00000
```

P7. Reserved/Unused Pattern

- The covert channel encodes hidden data into a reserved or unused header/PDU element.

- Examples:
  - Utilize undefined/reserved bits in IEEE 802.5/data link layer frames
  - Utilize (currently) unused fields in IPv4, e.g. Identifier field, Don‘t Fragment (DF) flag or reserved flag or utilize unused fields in IP-IP encapsulation
  - Utilize the padding field of IEEE 802.3

P8. Inter-arrival Time Pattern

- The covert channel alters timing intervals between network PDUs (inter-arrival times) to encode hidden data.

- Examples:
  - Alter timings between LAN frames
  - Alter the response time of a HTTP server

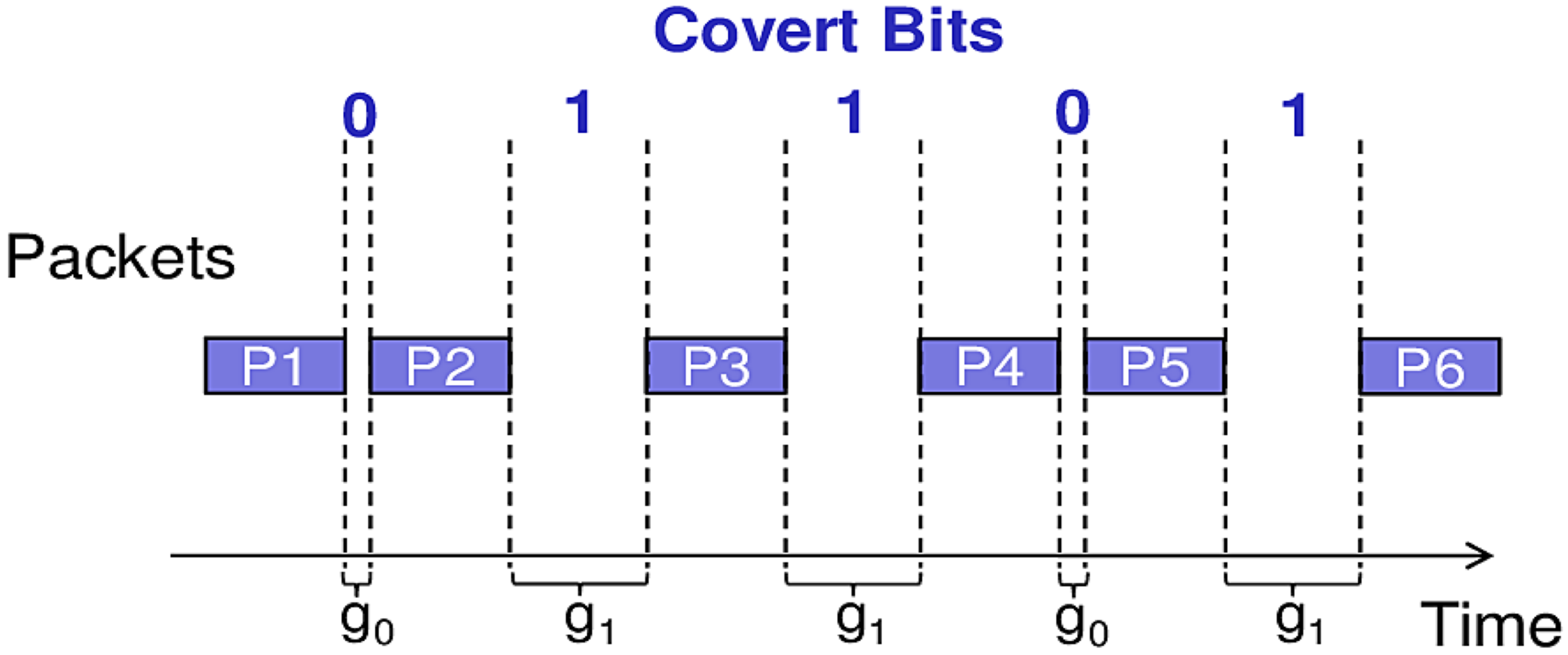


Image source: (Mazurczyk et al., 2016)

P9. Rate Pattern

- The covert channel sender alters the data rate of a traffic flow from itself or a third party to the covert channel receiver.

- Examples:
  - Exhaust the performance of a switch to affect the throughput of a connection from a third party to a covert channel receiver over time.
  - Directly alter the data rate of a legitimate channel between a covert channel sender and receiver.

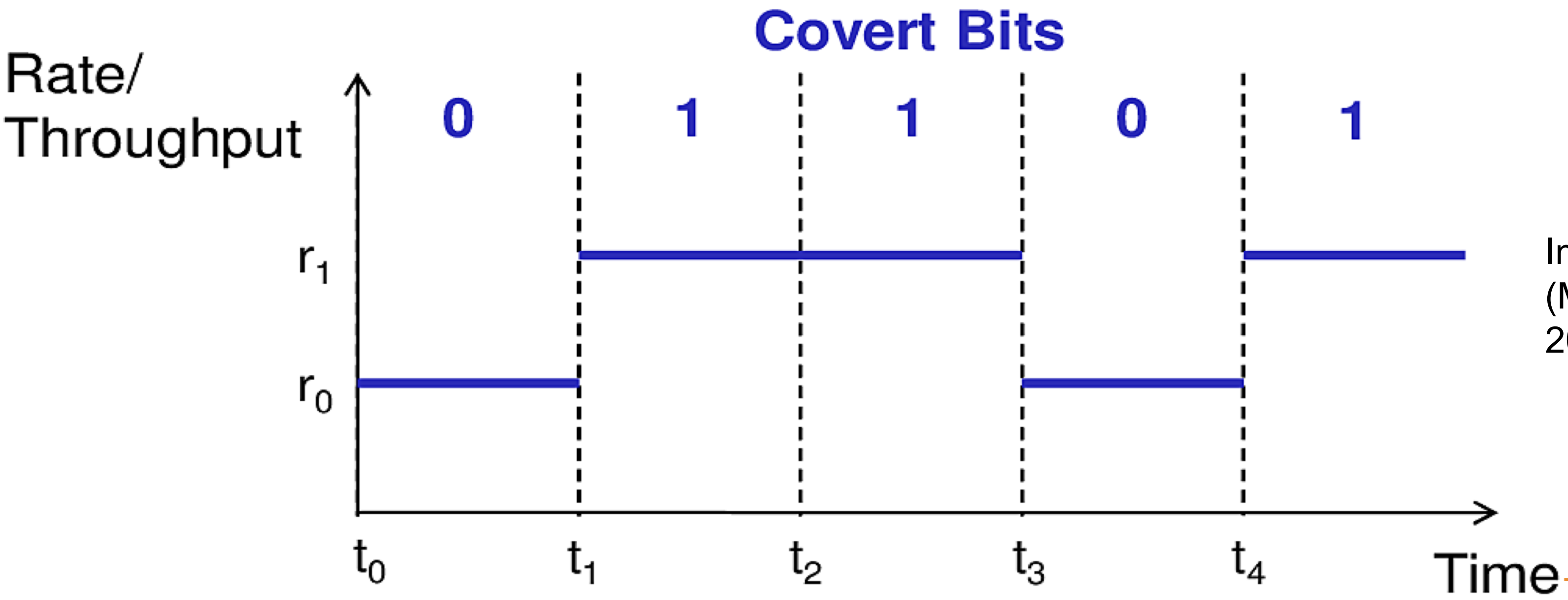


Image source: (Mazurczyk et al., 2016)

P10. PDU Order Pattern

- The covert channel encodes data using a synthetic PDU order for a given number of PDUs flowing between covert sender and receiver.

- Examples:
  - Modify the order of IPSec Authentication Header (AH) packets
  - Modify the order of TCP segments

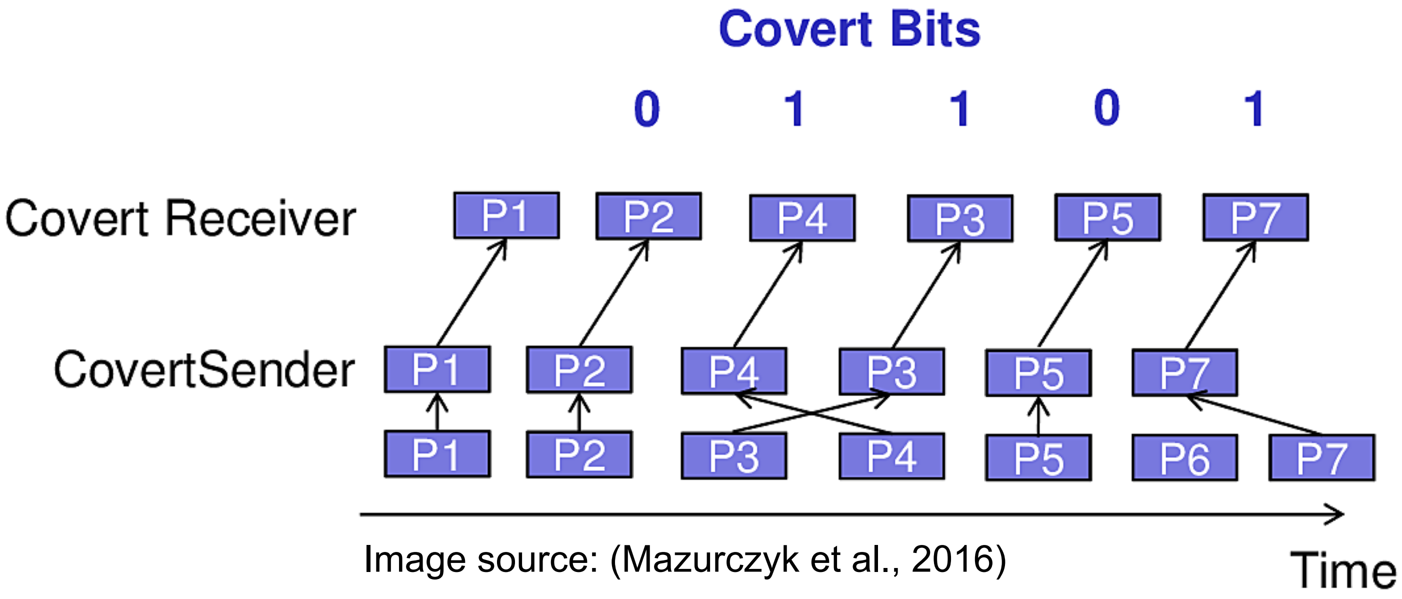
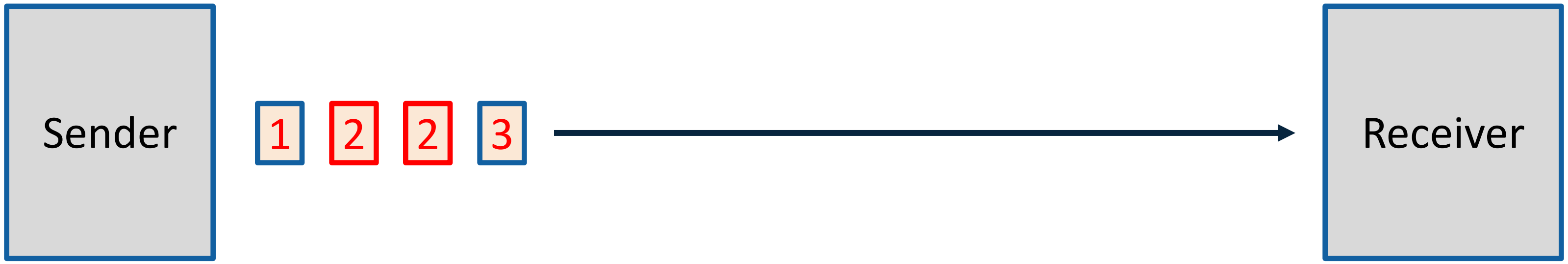


Image source: (Mazurczyk et al., 2016)

P11. Re-Transmission Pattern

- A covert channel re-transmits previously sent or received PDUs.
- Examples:
  - Transfer selected DNS requests once/twice to encode a hidden bit per request.
  - Duplicate selected IEEE 802.11 packets
  - Do not acknowledge received packets to force the sender to re-transmit a packet.



Published Hiding Techniques per Pattern

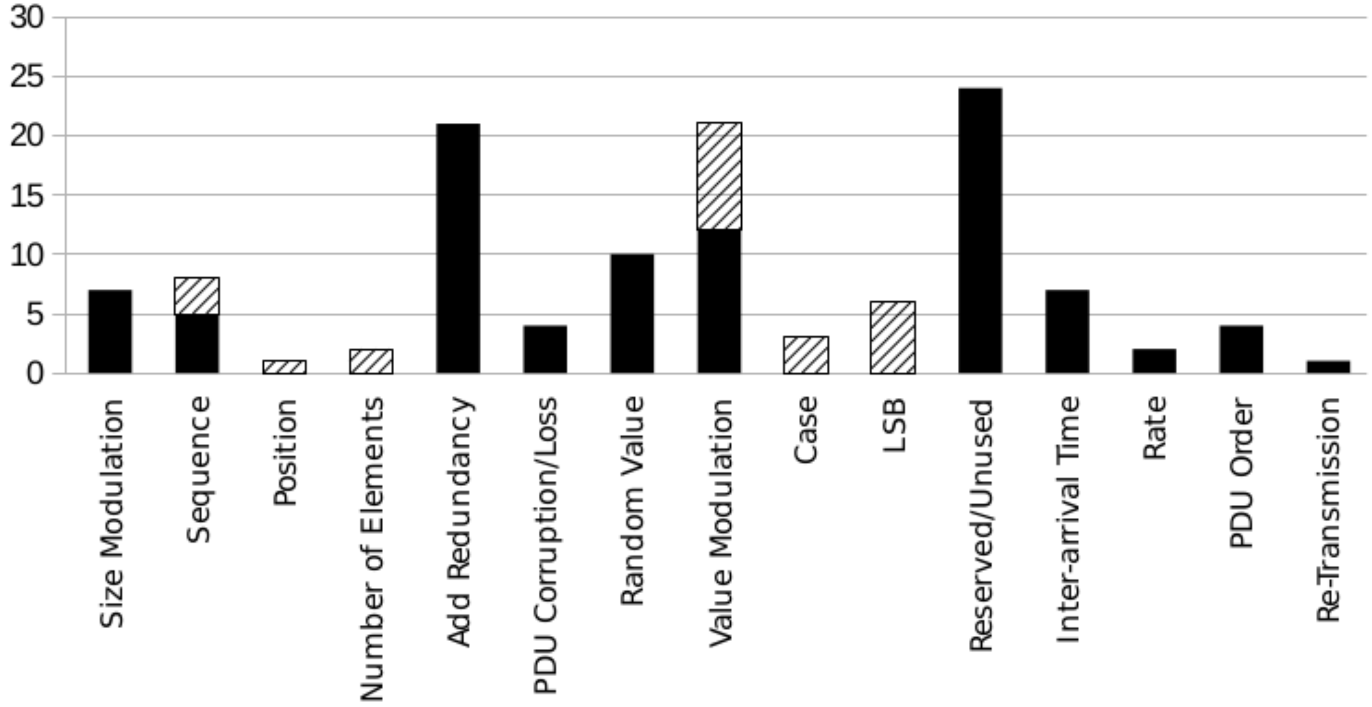


Fig. 3. Number of associated covert channel techniques per covert channel pattern. Shaded bars represent child patterns.

Image source: (Wendzel et al., 2015)

CHALLENGE #1

Challenge #1

FIND A NEW HIDING PATTERN, NOT A NEW HIDING TECHNIQUE.

Yes, but what if I found one?

Describe your new pattern in a way that everybody understands …
… a way that let‘s everybody compare it to existing work
… and increases the chance of acceptance.

We already worked this out for you – you can use it:

Unified Description Method

However, if found you a new hiding TECHNIQUE, simply use the same description method.

SOPHISTICATED HIDING TECHNIQUES

Micro Protocols & Fun With Patterns

- **Covert Channel-internal Control Protocols**
  - Error detection/correction; building up dynamic overlay networks with dynamic routing, bypassing filters, determining countermeasures, upgrading CC software

- **Pattern Combination**
  - Instead of utilizing one Hiding Pattern, one can use multiple … combined in the same transfer
    - for instance: Reserved/Unused and Inter-arrival Time
    - If one covert flow is detected, the other flows still remain undetected

- **Pattern Hopping**
  - (Randomly) select a new Hiding Pattern for every new packet to be sent.

CHALLENGE #2

Challenge #2

IMPROVE EXISTING COUNTERMEASURES, ESPECIALLY FOR STEGO DETECTION & ELIMINATION.

STEGANOGRAPHY IN THE IOT

Why + How?

- Why?

  > secretly storing data in cyber-physical systems

  > bypassing filter technologies of the major network

- How?

  > unused registers

  > modification of actuator values

  > network covert channels

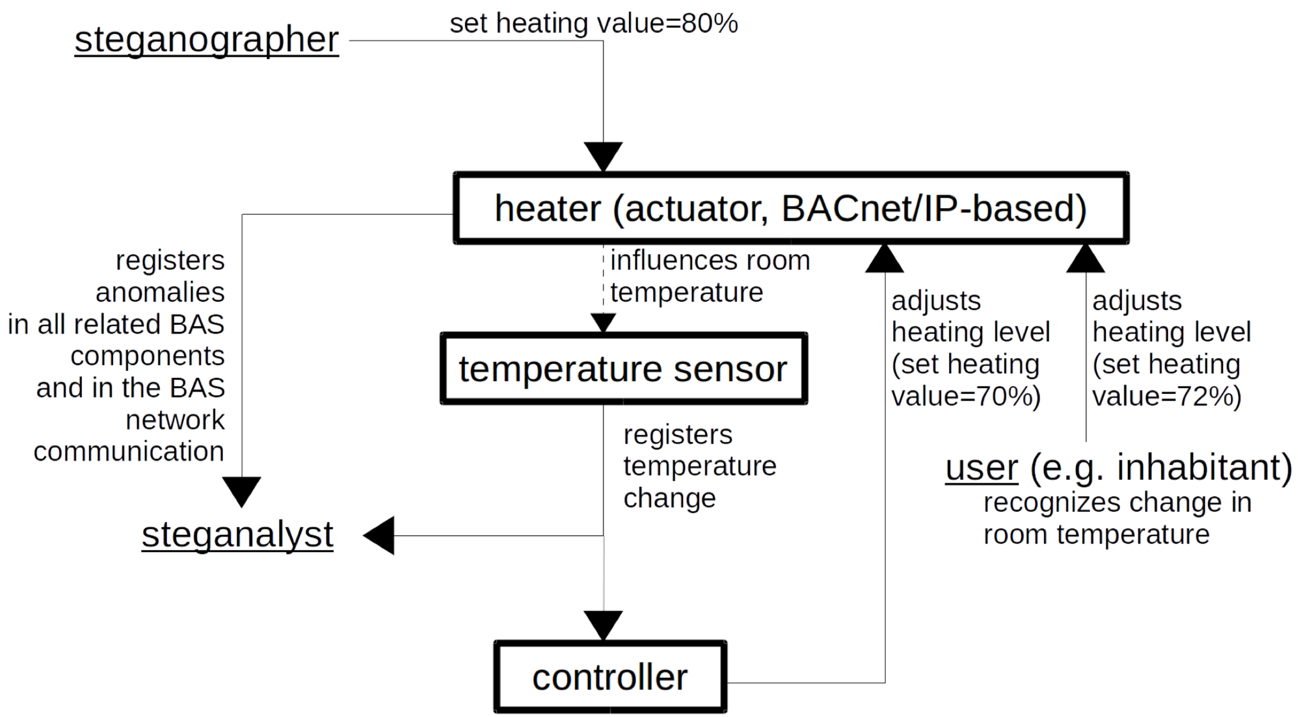

steganographer
set heating value=80%
heater (actuator, BACnet/IP-based)
registers anomalies in all related BAS components and in the BAS network communication
influences room temperature
adjusts heating level (set heating value=70%)
adjusts heating level (set heating value=72%)
temperature sensor
registers temperature change
user (e.g. inhabitant)
recognizes change in room temperature
steganalyst
controller

Image source: (Wendzel et al., 2017)

Results?

- *350* bits - *1.7* Kbytes of secret data can be stored in a medium-sized building automation system.
- Requires approx. 30 actuators only to store 128 bit AES key
- More work needed so that we can store more data in CPS.

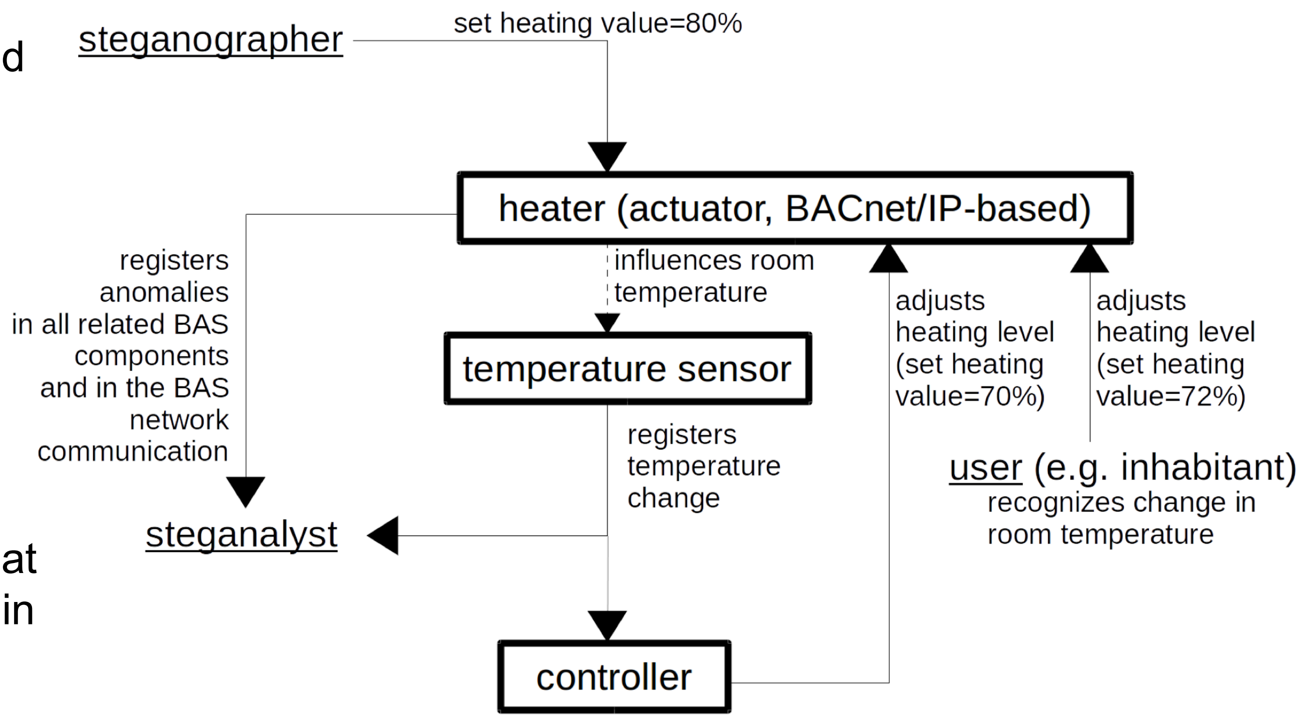

steganographer
set heating value=80%
heater (actuator, BACnet/IP-based)
registers anomalies in all related BAS components and in the BAS network communication
influences room temperature
adjusts heating level (set heating value=70%)
adjusts heating level (set heating value=72%)
temperature sensor
registers temperature change
user (e.g. inhabitant)
recognizes change in room temperature
steganalyst
controller

Image source: (Wendzel et al., 2017)

CHALLENGE #3

Challenge #3

STORE <u>MORE</u> DATA IN A CPS + TRY STEGO WITH NEW TYPES OF CPS, E.G. WEARABLES.

References

- Petitcolas, F.A.P., Anderson, R., Kuhn, M.G.: Information Hiding – A Survey, Proc. IEEE, 1999.
- Pfitzmann, B.: Information Hiding Terminology, Proc. 1st Information Hiding Workshop, Springer, 1996.
- Lampson, B.W.: A Note on the Confinement Problem, Comm. ACM, 1973.
- Petitcolas, F.A.P., Anderson, R., Kuhn, M.G.: Information Hiding – A Survey, Proc. IEEE, 1999.
- Mazurczyk, W., Wendzel, S., Zander, S. et al.: Information Hiding in Communication Networks, Wiley / IEEE Comp. Soc. Press, 2016.
- Wendzel, S. and Keller, J.: Low-attention forwarding for mobile network covert channels. In Proc. 12th Conference on Communications and Multimedia Security (CMS 2011), volume 7025 of LNCS, pages 122–133. Springer, Gent, BE, October 2011.
- Wendzel, S., Keller, J.: A survey on covert channel-internal control protocols, Annals of Telecommunications, Springer, 2014.
- Wendzel, S., Zander, S., Fechner, B., Herdin, C.: Pattern-based Survey and Categorization of Network Covert Channel Techniques, Computing Surveys, No. 47(3), pp. 50:1-26, ACM, 2015.
- Fridrich, J.: Steganography in Digital Media, Cambridge University Press, 2010.
- Mazurczyk, W., Wendzel, S.: Information Hiding: Challenges for Forensic Experts, Communications of the ACM, 2017.
- Vane-Wright, R. I.: A unified classification of mimetic resemblances, Biological Journal of the Linnean Society, 1976.
- Wendzel, S., Mazurczyk, W., Zander, S.: Unified Description for Network Information Hiding Methods, Journal of Universal Computer Science, 2016.
- Wendzel, S., Mazurczyk, W., Haas, G.: Information Hiding in Cyber-physical Systems, Journal of Cyber Security and Mobility (JCSM), 2017.

You can find all my publications for download here: http://steffen-wendzel.blogspot.de/p/publications.html

THANK YOU FOR YOUR ATTENTION.