

# NETWORK INFORMATION HIDING

## CH. 4: INTRODUCTION TO NETWORK INFORMATION HIDING

Prof. Dr. Steffen Wendzel

<https://www.wendzel.de>

## Definition

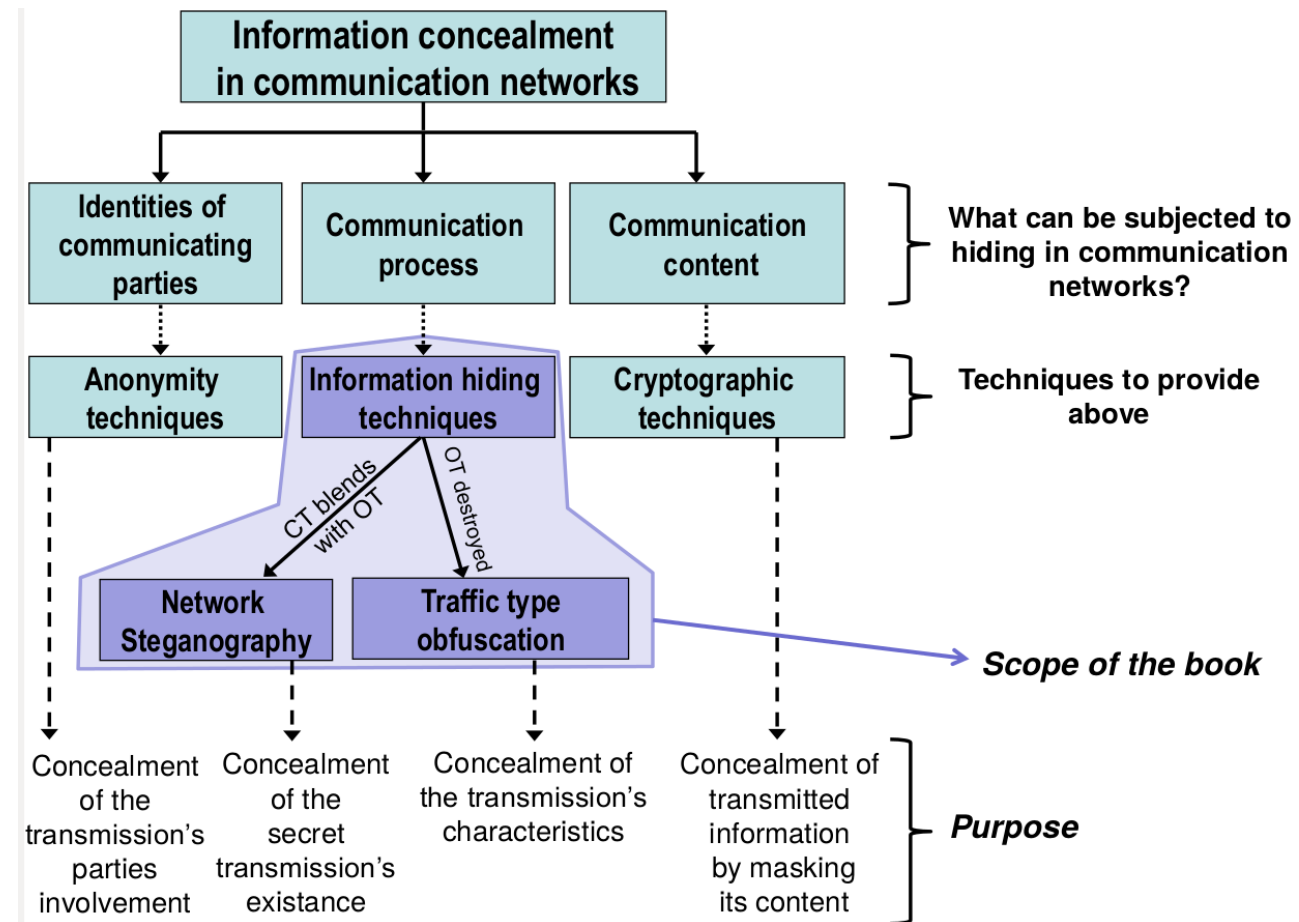


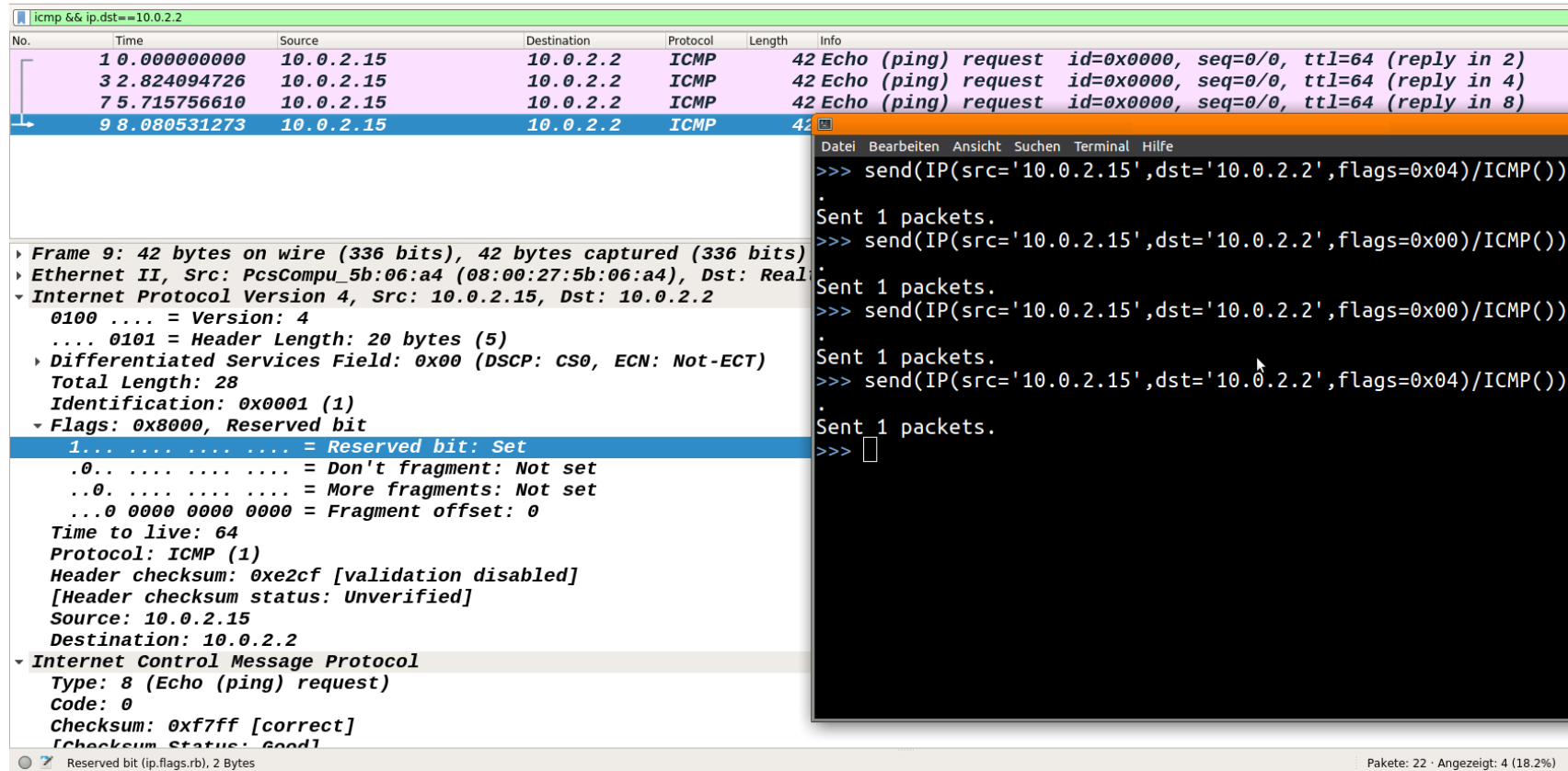
Fig.: W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016

## Differences to traditional digital media steganography

- **Inconsistent terminology:** no clear distinction between **steganography** and **covert channel**
  - See Ch. 1 for definitions of the terms steganography and covert channel and that both are considered as different research domains (covert channels in MLS context!).
  - Thus, in the network context: **network covert channel** or **network steganographic channel** handled separately
  - Unified: a steganographic **method** creates such a **covert channel** [1, Chapter 3]
- A bit more terminology:
  - Covert data is hidden in *overt* network transmissions
  - The „cover object“ is now called „carrier“ in the network context
  - Advantage of a constant transmission (e.g. permanent data leakage)
- Advantages:
  - Difficult to analyze **all** network data; smaller delay; with the growth of the Internet, the options for network IH grew and grow, too.

[1] W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016

## Example 1: Trivial Network Covert Channel via IPv4 Reserved Bit, sending message "1001"



The image shows a Wireshark packet capture and a terminal window. The Wireshark packet list shows four ICMP Echo (ping) requests from 10.0.2.15 to 10.0.2.2. The packet details for the first packet (No. 1) show the following fields:

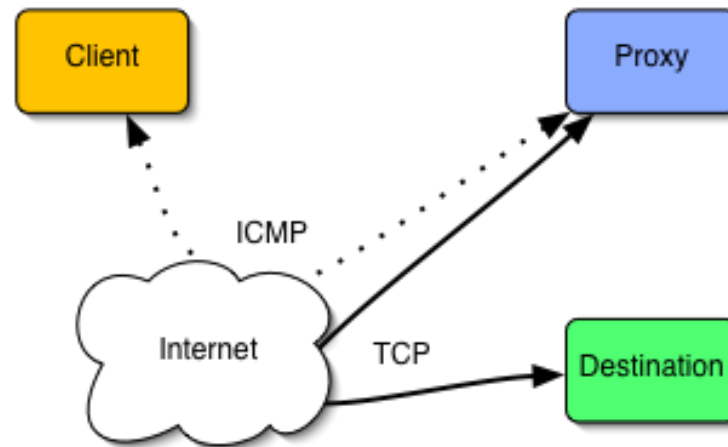
- Frame 9: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
- Ethernet II, Src: PcsCompu\_5b:06:a4 (08:00:27:5b:06:a4), Dst: Real
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.2
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 28
  - Identification: 0x0001 (1)
  - Flags: 0x8000, Reserved bit
  - 1... .... = Reserved bit: Set
  - .0.. .... = Don't fragment: Not set
  - ..0. .... = More fragments: Not set
  - ...0 0000 0000 0000 = Fragment offset: 0
  - Time to live: 64
  - Protocol: ICMP (1)
  - Header checksum: 0xe2cf [validation disabled]
  - [Header checksum status: Unverified]
  - Source: 10.0.2.15
  - Destination: 10.0.2.2
- Internet Control Message Protocol
  - Type: 8 (Echo (ping) request)
  - Code: 0
  - Checksum: 0xf7ff [correct]
  - [Checksum status: Good]

The terminal window shows the following commands and output:

```
>>> send(IP(src='10.0.2.15',dst='10.0.2.2',flags=0x04)/ICMP())
.
Sent 1 packets.
>>> send(IP(src='10.0.2.15',dst='10.0.2.2',flags=0x00)/ICMP())
.
Sent 1 packets.
>>> send(IP(src='10.0.2.15',dst='10.0.2.2',flags=0x00)/ICMP())
.
Sent 1 packets.
>>> send(IP(src='10.0.2.15',dst='10.0.2.2',flags=0x04)/ICMP())
.
Sent 1 packets.
>>> 
```

The bottom status bar of the Wireshark window indicates: "Reserved bit (ip.flags.rb), 2 Bytes" and "Pakete: 22 · Angezeigt: 4 (18.2%)"

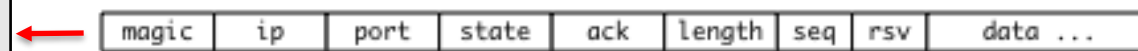
## Example 2: Ping Tunnel



**Analysis and improvements:**  
 Jaspreet Kaur, Steffen Wendzel,  
 Omar Eissa, Jernej Tonejc, Michael  
 Meier: [Covert Channel-internal  
 Control Protocols: Attacks and  
 Defense](#), *Security and  
 Communication Networks (SCN)*,  
 Vol. 9(15), Wiley, 2016.

Ethernet Frame
IP Header
ICMP Header
ICMP Echo Header
ICMP Echo Payload

Secret data is embedded into the ICMP echo payload.  
 In addition, a small protocol of the following format is used:



Figs.: <http://www.cs.uit.no/%7Edaniels/PingTunnel/>

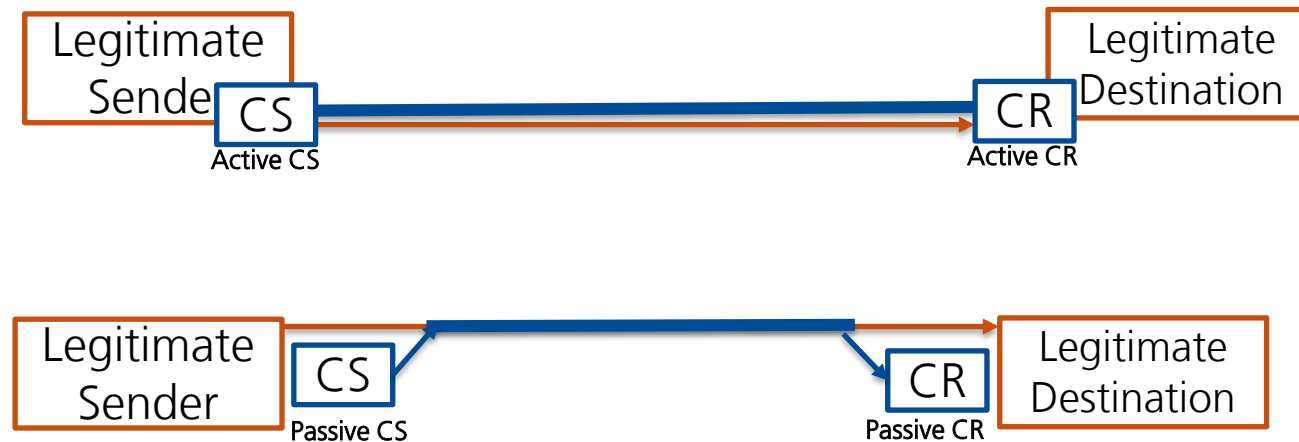
## Types of (Network) Covert Channels

Fundamental:

- **Local** and **network** covert channels
- **Storage** and **timing** channels
- **Noisy** and **noise-free** covert channels

## Types of (Network) Covert Channels: Active/Passive Cov. Channels

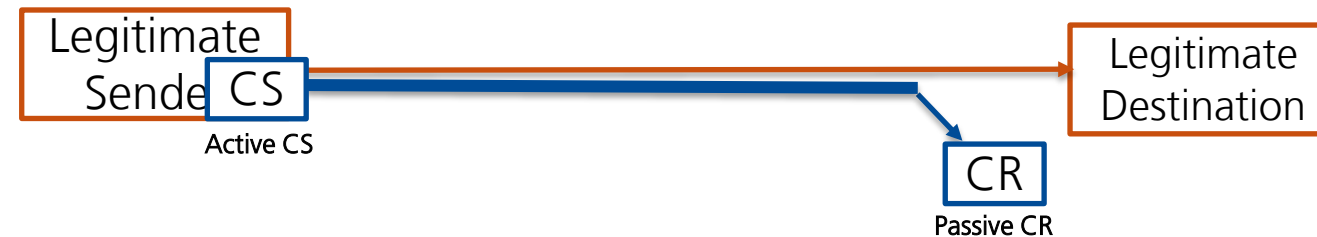
- **Active** and **passive** Covert Channels (passive elements have a different sender/receiver than the legitimate sender/receiver)



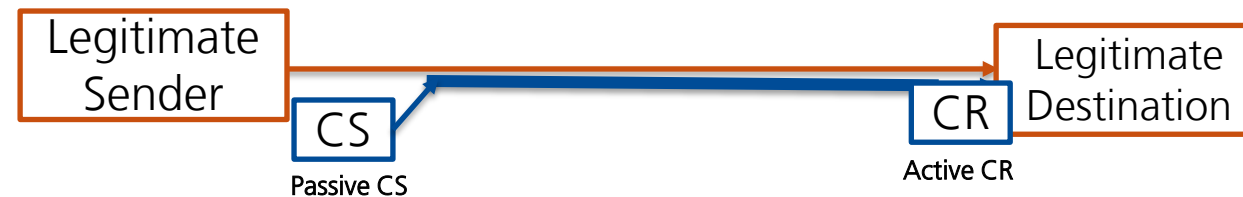
## Types of (Network) Covert Channels: Semi-active/passive Cov. Channels

- Semi-active and semi-passive Covert Channels [1]

- Semi-active:



- Semi-passive:



[1] K. Lamshöft, J. Dittmann: *Assessment of Hidden Channel Attacks: Targetting Modbus/TCP*, IFAC-PapersOnLine, 53(2), 2020.



## Types of (Network) Covert Channels: History Cov. Channels

- Most covert channels focus on the **present**, e.g., packets might contain secret stego data in their **current** payload.
- History** covert channels optimize transmission sizes by transferring solely pointers to larger data chunks already seen somewhere, e.g., in previous packets or online data [1]. These data chunks represent the actual secret information. First implementation called “**DYST**” (*Did You See That?*).
- Predictive** covert channels are a derivative of history channels but **anticipate upcoming** data they point to (e.g., anticipated regularly occurring network packets) [1].



⇒ **Reading Assignment:** S. Wendzel, T. Schmidbauer, S. Zillien, J. Keller: *Did You See That? A Covert Channel Exploiting Recent Legitimate Traffic*, 2022.  
<https://doi.org/10.48550/arXiv.2212.11850>

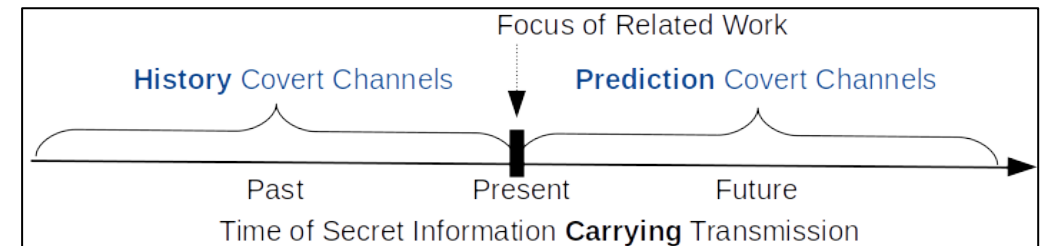


Fig.: [1]

[1] S. Wendzel, T. Schmidbauer, S. Zillien, J. Keller: *Did You See That? A Covert Channel Exploiting Recent Legitimate Traffic*, ArXiv pre-print, Dec-2022. Available online: <https://doi.org/10.48550/arXiv.2212.11850>

## Types of (Network) Covert Channels: History Cov. Channels

- History/prediction channels enable a new category of **fully-passive covert channels** (see Fig. below), where a stego data channel (in this case "DYST") can be represented through 100% legitimate traffic – solely the signaling channel (containing the pointer) needs to craft new/modify existing packets [1].



		Covert Sender		
		Active (generates own overt traffic in which it embeds covert data)	Passive (embeds covert data in overt traffic of third-party nodes)	Fully-passive (utilizes third-party traffic without modifying it)
Covert Receiver	Active (is the destination of the overt traffic)	Active Covert Channel	Semi-passive Covert Channel	Fully-and-semi-passive Covert Channel
	Passive (is not the direct destination of the overt traffic, e.g., a router)	Semi-active Covert Channel  DYST's Signal Channel	Passive Covert Channel	Fully-passive Covert Channel  DYST's Data Channel

Fig.: [1]

[1] S. Wendzel, T. Schmidbauer, S. Zillien, J. Keller: *Did You See That? A Covert Channel Exploiting Recent Legitimate Traffic*, ArXiv pre-print, Dec-2022. Available online: <https://doi.org/10.48550/arXiv.2212.11850>

## Types of (Network) Covert Channels: History Cov. Channels: DYST

- How do history covert channels work?
  - Different approaches feasible, also outside of networks.
- Together with the concept of history covert channels, we introduced a first implementation (before-mentioned **DYST**) in [1].

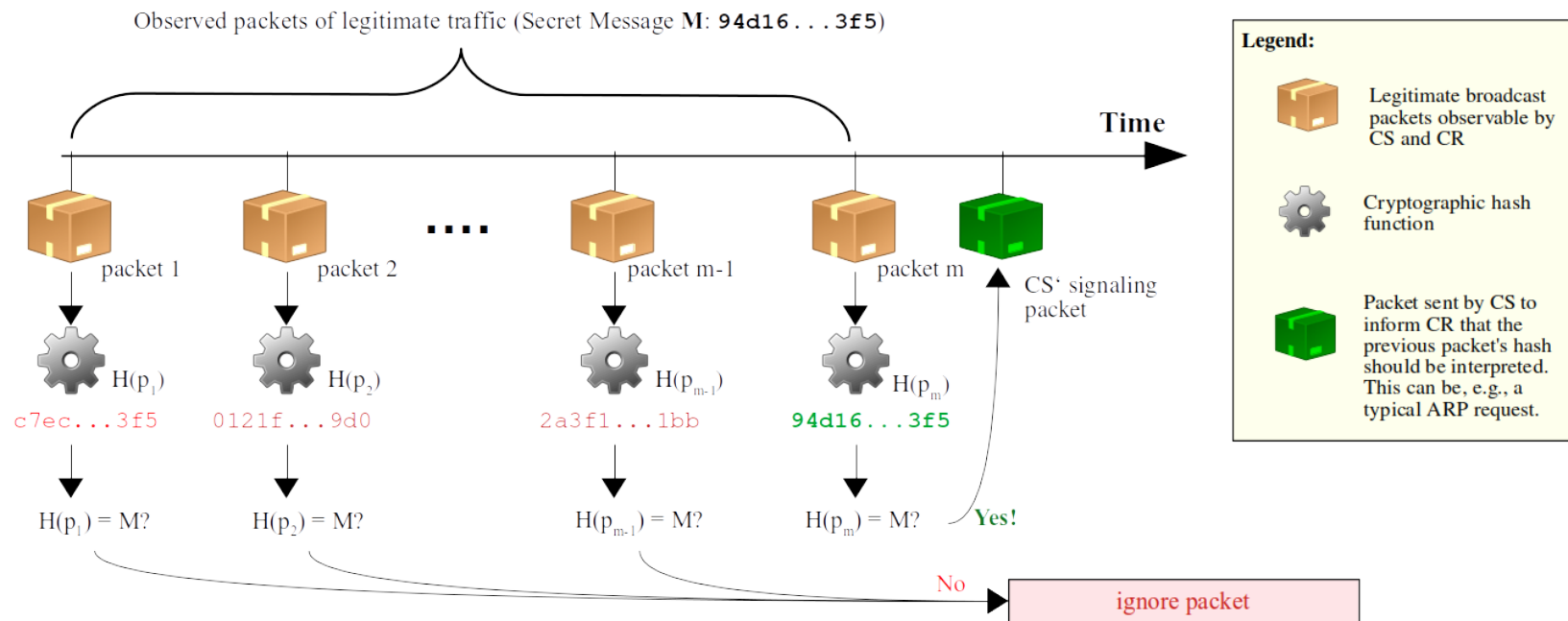


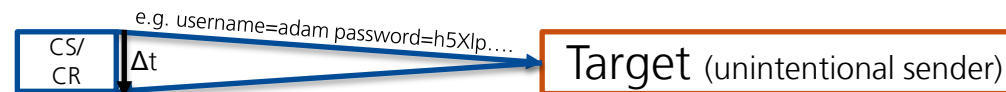
Fig.: [1]

[1] S. Wendzel, T. Schmidbauer, S. Zillien, J. Keller: *Did You See That? A Covert Channel Exploiting Recent Legitimate Traffic*, ArXiv pre-print, Dec-2022. Available online: <https://doi.org/10.48550/arXiv.2212.11850>

## Types of (Network) Covert Channels: (Un)Intentional Cov. Ch.

- Intentional (covert) and unintentional (side) channels
  - e.g. side channels in web applications, see [talk by S. Schinzel](#)

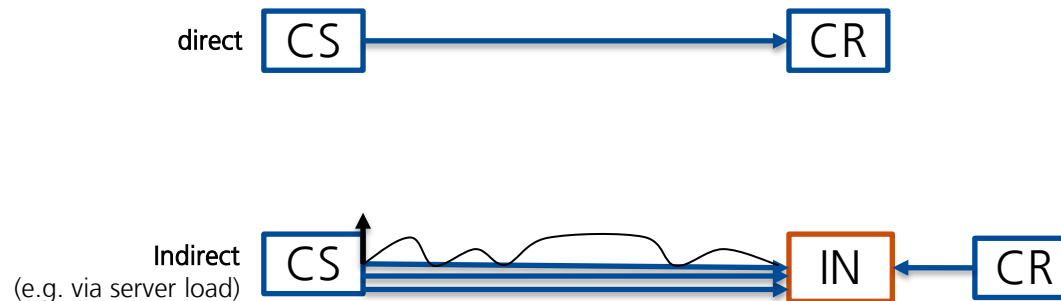
- Example:



\* Traffic must be sent many times and measured exactly to gain any useful information out of this.

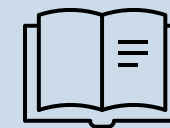
## Types of (Network) Covert Channels: (In)Direct Cov. Channels

- **Direct** and **indirect** covert channels: direct channels do not rely on intermediate nodes (IN).
  - Example: via web page + server load
  - General illustration:



Further differentiation into **two major patterns** for the intermediate node (IN): **redirector** and **broker**.

- A broker can be a **proxy** or a **dead drop**.



⇒ **Reading Assignment:** T. Schmidbauer, S. Wendzel: *SoK A Survey of indirect network-level covert channels*, in Proc. 17th AsiaCCS, ACM, 2022. **Section 3.** <https://doi.org/10.1145/3488932.3517418> (PDF available through Moodle).

## How to „measure“ covert channels?

Only in brief as this **will be covered in more detail in the course 01730 „Introduction to Information Hiding“ by J. Keller.**

- Capacity, Bitrate and Bandwidth (how much information or data can be transferred per time?)
- Undetectability / covertness (how detectable is the covert channel?)
- Robustness (for noisy channels: how fragile is the covert channel?)

## How to „measure“ covert channels?

- Introduction of **Covertness** by Giani et al. [1]:

Covertness  $\propto$  (Capacity of the medium – Transmission Rate)

If the whole capacity of a transmission medium (e.g. network packets or an audio CD) is used, the covertness is zero, leading to a trivial detection. However, if only a tiny fraction of the capacity is used, the covertness can remain close to one.

[1] A. Giani, V. H. Berk, G. V. Cybenko: Data Exfiltration and Covert Channels, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense V. Vol. 6201. International Society for Optics and Photonics, 2006.

## How to „measure“ covert channels?

- **Steganographic Cost (SC)** by Mazurczyk et al. [1]:
  - Measure of degradation or distortion of a carrier caused by the application of a steganographic method.
  - Calculation depends on context. For instance, for *LACK* steganography, which exploits packet loss, the SC can be calculated using the *Mean Opinion Score* (MOS) as a difference in quality of the voice signal (RQ) without and with LACK applied (LQ):

$$SC_{T-LACK}(t) = \Delta MOS(t) = RQ(t) - LQ(t)$$

- For *Retransmission Steganography* (RSTEG), one can calculate the retransmission difference  $R_D$  instead:

$$SC_{T-RSTEG} = R_D = R_{N-RSTEG} - R_N$$

- $R_{N-RSTEG}$  denotes retransmissions in the network with RSTEG and  $R_N$  the network's retransmissions without applying RSTEG.

[1] W. Mazurczyk, S. Wendzel, I. Azagra Villares, K. Szczypiorski: On importance of steganographic cost for network steganography, SCN, 9(8), 781-790, Wiley, 2016.



## How to „measure“ covert channels?

- Steganographic Cost by Mazurczyk et al. [1]:
  - If multiple steganographic methods exploit the same subcarrier **S1** of the carrier **C1**, the **total steganographic cost of the carrier  $SC_{T(C1)}$**  can be expressed as:

$$SC_{T(C1)}(n) = \sum_{n=1}^n SC_{S1-n}$$

- $SC_{S1-n}$  is the steganographic cost of the  $n$ 'th method applied to subcarrier **S1**.

[1] W. Mazurczyk, S. Wendzel, I. Azagra Villares, K. Szczypiorski: On importance of steganographic cost for network steganography, Security and Communication Networks (SCN), Vol. 9(8), 781-790, Wiley, 2016.