NETWORK INFORMATION HIDING

CH. 4: INTRODUCTION TO NETWORK INFORMATION HIDING

Prof. Dr. Steffen Wendzel
Worms University of Applied Sciences

https://www.wendzel.de (EN) | https://www.hs-worms.de/wendzel/ (EN)

Online Class: https://github.com/cdpxe/Network-Covert-Channels-A-University-level-Course/

Definition

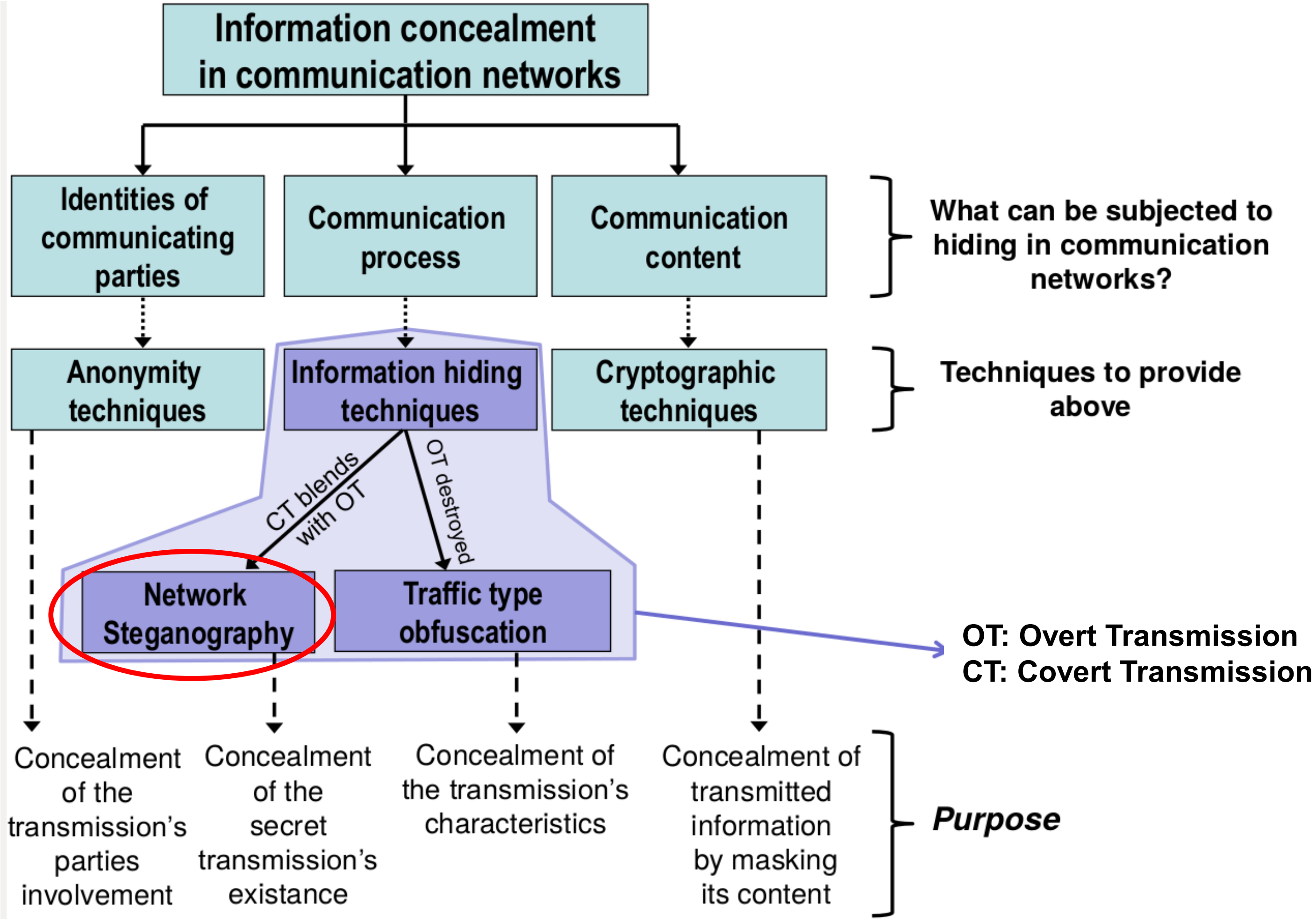

Information concealment in communication networks
Identities of communicating parties
Communication process
Communication content
What can be subjected to hiding in communication networks?
Anonymity techniques
Information hiding techniques
Cryptographic techniques
Techniques to provide above
CT blends 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

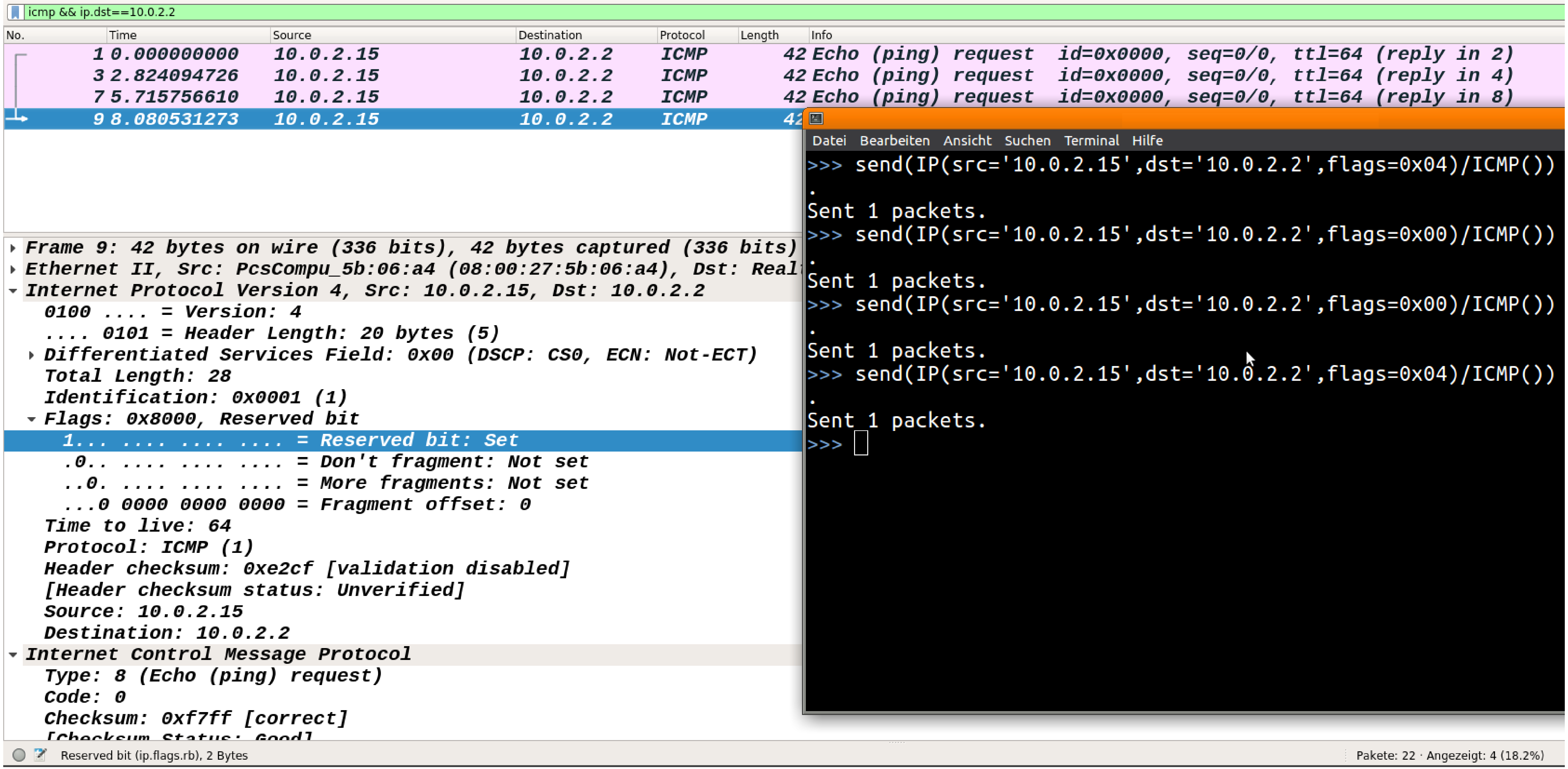
Fig.: W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016

Differences to **traditional** digital media steganography

- No clear distinction between **steganography** and **covert channel**
  - Instead: **network covert channel** or **network steganographic channel handled separately**
  - Unified: a steganographic **method** creates such a **covert channel** [1, Chapter 3]
- Covert data is hidden in overt network transmissions
- The „cover object“ is now called „carrier“
- Advantage of a constant transmission (e.g. permanent data leakage)
- 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”



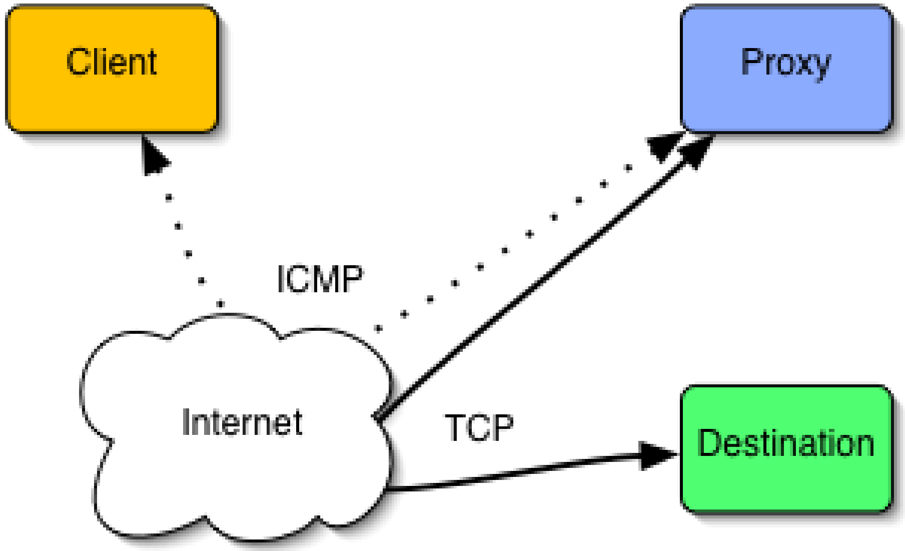
```
icmp && ip.dst==10.0.2.2

No.  Time           Source       Destination  Protocol  Length  Info
  1  0.000000000    10.0.2.15    10.0.2.2     ICMP          42  Echo (ping) request  id=0x0000, seq=0/0, ttl=64 (reply in 2)
  3  2.824094726    10.0.2.15    10.0.2.2     ICMP          42  Echo (ping) request  id=0x0000, seq=0/0, ttl=64 (reply in 4)
  7  5.715756610    10.0.2.15    10.0.2.2     ICMP          42  Echo (ping) request  id=0x0000, seq=0/0, ttl=64 (reply in 8)
  9  8.080531273    10.0.2.15    10.0.2.2     ICMP          42
```

```
▸ 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]
```

```
Reserved bit (ip.flags.rb), 2 Bytes                    Pakete: 22 · Angezeigt: 4 (18.2%)
```

```
>>> 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.
>>> 
```

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 Payload ←

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

magic	ip	port	state	ack	length	seq	rsv	data ...

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

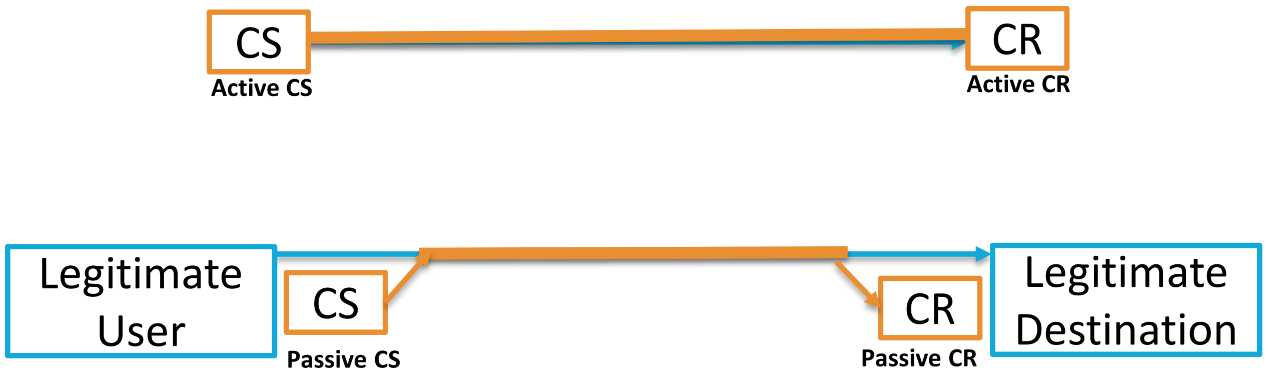
Types of (Network) Covert Channels

Fundamental:

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

Types of (Network) Covert Channels

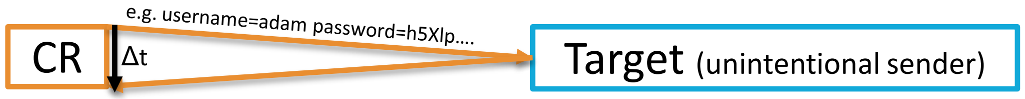
- Active and passive covert channels



Types of (Network) Covert Channels

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

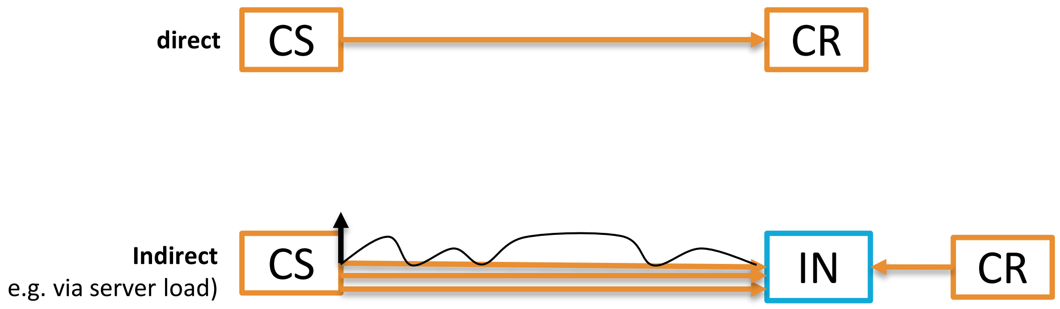
  - Example:


e.g. username=adam password=h5Xlp....
CR
Δt
Target (unintentional sender)

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

Types of (Network) Covert Channels

- Direct and indirect covert channels
  - e.g. via web page + server load


direct
CS
CR
Indirect
e.g. via server load)
CS
IN
CR