NETWORK INFORMATION HIDING:
A COURSE ON STEGANOGRAPHY AND COVERT CHANNELS

Prof. Dr. Steffen Wendzel
Worms University of Applied Sciences

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

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

Introducing myself

Prof. at Worms Univ. of Appl. Sciences, Germany

Primary research interests:

- Network Information Hiding/Covert Channels
  - cleaning up the terminology, taxonomy, methodology
  - developing countermeasures and new hiding techniques
  - cf. https://ih-patterns.blogspot.com
- IoT/Smart Home/Smart Building Security
  - network-level security, e.g. traffic normalization, anomaly detection, communication protocols
- also:
  - Operating Systems (+Security) / Linux & BSD, author of some German Linux books
  - Methodology of Information Security (IWSMR) & Scientometrics
  - Retro Computing ☺

Photo: Elonicate Photography, https://www.instagram.com/elocinate/

Overview of this Course

1. Introduction to **steganography** and **covert channels**
2. Introduction to local covert channels
3. Fundamental countermeasures (not network-specific)
4. Fundamental network information hiding techniques
5. Getting the big picture: **hiding patterns**
6. Staying under the radar: sophisticated hiding methods
7. Selected countermeasures
8. Replicating experiments for scientific advancement
9. OMG! I found a new hiding method. How to get famous?!1!
   a.k.a. How to describe a new hiding method in a paper?
10. My smart fridge does strange things …
    a.k.a. Steganography in the Internet of Things (IoT)
11. Overall conclusion

NETWORK INFORMATION HIDING

CH. 1: INTRODUCTION

Prof. Dr. Steffen Wendzel
Worms University of Applied Sciences

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

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

Introduction

Several content of this lecture is based on our book on Information Hiding in Communication Networks (Wiley-IEEE, 2016).

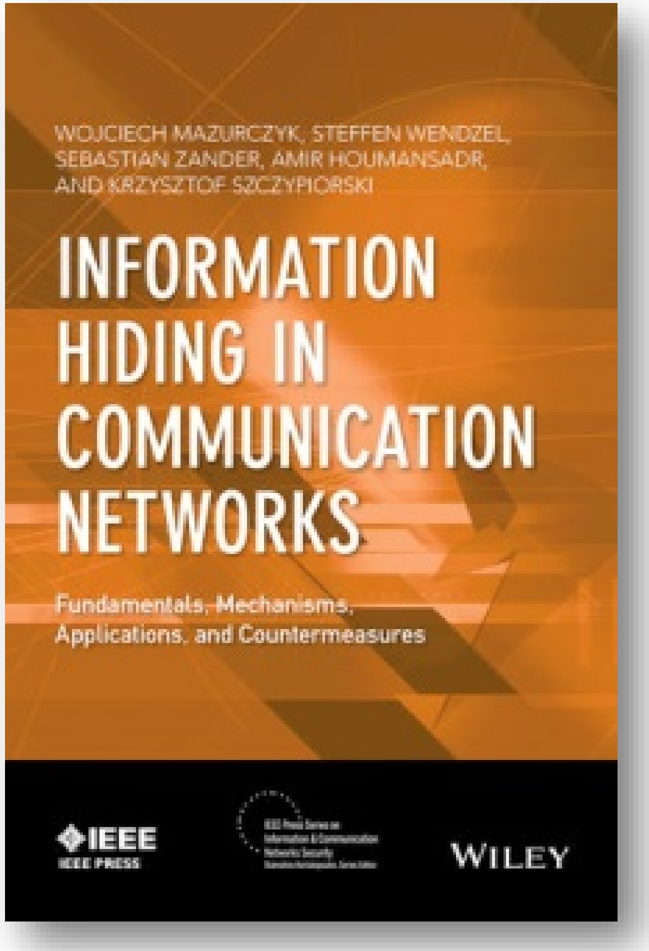
- Book should be **freely downloadable via IEEEXplore if you are an IEEE member** (or: if your university is a member ☺)

- Community agreed on common understanding of many things to find a good basis for this book.

- Based on several years of research of the authors.

- Please note: the chapters on traffic obfuscation and network flow watermarking are not part of this course.

- After >10 years of active research in network information hiding, my co-authors and me published quite a lot of work. If my name appears in a citation, you will find the paper linked on my website.



WOJCIECH MAZURCZYK, STEFFEN WENDZEL, SEBASTIAN ZANDER, AMIR HOUMANSADR, AND KRZYSZTOF SZCZYPIORSKI

INFORMATION HIDING IN COMMUNICATION NETWORKS

Fundamentals, Mechanisms, Applications, and Countermeasures

IEEE
IEEE PRESS

WILEY

Information Hiding: What is it?

What is „Information Hiding“? Two different examples:

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

Information Hiding: What is it?

Fundamental Taxonomy on Information Hiding by Petitcolas et al. [1]

Note: I will later show two taxonomies specific to Network Information Hiding

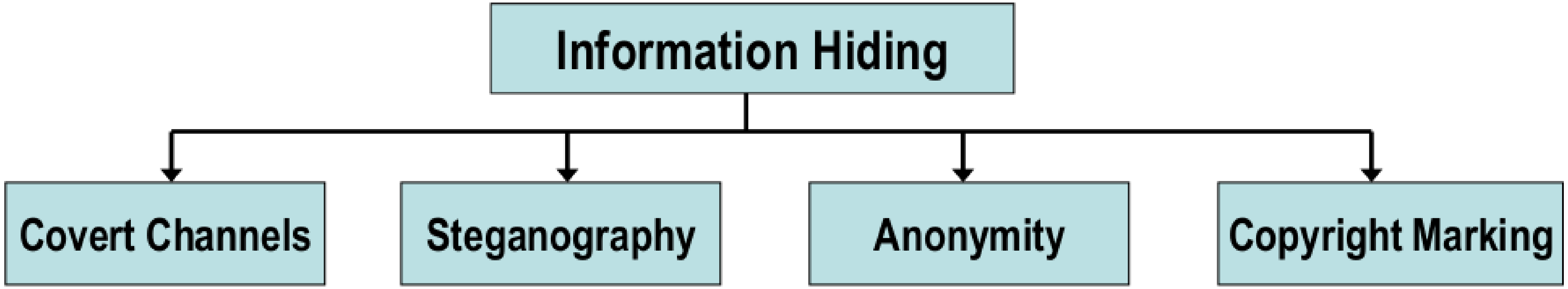


Fig.: [2] (but based on [1], where an extended taxonomy featuring linguistic/technical steganography and different types of copyright marking can be found).

[1] Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE*, *87*(7), 1062-1078.

[2] Mazurczyk, W. et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016.

Information Hiding: What is it?

… it appeared in ancient Greece.

499 BC: **Histiaeus** (ruler of Miletus) tattooed a message on the head of one of his slaves to send a message to Aristagoras (his son-in-law) to instruct him to revolt against the Persians.

(Several more cases of Steganography in ancient Greece are known.)

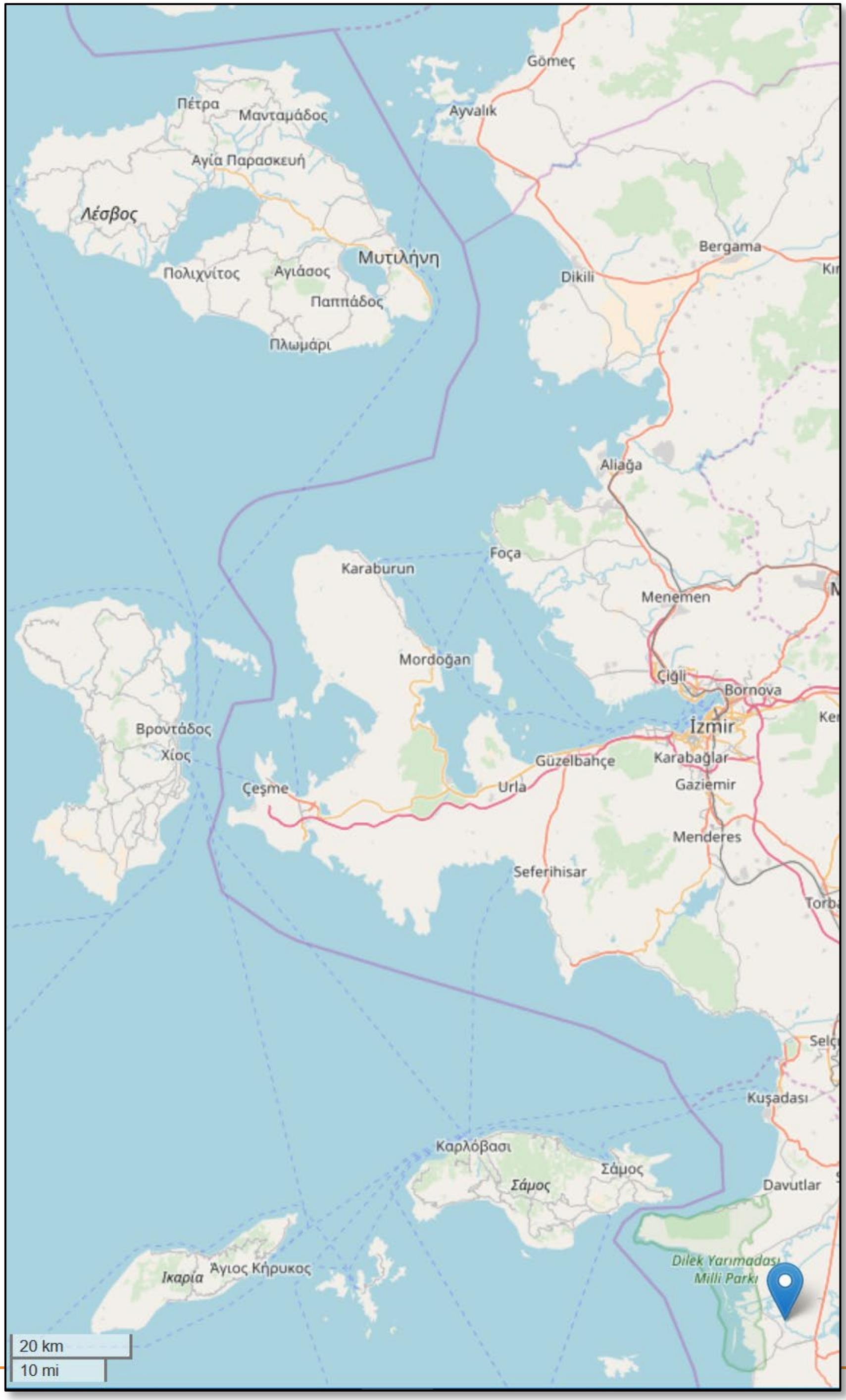


Image taken from Google Maps.

Information Hiding: What is it?

Another example:

- 1978 World Championship in chess between Viktor Korchnoi (CH/RU) and Anatoly Karpov (RU)

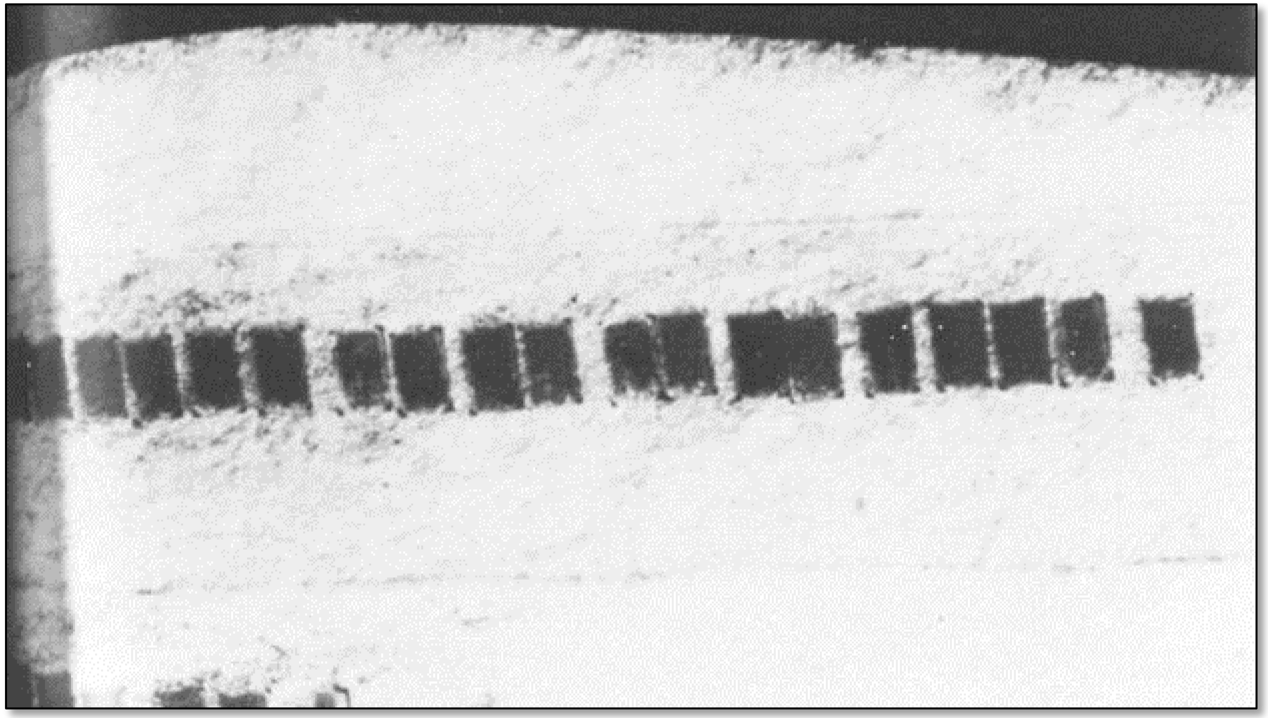
  Officials „limited Karpov to consumption of only one type of yogurt (violet) at a fixed time during the game.“ [1]

Fig.: private photo

[1] Fridrich, J.: Steganography in Digital Media, Cambridge University Press, 2010.

Information Hiding: What is it?

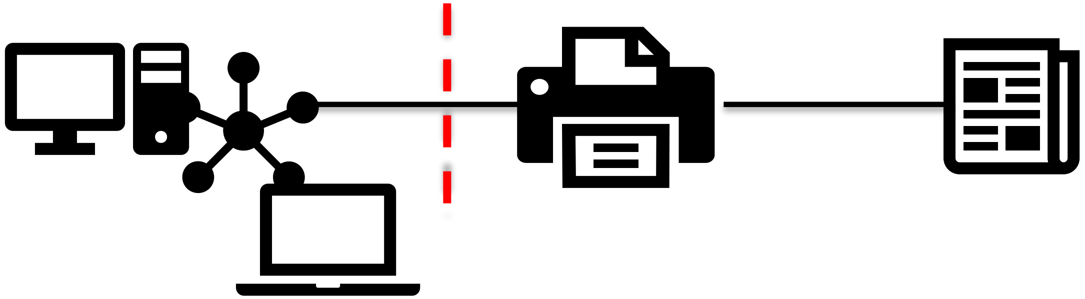
Another example: Microdots; used during WW2, e.g. by German spies in Mexico.



NSA photo of microdots used by German spies, source: Wikipedia, author: unknown

Information Hiding: What is it?

Another Example: Printer Watermarking



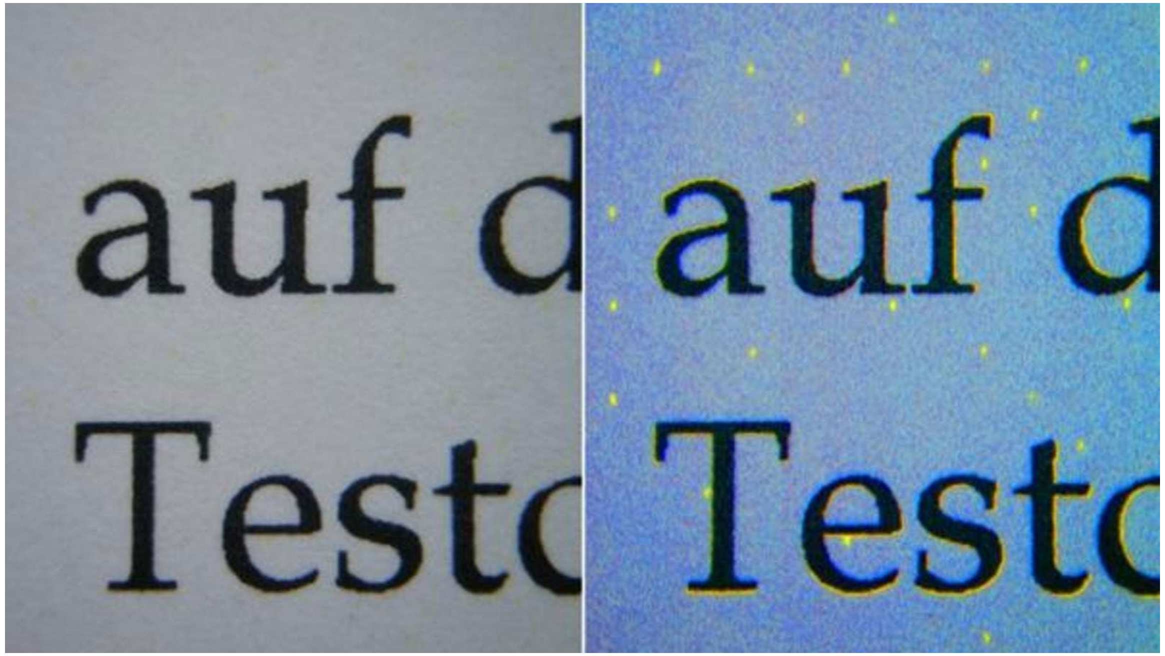
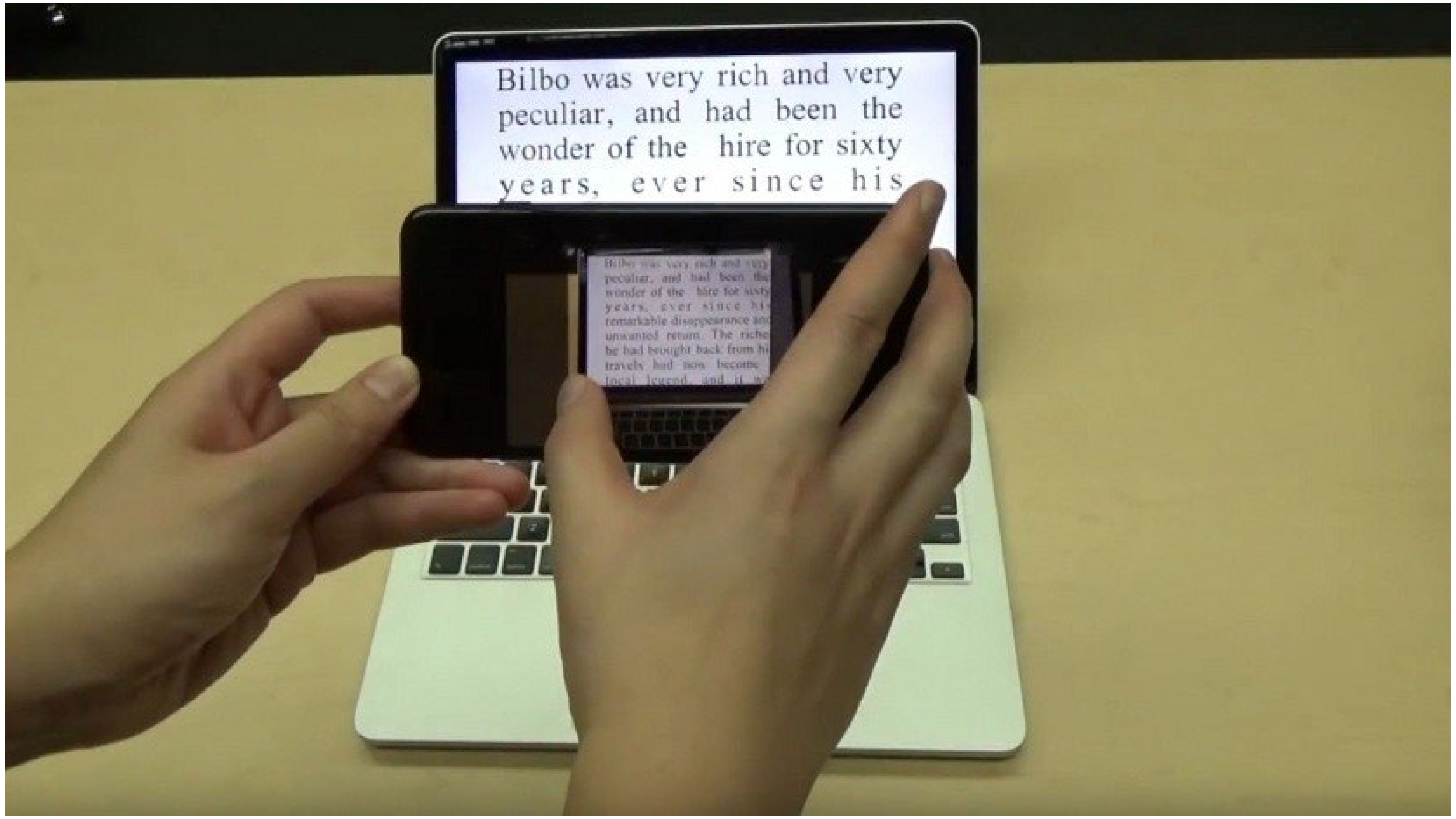


Fig. source/attribution: F. Heise/Wikipedia/BBC

Information Hiding: What is it?

Final example: *fontcode* (works with digital and printed documents)



Bilbo was very rich and very peculiar, and had been the wonder of the hire for sixty years, ever since his

Video: https://youtu.be/dejrBf9jW24

History of Information Hiding

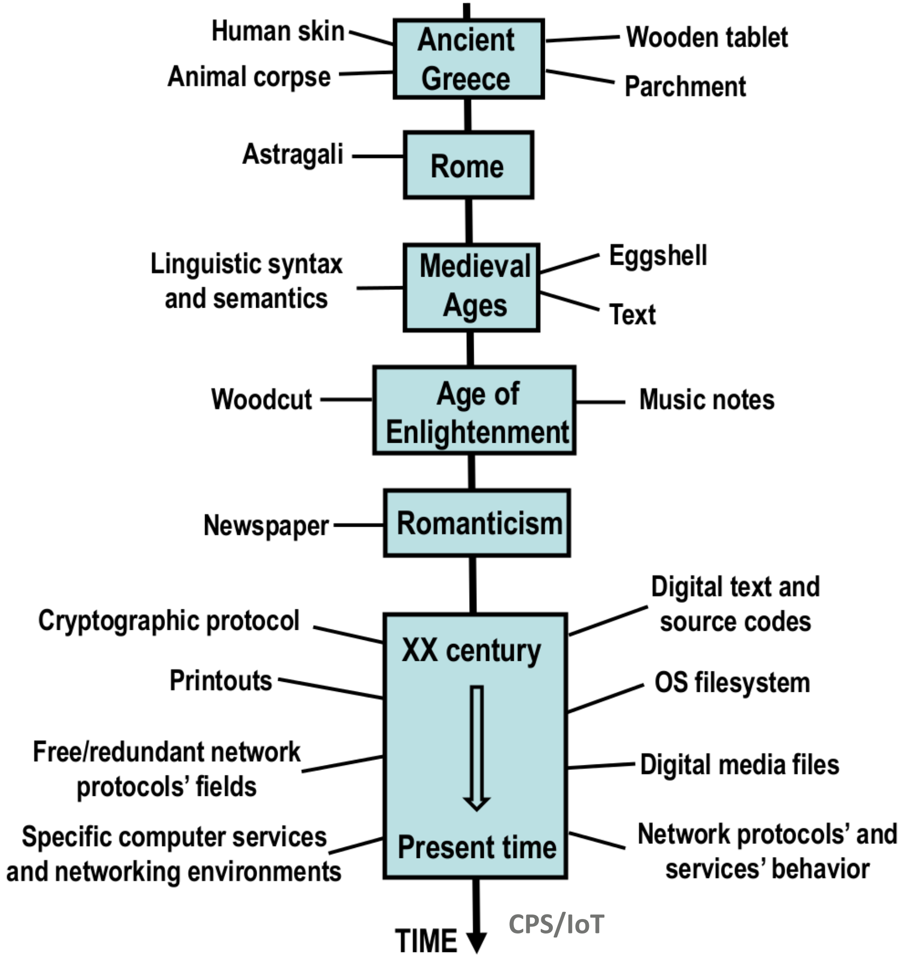


Fig.: W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016

History of Information Hiding

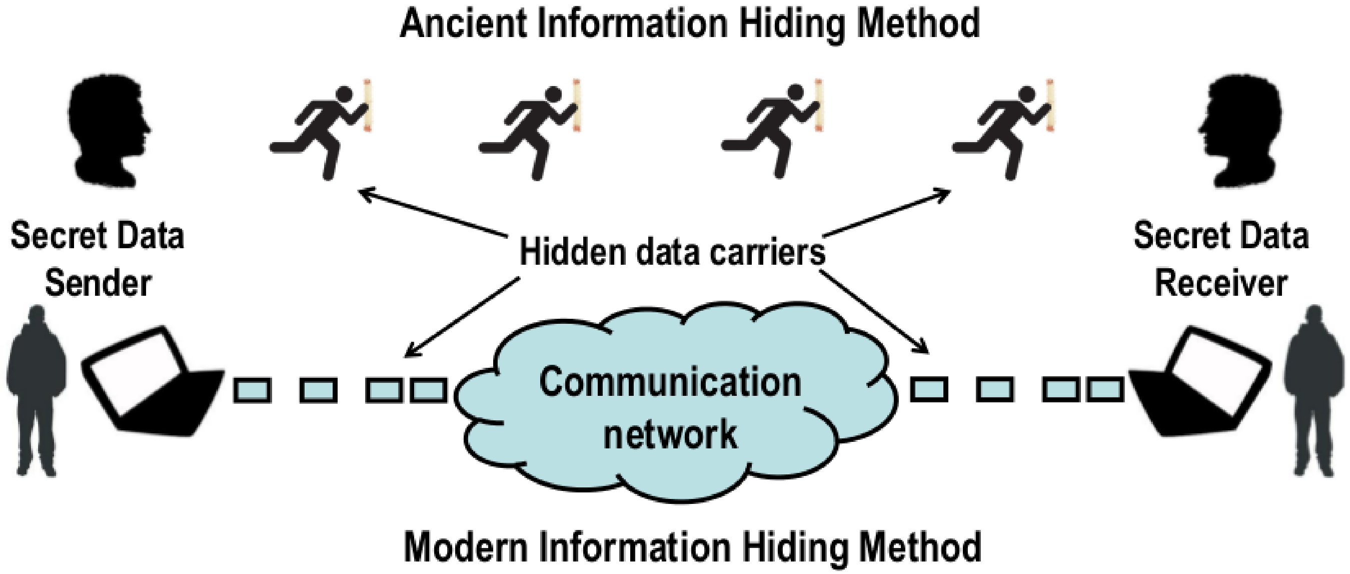


Fig.: W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016

Covert Data Storage & Communication

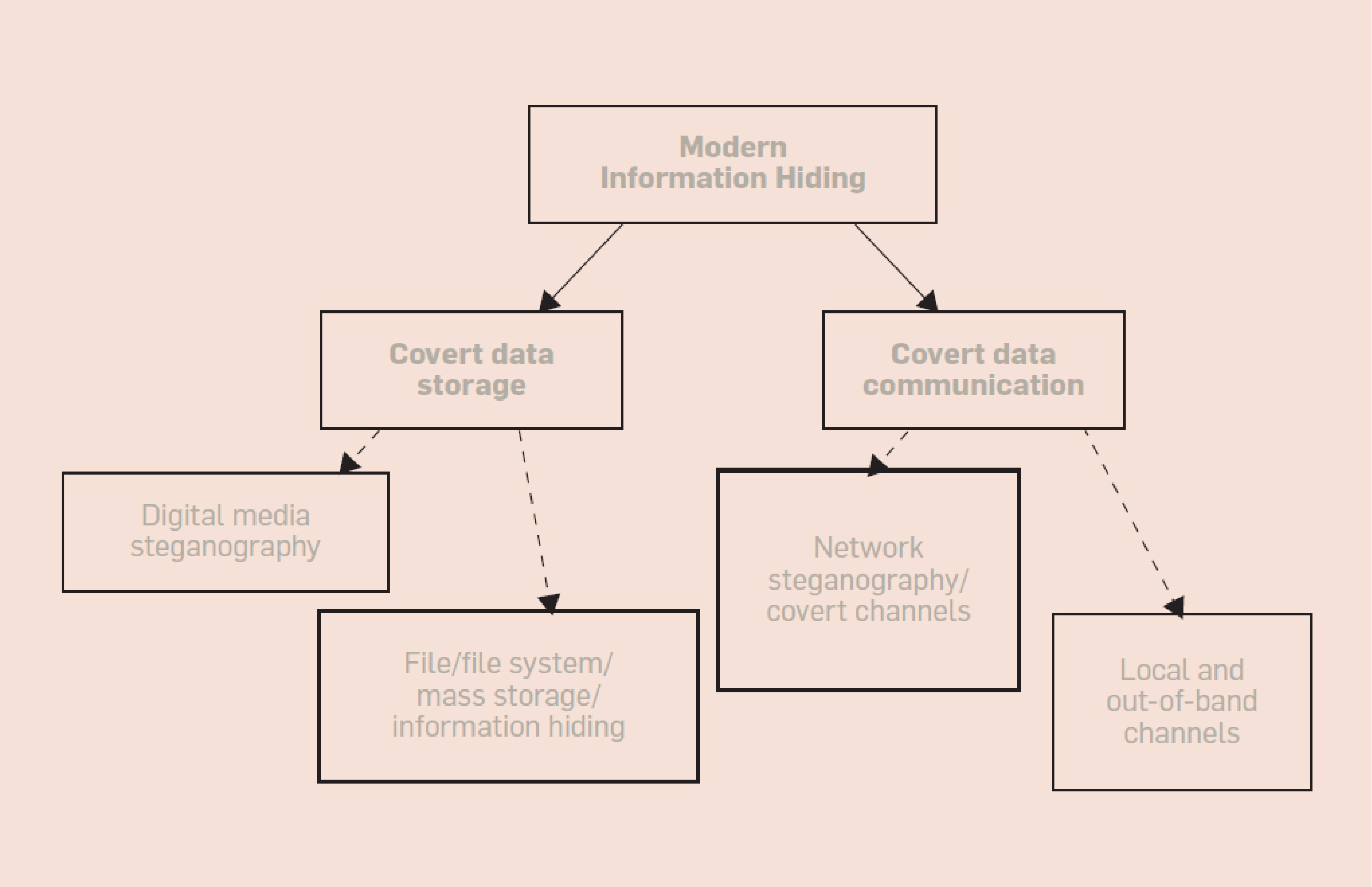
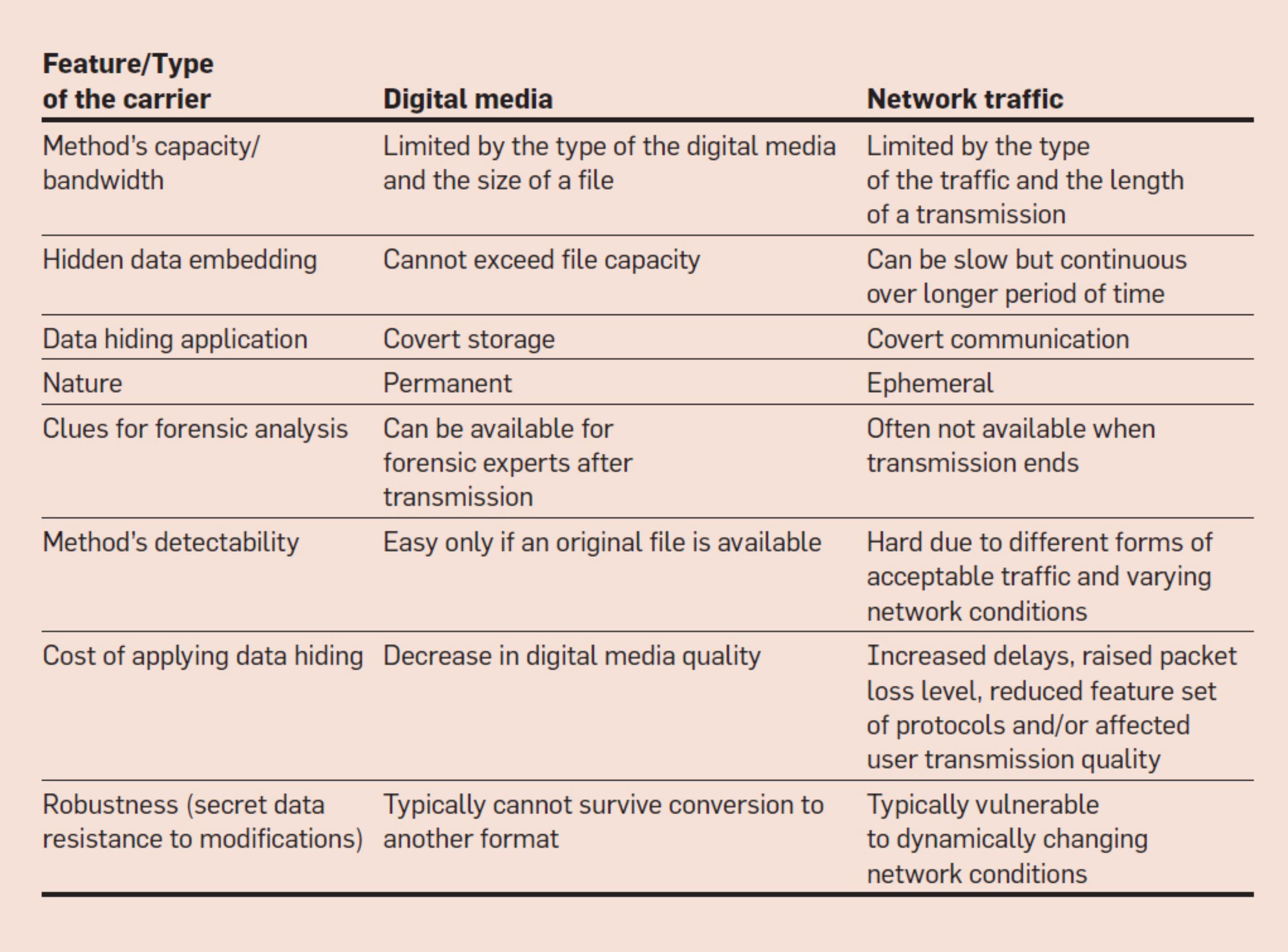

Modern Information Hiding
Covert data storage
Covert data communication
Digital media steganography
File/file system/ mass storage/ information hiding
Network steganography/ covert channels
Local and out-of-band channels

Fig.: W. Mazurczyk, S. Wendzel: Information Hiding: Challenges for Forensic Experts, Comm. ACM, 2018.

Application of Hiding Techniques

Okay, so what is the big difference between digital media and network carriers?



Feature/Type of the carrier	Digital media	Network traffic
Method's capacity/ bandwidth	Limited by the type of the digital media and the size of a file	Limited by the type of the traffic and the length of a transmission
Hidden data embedding	Cannot exceed file capacity	Can be slow but continuous over longer period of time
Data hiding application	Covert storage	Covert communication
Nature	Permanent	Ephemeral
Clues for forensic analysis	Can be available for forensic experts after transmission	Often not available when transmission ends
Method's detectability	Easy only if an original file is available	Hard due to different forms of acceptable traffic and varying network conditions
Cost of applying data hiding	Decrease in digital media quality	Increased delays, raised packet loss level, reduced feature set of protocols and/or affected user transmission quality
Robustness (secret data resistance to modifications)	Typically cannot survive conversion to another format	Typically vulnerable to dynamically changing network conditions

Fig.: W. Mazurczyk, S. Wendzel: Information Hiding: Challenges for Forensic Experts, Comm. ACM, 2018.

Basic Mimicry System [1]

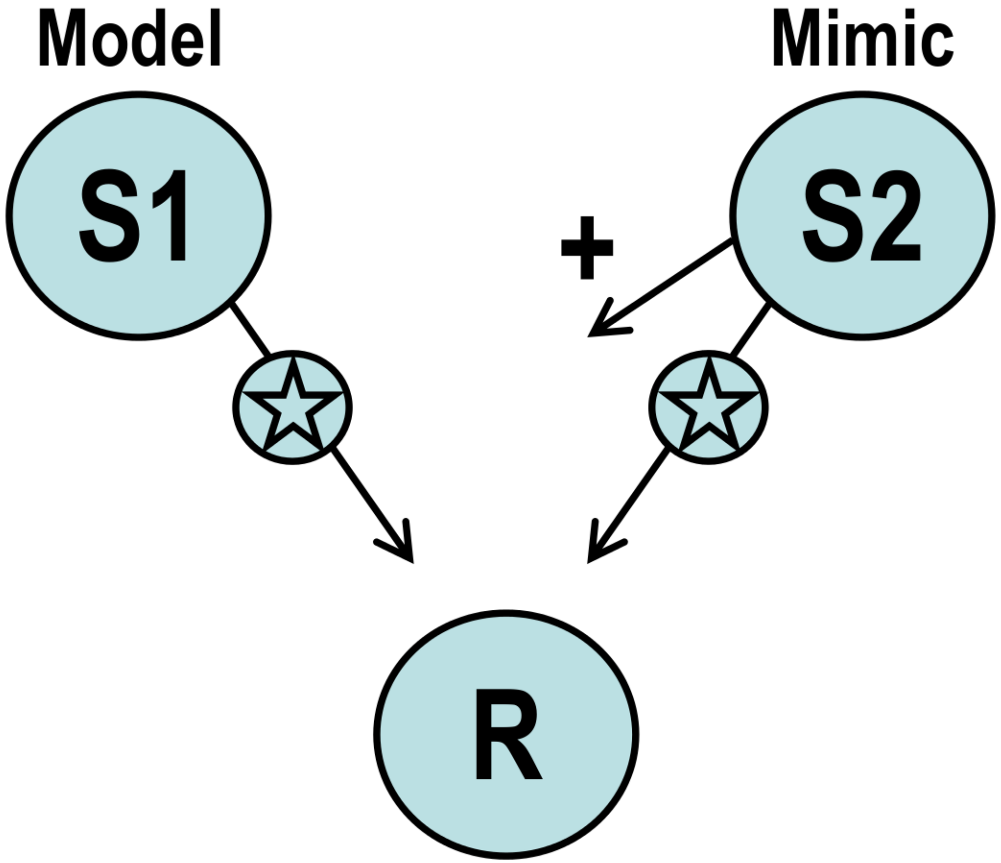


Fig.: [2]

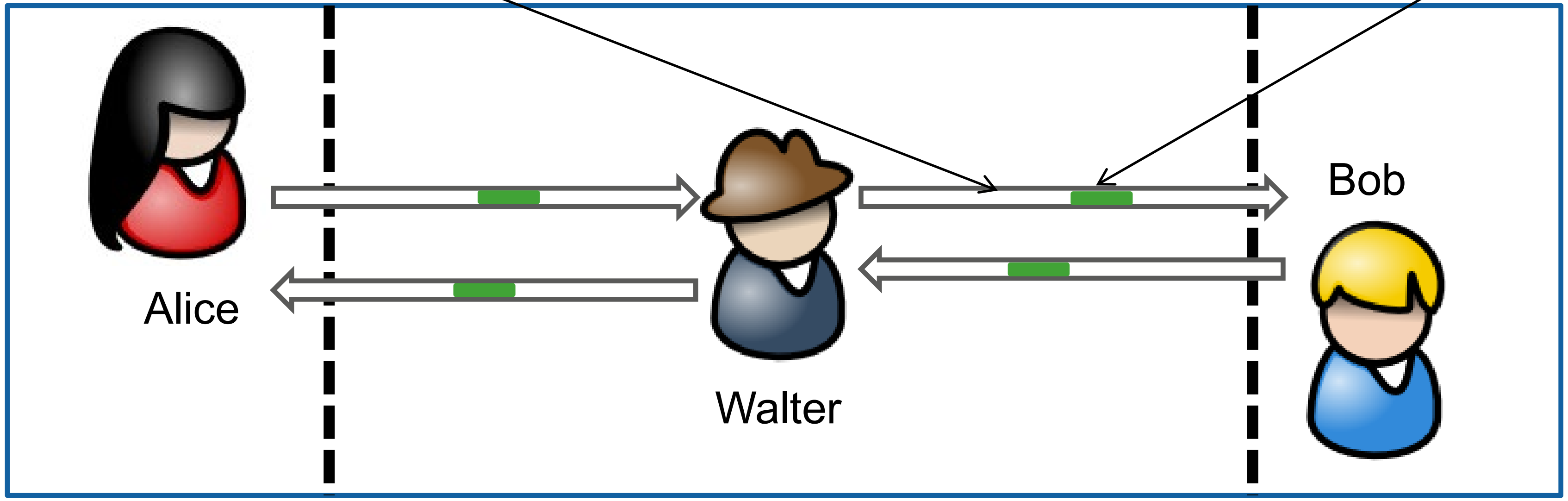
[1] Vane-Wright, R. I.: A unified classification of mimetic resemblances, Biological Journal of the Linnean Society, 1976.
[2] W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016

Terminology: Prisoner‘s Problem (Simmons, 1983)

- Covert Channel definition by Lampson [1]: *“…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) [2].

- Steganography [3]:
  - “Steganography can be informally defined as the practice of undetectably communicating a **message** **(a.k.a. steganogram)** in a **cover object**.“

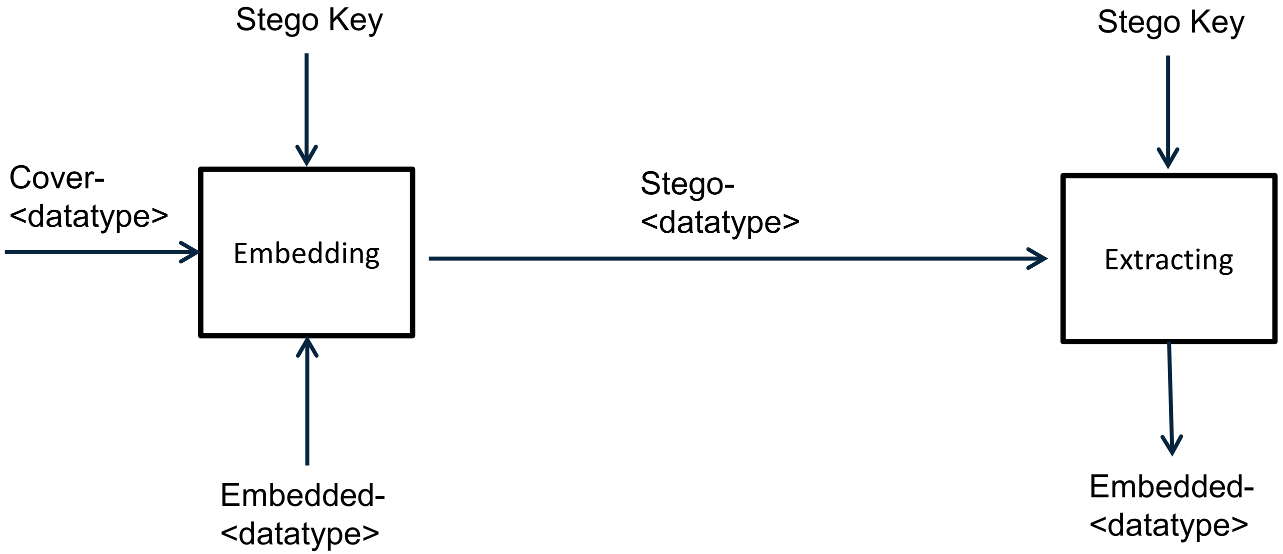
- Prisoner‘s Problem by Simmons [4]:



[1] Lampson, B.W.: A Note on the Confinement Problem, Comm. ACM, 1973. ||| [2] DoD: Trusted Computer System Evaluation Criteria (TCSEC), Department of Defense, 1985. ||| [3] Fridrich, J.: Steganography in Digital Media, Cambridge University Press, 2010. ||| [4] Simmons, G. J.: The Prisoners’ Problem and the Subliminal Channel, in Proc. Crypto’83 – Advances in Cryptology, 1984.

Terminology

- Remember [1]:
  - “Steganography can be informally defined as the practice of undetectably communicating a **message** **(a.k.a. steganogram)** in a **cover object**.“
- Terminology of Pfitzmann [2]:

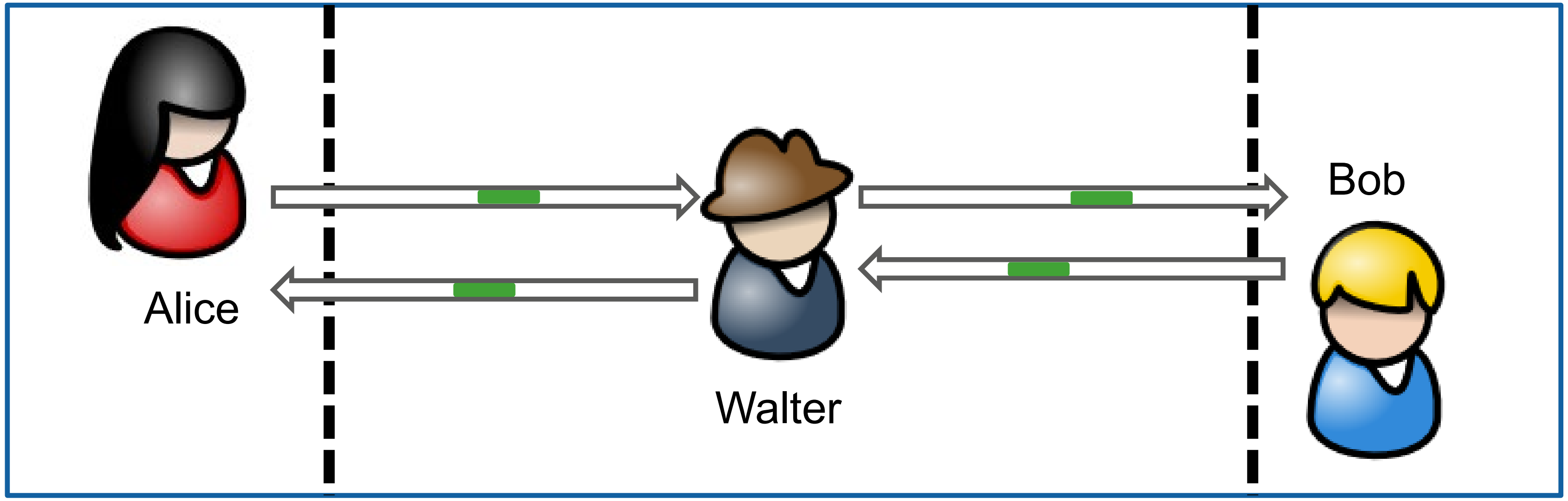


- This process is **bijective**.

[1] Fridrich, J.: Steganography in Digital Media, Cambridge University Press, 2010.
[2] Pfitzmann, B.: Information Hiding Terminology, Proc. 1st Information Hiding Workshop, Springer, 1996.

Terminology

- Walter is referred to as a **warden**. He performs a so-called **steganalysis**.
- A warden can be [1]
  - 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)

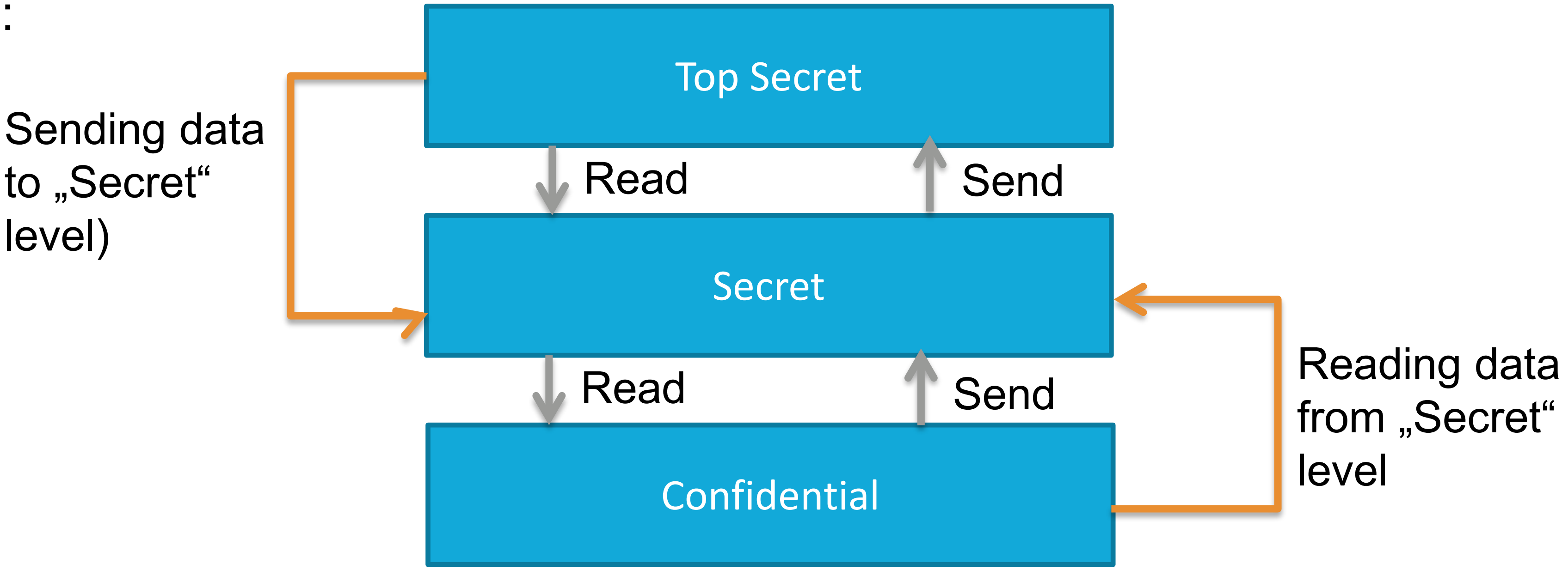


[1] Fisk, G., Fisk, M. Papadopoulos, C., Neil, J.: Eliminating Steganography in Internet Traffic with Active Wardens, Fisk, G., Fisk, M., Papadopoulos, C. and Neil, J., 2002, October. Eliminating steganography in Internet traffic with active wardens. In *International Workshop on Information Hiding* (pp. 18-35). Springer, Berlin, Heidelberg, 2002.

DoD Definition of Covert Channels in MLS Context

- In classical papers, a covert channel either violates the NRU (no read-up) or the NWD (no write-down) rule of the Bell-LaPadula (BLP) Model.

- Example:


Top Secret
Read
Send
Secret
Read
Send
Confidential
Sending data to „Secret“ level)
Reading data from „Secret“ level

cf. DoD: Trusted Computer System Evaluation Criteria (TCSEC), Department of Defense, 1985 and works on the BLP.

Is it applied in practice?

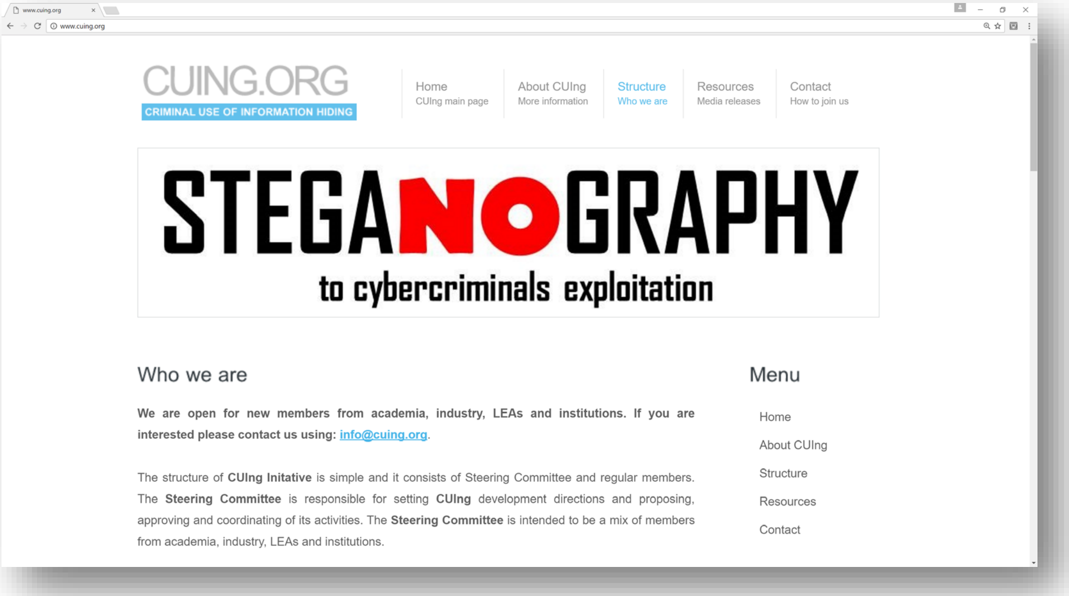
Early cases:

- 2002: „Operation Twins“ culminated in the capture of criminals associated with the „Shadowz Brotherhood“ group, a world-wide Internet pedophile organization.
  - Digital image steganography was used to hide a pornographic file within another innocent-looking one.
- 2008: Unknown person smuggled sensitive financial data out of U.S. Department of Justice using image steganography.
- 2010: Russian spy ring leaked classified information via image steganography from USA to Moscow.
- 2013: Linux Fokirtor malware hides traffic in SSH connections
- Since 2014: heaviy increase in (Network) Information Hiding-capable malware, so-called **Stegomalware**

Sources:

- Cases 1-3: Zielinska, E., Mazurczyk, W., Szczypiorski, K: Trends in steganography, Comm. ACM, 2014.
- Case 4: Schneier, B.: Fokirtor, https://www.schneier.com/blog/archives/2013/11/fokirtor.html, Nov. 2013.

Is it applied in practice?



CUING.ORG

CRIMINAL USE OF INFORMATION HIDING

Who we are

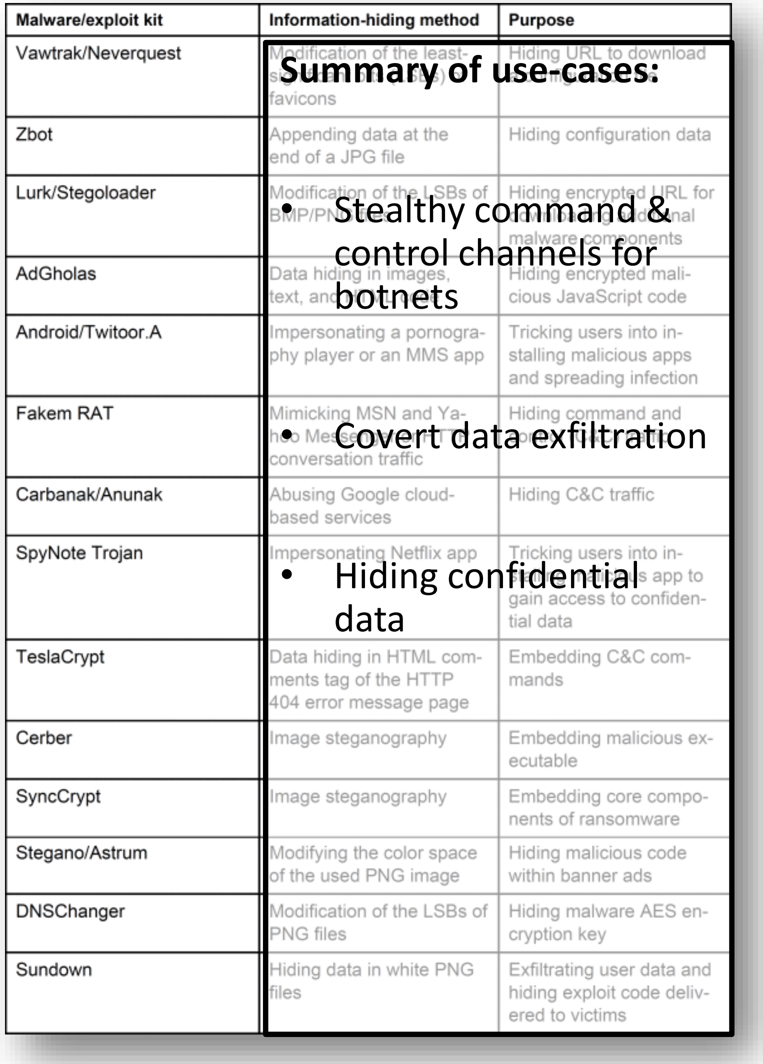
We are open for new members from academia, industry, LEAs and institutions. If you are interested please contact us using: info@cuing.org.

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.

Menu

- Home
- About CUIng
- Structure
- Resources
- Contact

cf. W. Mazurczyk, S. Wendzel: Information Hiding. Challenges for Forensic Experts, Communications of the ACM, 2018.



Malware/exploit kit	Information-hiding method	Purpose
Vawtrak/Neverquest	Modification of the least-significant bits (LSBs) of favicons	Hiding URL to download configuration file
Zbot	Appending data at the end of a JPG file	Hiding configuration data
Lurk/Stegoloader	Modification of the LSBs of BMP/PNG files	Hiding encrypted URL for downloading additional malware components
AdGholas	Data hiding in images, text, and HTML code	Hiding encrypted malicious JavaScript code
Android/Twitoor.A	Impersonating a pornography player or an MMS app	Tricking users into installing malicious apps and spreading infection
Fakem RAT	Mimicking MSN and Yahoo Messenger and HTTP conversation traffic	Hiding command and control (C&C) traffic
Carbanak/Anunak	Abusing Google cloud-based services	Hiding C&C traffic
SpyNote Trojan	Impersonating Netflix app	Tricking users into installing malicious app to gain access to confidential data
TeslaCrypt	Data hiding in HTML comments tag of the HTTP 404 error message page	Embedding C&C commands
Cerber	Image steganography	Embedding malicious executable
SyncCrypt	Image steganography	Embedding core components of ransomware
Stegano/Astrum	Modifying the color space of the used PNG image	Hiding malicious code within banner ads
DNSChanger	Modification of the LSBs of PNG files	Hiding malware AES encryption key
Sundown	Hiding data in white PNG files	Exfiltrating user data and hiding exploit code delivered to victims

Summary of use-cases:

- Stealthy command & control channels for botnets
- Covert data exfiltration
- Hiding confidential data

Kabaj et al.: *The new threats of information hiding: the road ahead*, IEEE IT Prof., Vol. 20(3), 2018 (Tab., r.).

Some potential scenarios

- Advanced Persistent Threats (APT): large-scale sophisticated data leakage, involving techniques such as `spear phishing'
- 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

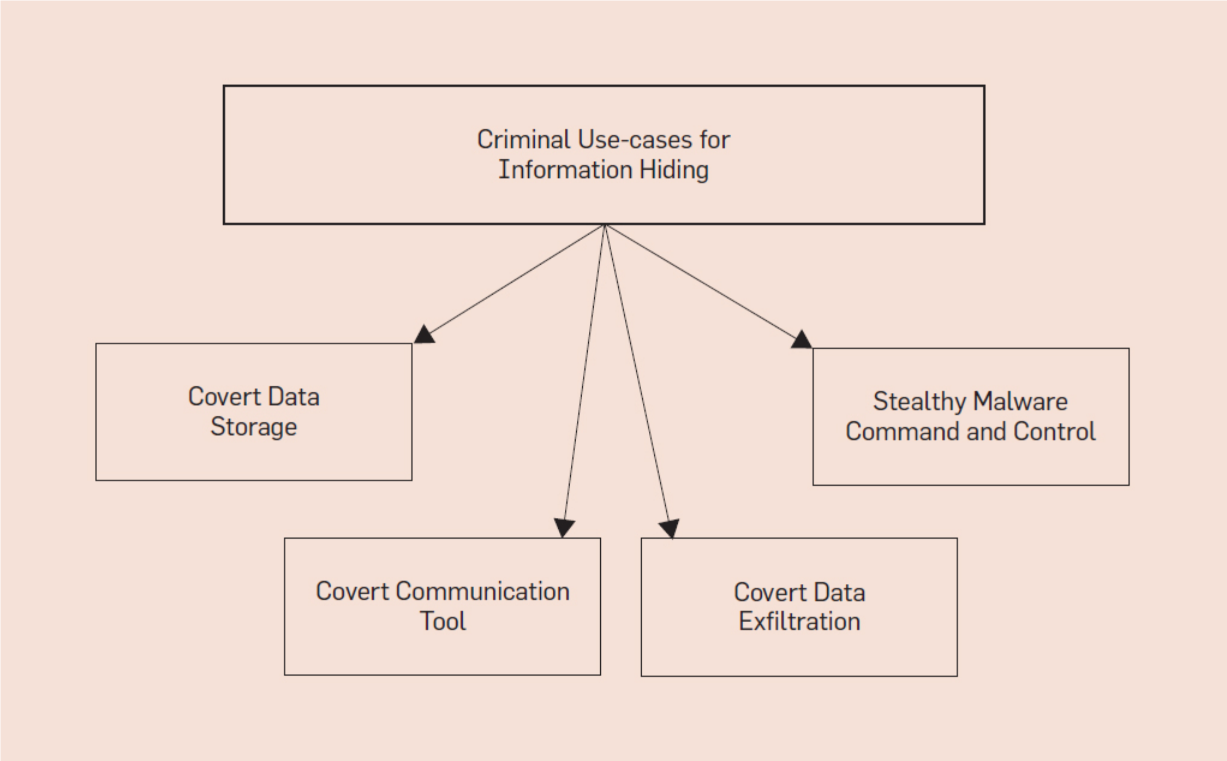
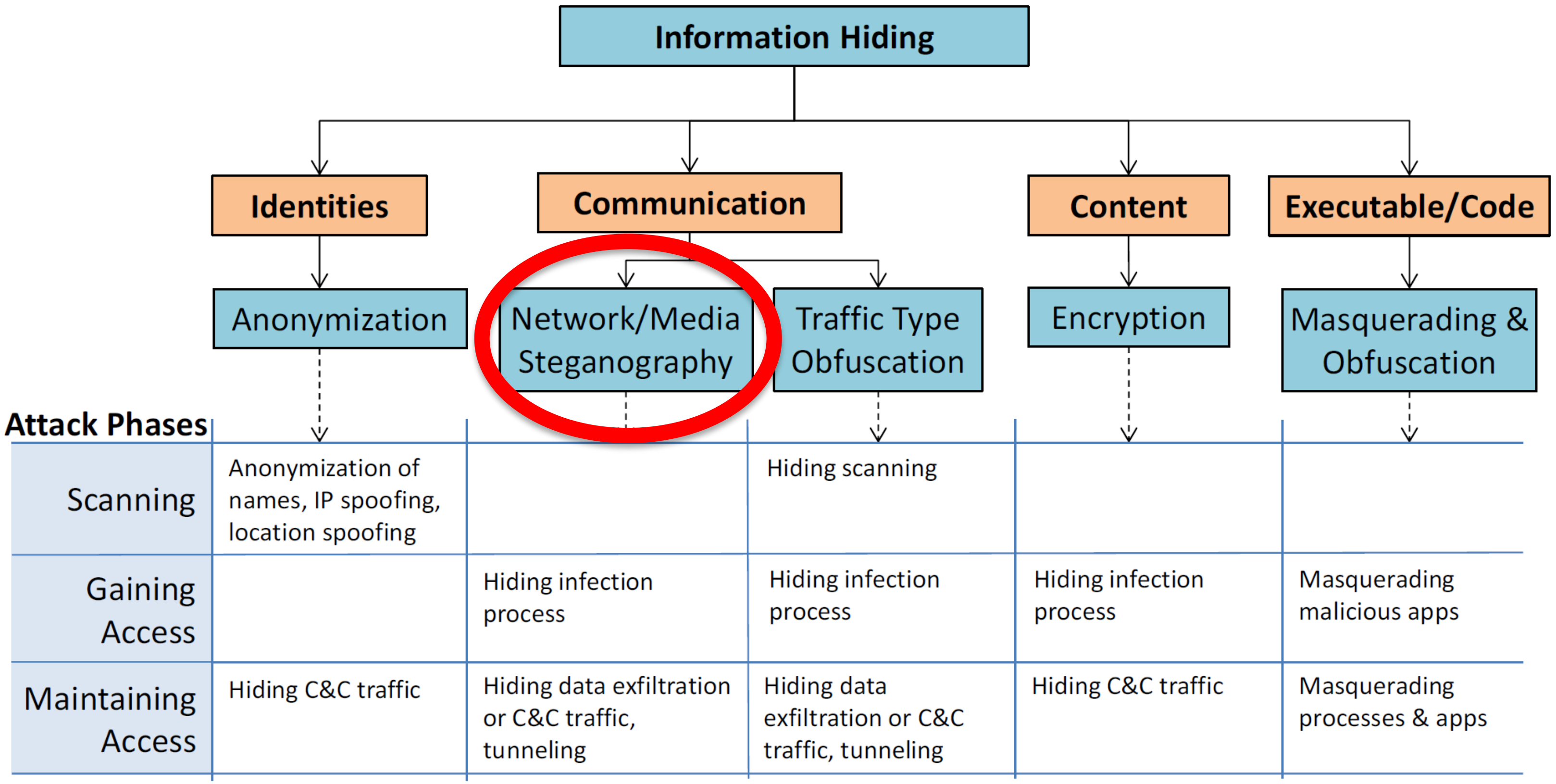

Criminal Use-cases for Information Hiding
Covert Data Storage
Stealthy Malware Command and Control
Covert Communication Tool
Covert Data Exfiltration

Fig.: W. Mazurczyk, S. Wendzel: Information Hiding: Challenges for Forensic Experts, Communications of the ACM, 2018. [link]

Classification of IH techniques and their relation to basic attack phases



Attack Phases	Anonymization	Network/Media Steganography	Traffic Type Obfuscation	Encryption	Masquerading & Obfuscation
Scanning	Anonymization of names, IP spoofing, location spoofing		Hiding scanning		
Gaining Access		Hiding infection process	Hiding infection process	Hiding infection process	Masquerading malicious apps
Maintaining Access	Hiding C&C traffic	Hiding data exfiltration or C&C traffic, tunneling	Hiding data exfiltration or C&C traffic, tunneling	Hiding C&C traffic	Masquerading processes & apps

Figure 1: Classification of hiding techniques and how they are used by malware in the different attack phases

Fig.: K. Cabaj et al.: The New Threats of Information Hiding: the Road Ahead, IT Professional, IEEE, 2018.