Steganography in the World of IoT

Aleksandra Mileva
University "Goce Delčev" in Štip
Republic of Macedonia

ARES Conference
International Conference on Availability, Reliability and Security

IoT-SECFOR 2018
Hamburg, August 27 –30, 2018

What is Steganography?

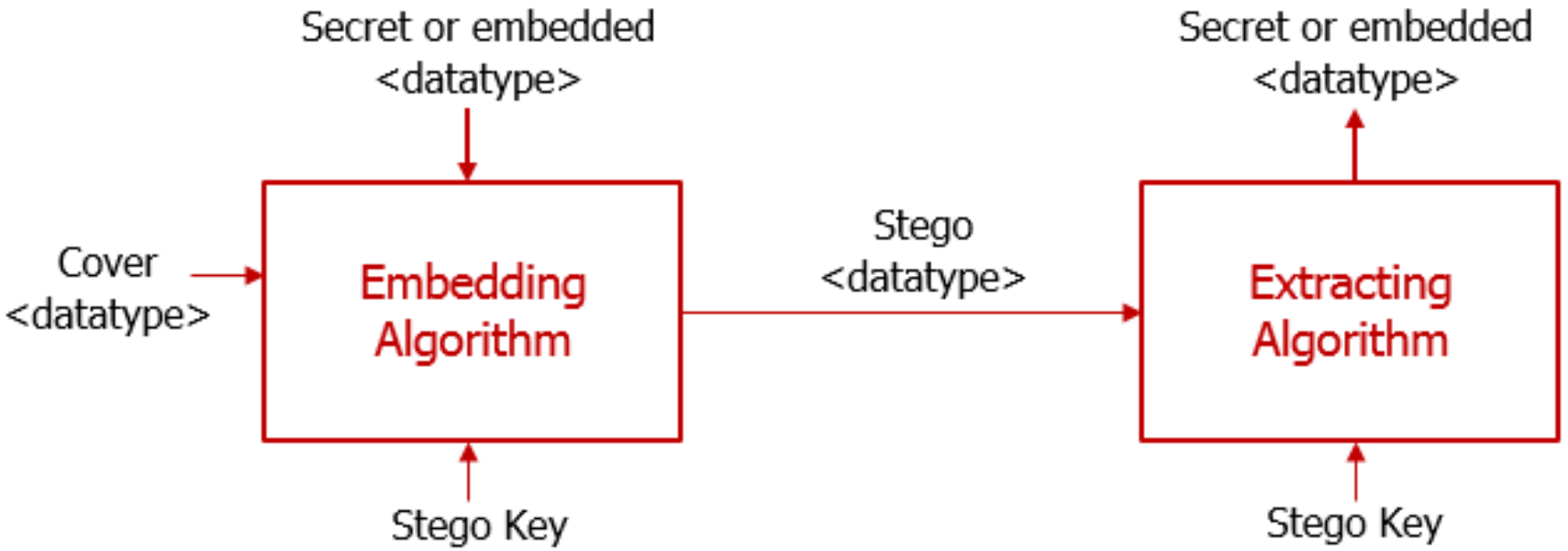
- Steganography is a practice of hiding a message (a.k.a. steganogram) in a legitimate carrier (a.k.a. cover object), so that no one suspects it exists.
  - the presence of the message is hidden.
  - provides only security through obscurity
- Steganalysis
- In the digital steganography the cover object can be:

•text
•image
•video file
•audio file
•other types of files
•network protocol header

•network flow
•file-system metadata
•blockchains
•cyber-physical systems
•cryptographic protocols and schemes
•...

Etymology and Terminology

- Etymology: steganos (“covered”) +graphia (“writing”)
  - first used by Johannes Trithemius (1462-1516)
- Terminology (Pfitzmann, 1996):



History

Histories (**440 B.C**) by Herodotus
Human skin (499 BC, Histiaeus)
Wax tablets (480 BC, Demaratus)

Magiae Naturalis (**1558**) by Giambattista della Porta
Eggshell

(**1550**)
Girolamo Cardano
Cardan grill

Vexierbild (**1535**)
Erhard Schon
Woodcut

Hypnerotomachia Poliphili
(**1499**) Francesco Colonna
Text steganography

(**1939-1945**)
World War II, Germans
Microdots

(**1970s**)
invisible watermarks
on pictures
Digital media files

(1978) Padlipsky, Snow, Karger
Network protocols

(**1999**)
Anderson, Needham, Shamir
OS filesystem

(**2012**)
Wendzel
Cyber-physical system

Animal corpse
(6th century BC, Harpagus)

Wax ball, "la wan"
China

Parchment

Astragal
(4th century BC, Aeneas Tacticus)

Invisible ink
(280-220 BC, Philo of Byzantium)
(43 BC – 17/18 AD, Ovid)
(23-79, Pliny the Elder)
...

Linguistic steganography
(**16th century**)

Music
Schola Steganographica
(**1680**) Gaspar Schott

Newspaper code
(**between 17-19th century**)

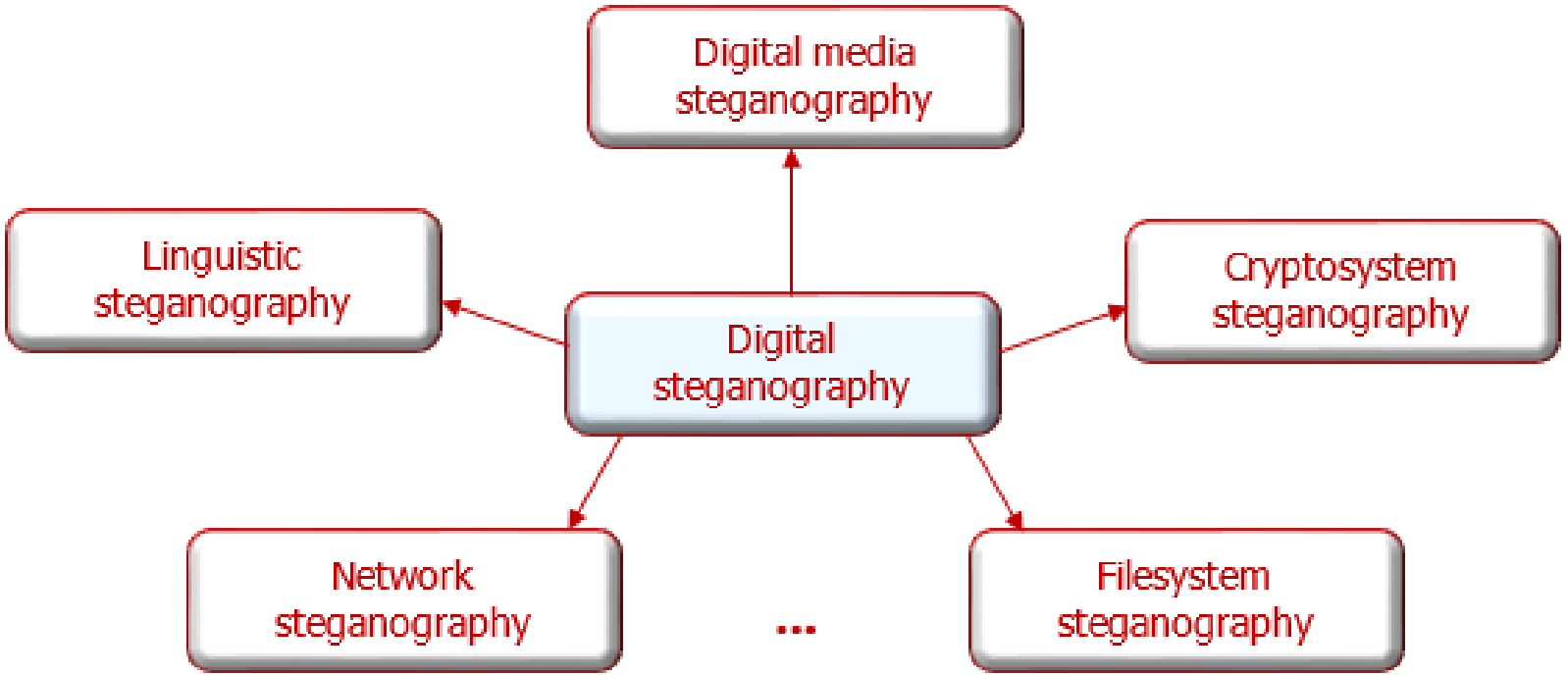
Cryptographic protocol (subliminal channel)
(**1984**) Gustavus Simmons

Printouts
(**end of the 20th century**)

Code
(**2004**) El-Khalil, Keromytis

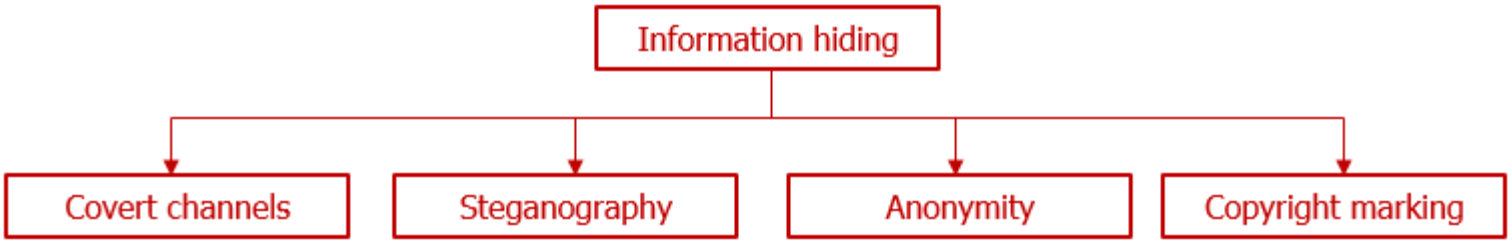
Internet services
(**21st century**)
IP telephony, Skype, BitTorrent
...

Classification of Digital Steganography



Taxonomy

Historical classification (Petitcolas et al., 1999)



Reproduced from (Petitcolas et al, 1999)

Steganography and Covert Channels

- Covert channels
  - those not intended for information transfer at all (Lampson, 1973)
  - can be exploited by a process to transfer information in a manner that violates the systems security policy (DoD, 1985)
  - when a process of a higher level can signal to a process of a lower level by affecting some shared resource (Anderson, 2008) - in the context of multi-level security
  - time vs storage covert channels
  - intentionality of the sender differs covert channels from side channels
- (Mazurczyk et al., 2016)
  - The current distinction between two terms is artificial especially in a communication networks environment.
  - Network steganography techniques create covert channels for hidden communication, but such covert channels do not exist in communication networks without steganography.

Taxonomy

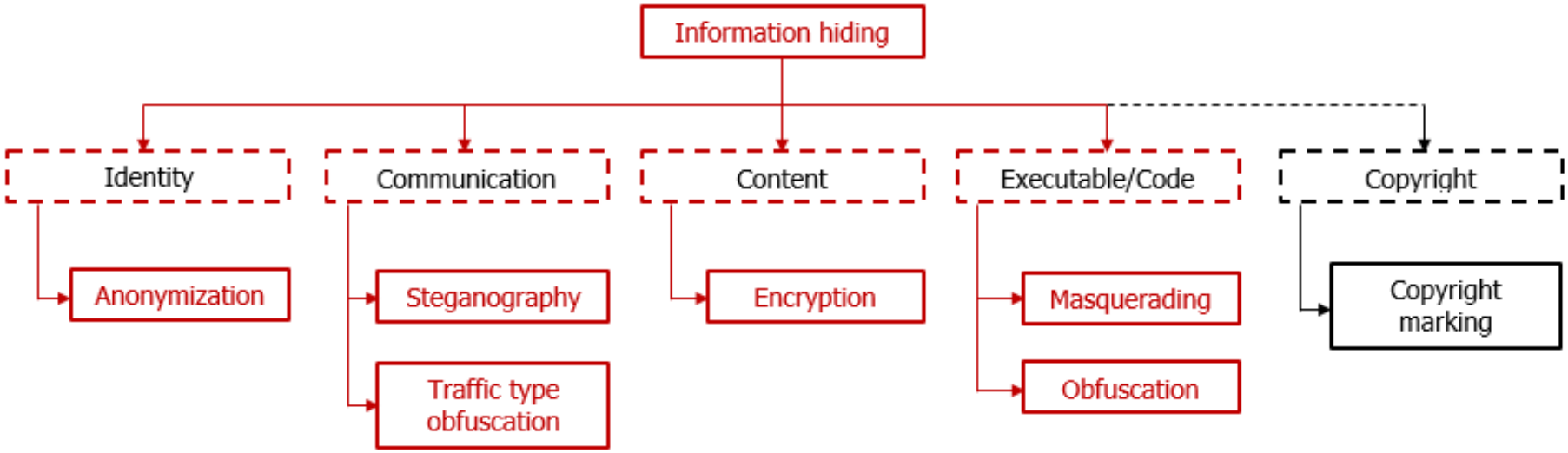
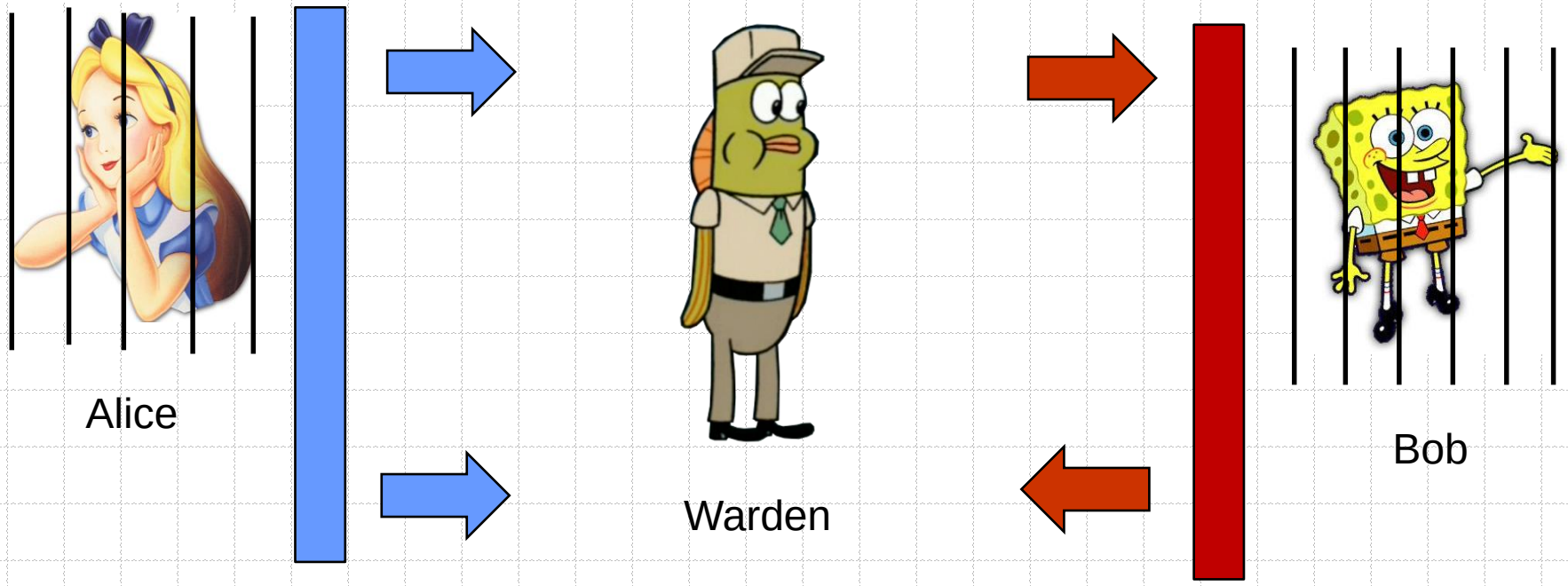


Image source with changes: (Cabaj et al, 2018)

The Prisoners' Problem



- (Simmons, 1984)
- Passive warden – tries to detect the existence of the hidden communication (and content of the steganogram)
- Active warden – modifies the cover object to destroy or replace the steganogram, fabricates own cover objects (malicious warden)

Applications

- Legal vs illegal - traditionally
  - Not quite good, since "legal" requires definition by some jurisdiction, and something which is legal under one jurisdiction may be illegal under another jurisdiction.

White hat applications

- Covert military communication in hostile environment
- Censorship circumvention
- Protection of journalists or whistle-blowers,
- Watermarking of network flows
- Secure network management communication
- Providing QoS for VoIP traffic
- Tracking anonymous peer-to-peer VoIP calls

Black hat applications

- Secret communication between terrorists and criminals
- Sharing of illegal material
- Industrial espionage
- Sophisticated data leakages
- Malware (e.g., hiding C&C communications as in Fakem RAT)

NOAH SHACHTMAN SECURITY 06.28.10 01:11 PM

FBI: SPIES HID SECRET MESSAGES ON PUBLI WEBSITES

The Cyber-Security source

FEATURES | BUYER'S GUIDE | OPINION

November 29, 2014 By Pierluigi Paganini

Security experts have detected an attack against a major

Kaspersky Lab Identifies

Secure | https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-identifies-worrying-trend-in-hackers-using-steganography

Solutions for: Home Products | Small Business 1-50 employees | Medium Business 51-999 employees | Enterprise 1000+ employees

KASPERSKY lab

About Us | Company | Team | Transparency | Press Releases | Press Center | Careers | Sponsorships

Home › About › Press releases

August 3, 2017

Kaspersky Lab Identifies Worrying Trend in Hackers Using Steganography

Researchers find multiple hacking groups are increasingly using the technique to hide stolen information inside images

CUING.ORG

CRIMINAL USE OF INFORMATION HIDING

Home
CUIng main page

About CUIng
More information

Structure
Who we are

Resources
Media releases

Contact
How to join us

STEGANOGRAPHY

to cybercriminals exploitation

About CUIng Initative

Criminal Use of Information Hiding (CUIng) Initative has been officially launched in June 2016 with the support by Europol's European Cybercrime Centre (EC3) to tackle the problem of criminal exploitation of information hiding techniques by working jointly and combining experiences of experts from academia, industry, law enforcement agencies and institutions.

The main objectives of CUIng are to:

- **Raise Awareness**: inform about the threat that information hiding techniques can pose. Increase sensitivity to cybercriminals' information hiding potential exploitation e.g. in companies. Emphasize e.g. how forensic investigations could be impacted and how significantly harder they are when such techniques are utilized.
- **Track Progress**: monitor sophistication and complexity of information hiding techniques found in the wild used by cybercriminals, terrorists and spies.
- **Share Strategic Threat Intelligence**: bring together security professionals from institutions, academics and industry to distribute information and share experience from different angles (security professionals, academics, law enforcements, companies, institutions etc.).
- **Work Jointly**: cooperate and benefit from joint potentials to develop effective countermeasures and

Menu

Home

About CUIng

Structure

Resources

Contact

- (Cabaj et al, 2018) - real-world threats observed in the 2011 – 2017

Network Steganography

- Network steganography describes the methods used for creating covert channels in communication networks (Mazurczyk et al., 2016)

- Carrier is one or more overt network flows.

- The best carriers must have two features:

1. they should be popular, so their utilization should not be considered as an anomaly.
2. modification of the carrier with the steganogram should not be "visible" to unaware third parties.

- If no traffic captured, nothing left for forensics analysis!

Why is Easy to use Network Flows as Carriers?

- Network protocols usually have:
  - a random value fields
  - an unused fields
  - there is no strict rule how to obtain new values for some fields
  - a feature that is not mandatory
  - a feature that has dual nature, i.e. , the same feature can be obtained in more than one way
  - …
- Additionally, the communication channel is not perfect, so data can be embedded by mimicking usual errors and network anomalies (Zielinska et al., 2014).
- Steganography-free protocols are probably practically impossible to design, without limiting their functionality!!!

Research Challenge 1

- Build some automated checking tool, that will help protocol designers to create almost steganography-free protocols, by eliminating unnecessary redundancy and dealing with under-definition in network protocols.

Network Steganography

Hiding patterns

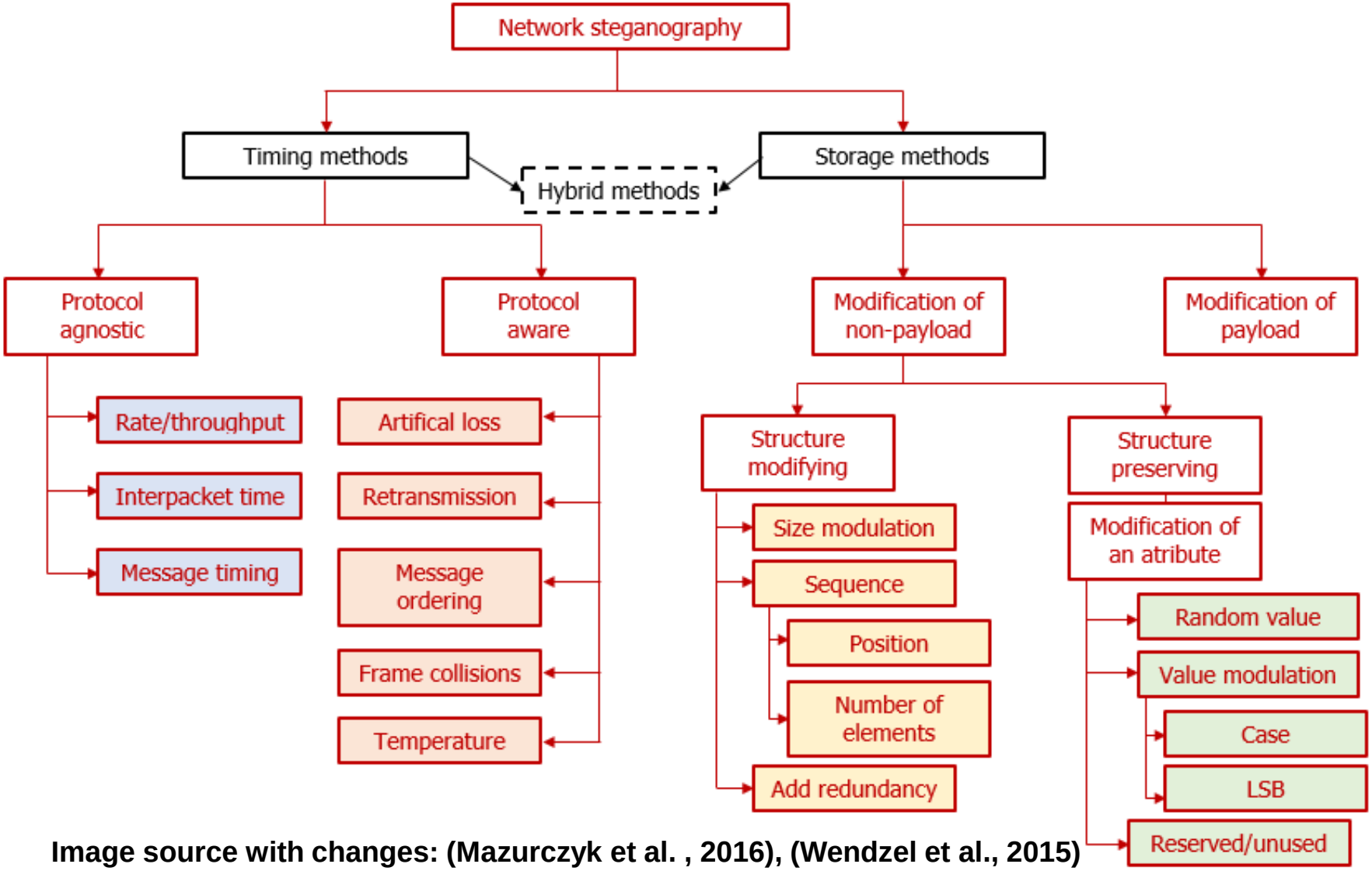


Image source with changes: (Mazurczyk et al. , 2016), (Wendzel et al., 2015)

Steganography + IoT

IoT Ecosystem

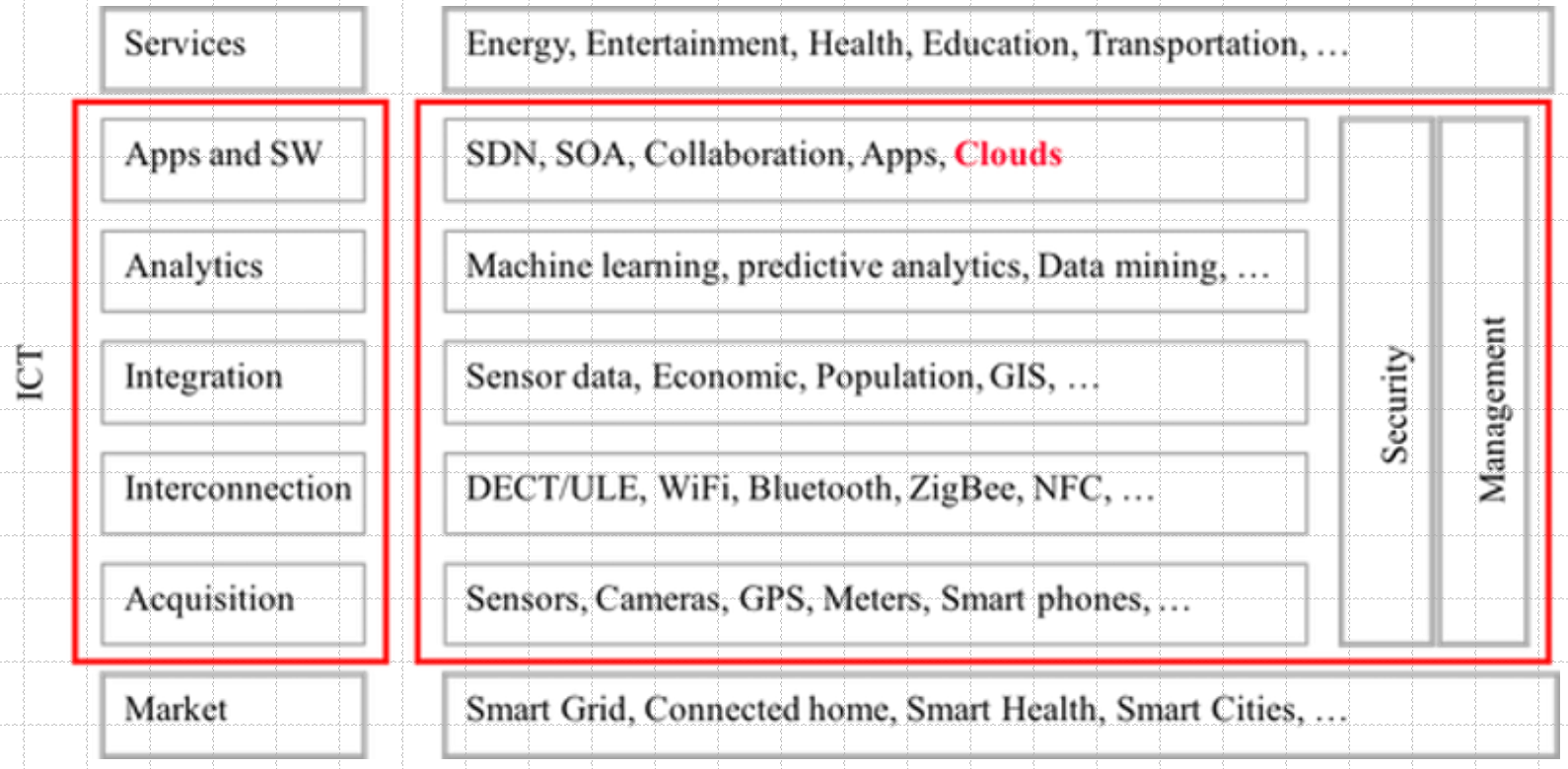


Image source : (Salman et al. , 2017)

- Cyber-Physical Systems (CPSs) - integrations of computation with physical processes (Lee, 2008)
  - smart homes and buildings, smart grid, autonomous cars, autopilot, industrial control systems, e-Health equipment, robotics system, etc.

Smartphones Case

- Steganography in smartphones is studied a lot.
- All classes of digital steganography are present.

Measured bandwidth between 0,22 and 3837 bps up to 2014!!!
(Mazurczyk et al., 2014)

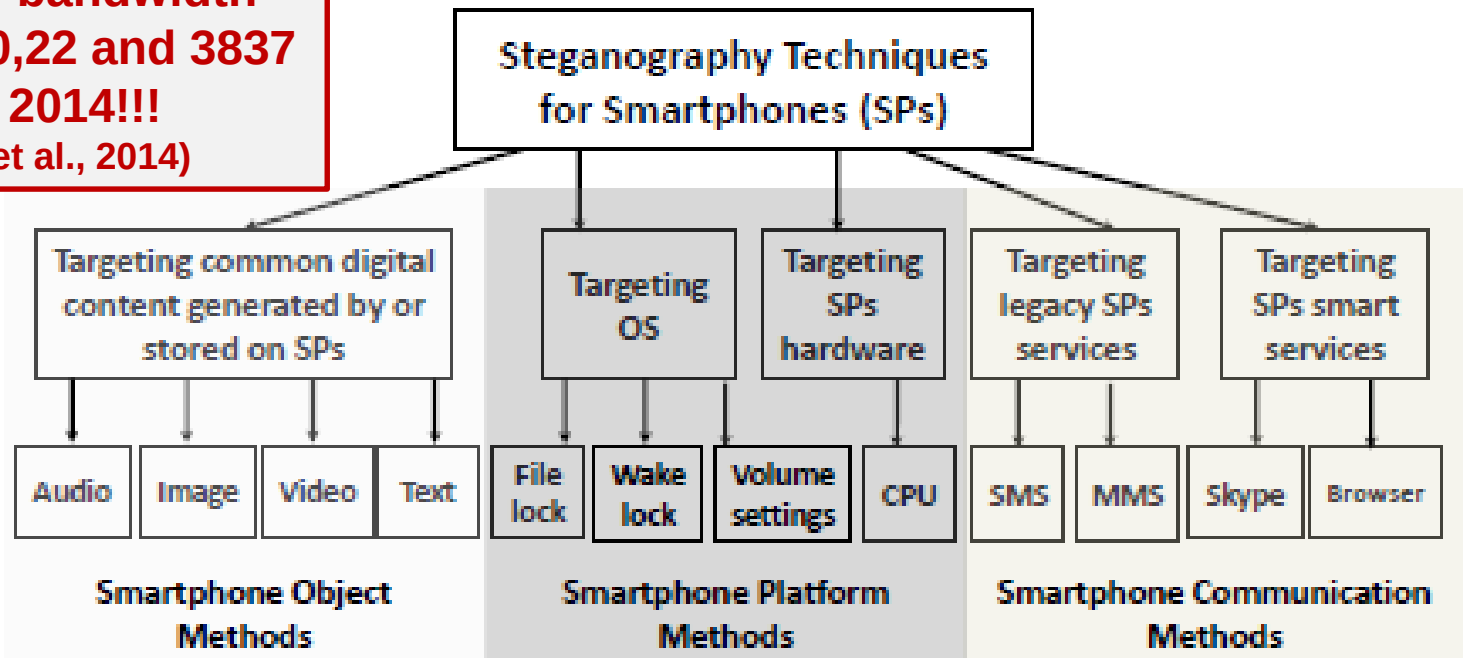
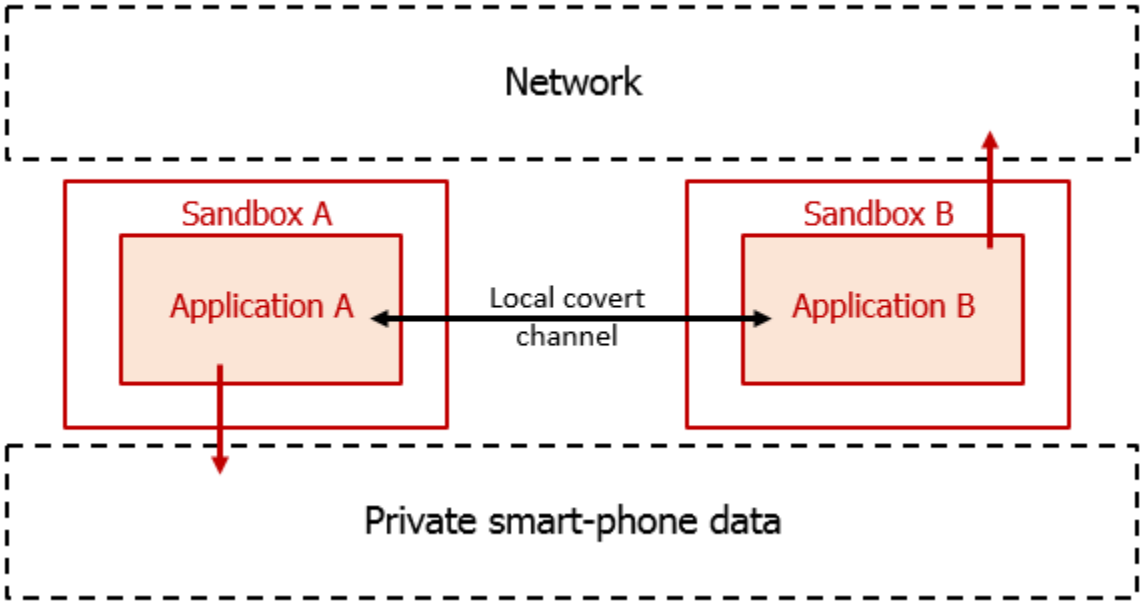


Image source : (Mazurczyk et al., 2014), Period: 2005-2014

Smartphones Case

Covert channels between colluding applications

- Smartphone OSs implement a permission-based security model (capability model).
- Use of local covert channels for Android-based devices



- Soundcomber (Schlegel et al, 2011)
  - vibration settings, volume settings, screen state, file lock

Resource-constrained IoT Devices and Networks

- Many resource-constrained devices such as RFID tags, industrial controllers, sensor nodes and smart cards.
  - 4-bit, 8-bit, 16-bit and 32-bit microcontrollers
    - small ROM and RAM, e.g., TI COP912C - 768 B ROM, 64 B RAM
  - small memory in RFID tags
    - e.g., ISO RFID HF Tag with memory at least 128 B
- Low-Power Lossy Networks
  - data rates of order of 100 kbps and less,
  - high packet loss (~ 20%)

What can we do?

- Can we apply the network steganography?

Some IoT Protocols

IPv6 over Bluetooth Low Energy

Bluetooth Low Energy

SASL

LOADng

G.9959

CORPL

OSCORE

CoAP

Wightless

MQTT

TLS/DTLS

COSE

TR-069

RPL

AMQP

6LoWPAN

IEEE 802.15.4

IEEE 802.11 AH

LOAD

STOMP

LTE-A

IEEE 1905.1

LWM2M

XMPP

IPv6 over G.9959

E-CARP

LoRaWAN

KNX

Zigbee Smart Energy

HomePlug

OAuth 2.0

6Lo

OMA-DM

SMQTT

ACE-OAuth

Z-Wave

WirelessHART

CARP

CTP

DDS

ISO/IEC/IEEE 18883

IEEE 1451

DASH7

6TiSCH

DECT/ULE

BACnet

Network Steganography in IoT

- **Yes** - easy to apply

Example 1 – Building Automation and Control Networking Protocol - BACnet (Wendzel et al., 2012)

- 2 storage and 1 timing covert channels

1.1 A Message-Type based storage covert channel

- Send *Who-Is-Router-To-Network* for binary 1
- Send *I-Am-Router-To-Network* for binary 0

1.2 A Parameter-based storage covert channel

- 16-bit *DNET* in the *Who-Is-Router-To-Network*

1.3 A timing covert channel

- with inter packet gaps

- Suggested protection: implementing multi-level security in BACnet firewall router (BFR)

Network Steganography in IoT

Example 2 – Extensible Messaging and Presence Protocol - XMPP (RFC 6120, 6121), (Reshad et al., 2013)

```
<message from='adam@test.com' to='bart@test.com' type='chat'
id='7df1ddbe'><body>Message.</body></message>
```

2.1 Type Attribute-based storage covert channel

- case, presence/absence or value

2.2 id Attribute-based storage covert channel

- case or value

2.3 xml:lang Attribute-based storage covert channel

- presence/absence or value

2.4 Message body content-based storage covert channel

- leading and trailing space redundancy, synonyms, spelling mistakes

Network Steganography in IoT

Example 3 – Constrained Application Protocol - CoAP (RFC 7252), (Mileva et al., 2018)

- 6 storage and 2 timing covert channels

3 Storage covert channel using conditional requests

If somebody knows for sure that given condition C1 is fulfilled (for example, the resource is created or deleted in previous message) and other C2 is not fulfilled, using either of If-Match and If-None-Match options:

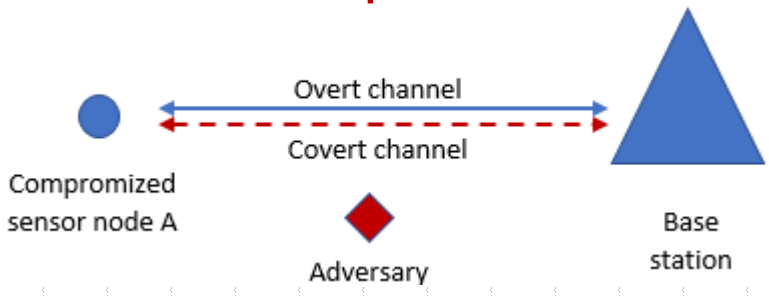
- sending a given message without fulfilled condition to be binary 1 (e.g., If-Match + C2), and
- sending a given message with fulfilled condition (e.g., If-Match + C1) to be binary 0.

Network Steganography in IoT

Wireless Sensor Networks case, covert channels independent from the used protocols

Example 4 (Tuptuh et al., 2015)

- 2 covert channels



4.1 Covert channel with modulation of transmission power

- which impacts the RSSI/LQI of a message
- experiments: Orisen nodes, with a user-selectable transmission power level that can range from -30 dBm to +4 dBm (power level 0 to 18), giving ranges from about 50cm to around 70m outdoors.
  - power level 18 – binary 0, while 17 – binary 1
  - cover message encoded with Hamming (7, 4) + preamble bits

4.2 Storage covert channel with modulated sensor readings

- LSBs of encrypted sensor readings are the cover bits
- While (LSB $\neq$ cover bit)
  - add small offset to the sensor reading (e.g., temperature)
  - encrypt the value

Network Steganography in IoT

Covert channels on the physical layer that need a new pattern

Example 5

4.1 Covert channel with modulation of transmission power (Tuptuh et al., 2015)

5.1 Covert channel with Radio Frequencies – AirHopper (Guri et al., 2014)

5.2 Covert channel with Electromagnetic emission from USB– USBee (Guri et al., 2016)

One solution is to change the pattern Temperature into the pattern EM Emanation, because thermal radiation is a form of electromagnetic emanation!!!

Steganography in the Applications above the Network Protocols

Wearables case

- (Denney et al., 2016) A novel storage covert channel that sends data to other applications, through the use of notifications that are normally displayed on the status bar of an Android device.
- A notification listening service on the wearables needs to be implemented.
- Notifications can be shared across multiple devices
- Data are hidden in the 32-bit notification ID numbers
- Their exchange with notify and cancel functions.
  - If notifying function is immediately followed by the canceling function, the notification is never displayed to the user although it can be seen in the log files, so the communication is hidden from the user that wear the device.

What can we do?

- Can we apply the network steganography?

Yes

- Can we apply the cryptosystem steganography?

Cryptosystem Steganography in IoT

- Security in IoT
  - TLS/DTL, OAuth 2.0, SASL, ACE-OAuth, ISO/IEC/IEEE 18883:2016, OSCORE, COSE...
- **Concise Binary Object Representation (CBOR)** is a data format designed for small code size and small message size.
- Most relevant security IETF standards or drafts for IoT:
  - COSE (CBOR Object Signing & Encryption) – RFC 8152
  - ACE-OAuth (Authorization and Authentication in Constrained Environments using the OAuth 2.0) - draft
  - OSCORE (Object Security for CORE) - draft
- Known subliminal channels in signature algorithms: DSA, ECDSA, EdDSA, ElGammal, RSA, etc.
  - Suggested subliminal-free versions for DSA and ECDSA
    - not used in practice?

Cryptosystem Steganography in IoT

- TLS/DTLS uses RSA, DSA, ECDSA and EdDSA (in v1.3)
  - CoAP is secured using DTLS over UDP.
  - Recommendation: TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
- Authentication SASL mechanisms supports RSA, DSA and ECDSA as signature algorithms.
- COSE uses ECDSA and EdDSA

Research Challenge 2

- Examine new IoT security solutions (standards and draft versions) for existence of novel subliminal channels, or other novel covert channels.

What can we do?

- Can we apply the network steganography?

Yes

- Can we apply the cryptosystem steganography?

Yes

- Can we secretly store data in the CPSs?

CPS - Building Automation Systems

secret data storage

- (Wendzel et al., 2017) - one can places hidden data in the CPS environment by slightly modifying some of its components.
  - Actuators, sensors, controllers, and monitoring equipment
- Scenario – two agents use the airport BAS

Two approaches:

1. utilization of unused registers – trivial
   - e.g., temperature sensor *Used Maxim Integrated Products, Inc., 1-Wire DS18B20* with two 8-bit alarm registers (min/max temperature) and 0x4b46 default value,
   - accept values between –55 and +125°C $\Rightarrow$ not all 8 bits can be utilized
   - serial numbers of sensors can be used for sort hiding data in several components

CPS - Building Automation Systems

secret data storage

2. modulation of actuator states

- actuator states change and influence the physical environment, i.e. steganographic operations may not be robust and be easily detectable and thus need a reasonable storage strategy
- BACnet (ISO standard 16484-5:2014)
- BACnet devices typically allow to store between 1 and 16 bits per present value property.

Small amount of data stored within a single smart building!!!

e.g., heating value
of 80% binary "0"
of 79% binary "1"

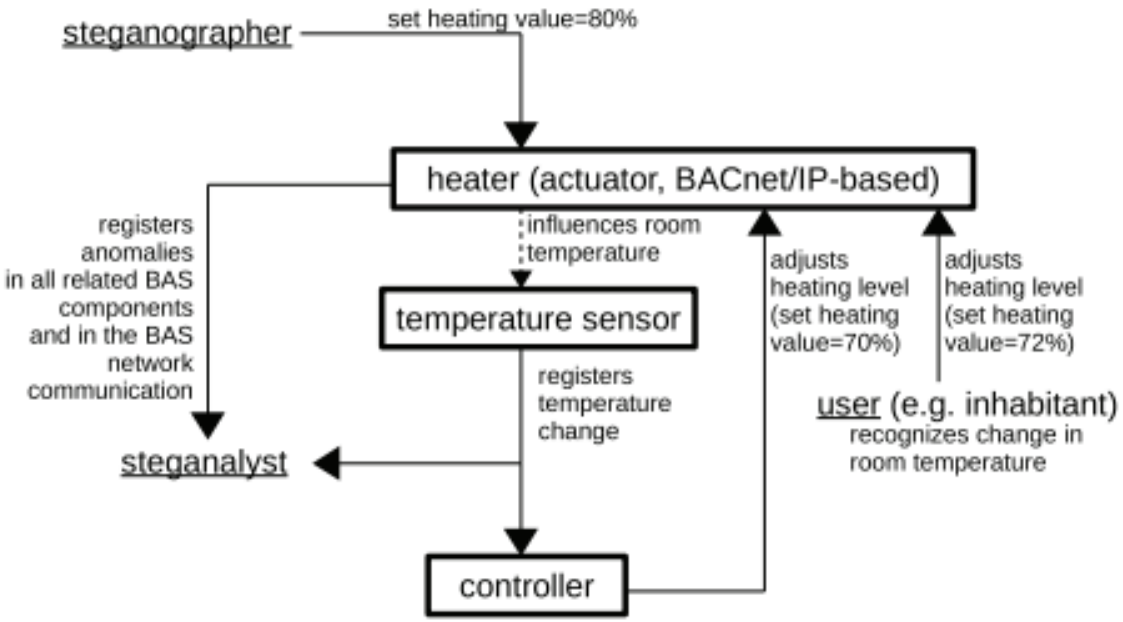


Image source: (Wendzel et al., 2017)

Research Challenge 3

- Examine the secret data storage capacity and possibilities of other CPSs, e.g., autonomous cars and e-Health equipment.
- These CPSs are of special type, because they are mobile and can be moved by people from one place to another!!!

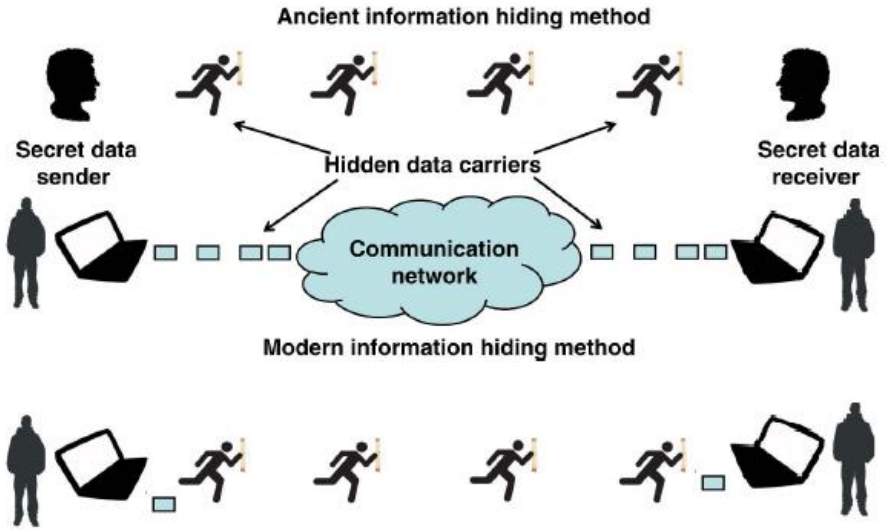


Image source with changes: (Mazurczyk et al. , 2016)

What can we do?

- Can we apply the network steganography?

Yes

- Can we apply the cryptosystem steganography?

Yes

- Can we secretly store data in the CPSs?

Yes

- Can we apply the filesystem steganography?

Filesystem Steganography in IoT

- IoT OSs
  - RIOT OS, Microsoft Windows 10 for IoT, WindRiver VxWorks, Google Brillo, ARM Mbed OS, Embedded Apple iOS, Nucleus RTOS, ...
- Potentially, it can be used in IoT devices with embedded multiple-time programmable non-volatile memory, embedded Flash memory, external Flash memory, eMMC memory, or similar.

What can we do?

- Can we apply the network steganography?

Yes

- Can we apply the cryptosystem steganography?

Yes

- Can we secretly store data in the CPSs?

Yes

- Can we apply the filesystem steganography?

Promising

- Can we use steganography for securing IoT?

Securing IoT Devices using Steganography

- Not successful yet!!!
- e.g. (Yin et al., 2015)
- *Scenario*: image face recognition for authentication in smart homes with IP camera for unlocking doors.
  - with eavesdropping of home LAN, the attacker will obtain the image
- *Idea*: IP camera takes the picture of the resident, and hides it in other image, by some steganographic method
  - Stego image is sent to the authentication server
- Many problems!!!
  - e.g., Replay attacks
- Cannot replace cryptography with steganography in IoT!!!
- Also, similar problems with suggested solutions that combine steganography and cryptography.

Securing IoT Devices using Steganography

- (Islam et al., 2017)
- Authenticating geolocation of IoT devices – important
  - Device relocation can be an attack
- Uses ICMP covert channels for authenticating Internet packet routers as an intermediate step towards proximal geolocation of IoT devices.
- Inherited weaknesses of IP-based geolocation techniques
  - many Internet clients may stay behind proxies or firewalls, so, any external network searching for a client IP address may actually find a proxy, which may be erroneous for location mapping.

What can we do?

- Can we apply the network steganography?

Yes

- Can we apply the cryptosystem steganography?

Yes

- Can we secretly store data in the CPSs?

Yes

- Can we apply the filesystem steganography?

Promising

- Can we use steganography for securing IoT?

Not successful yet

What about Steganalysis?

- Steganalysis is much more difficult than steganography!!!
- The existing solutions, like traffic normalizers and similar active wardens, can be applied for IoT case, also.
- In steganography, proactive solutions are more promising than reactive.

References

- Anderson, R.: Security Engineering - A Guide to Building Dependable Distributed Systems. Wiley, (2008).
- Cabaj, K., Caviglione, L., Mazurczyk, W., Wendzel, S., Woodward, A., Zander, S.: The New Threats of Information Hiding: the Road Ahead. IEEE IT Professional 20 (3), (2018).
- Denney, K., Uluagac, A. S. , Akkaya, K., Bhansali, S.: A novel storage covert channel on wearable devices using status bar notifications. In CCNC 2016, pp. 845-848 (2016).
- Department of Defense, Department of defense trusted computer system evaluation criteria, Technical Report DOD 5200.28-ST., Supersedes CSC-STD-001-83, December 1985
- Guri, M., Kedma, G., Kachlon, A., Elovici, Y.: AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies. In MALWARE 2014, (2014).
- Guri, M., Monitz, M., Elovici, Y.: USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB. IEEE, pp. 264-268, (2016).
- Islam, M.N., Patil, V.C., Kundu, S.: Determining proximal geolocation of IoT edge devices via covert channel. In ISQED 2017, pp. 196-202, (2017).
- Lampson, B.W.: A Note on the Confinement Problem, Comm. ACM, (1973).
- Lee, E.A.: Cyber physical systems: Design challenges. In 11th IEEE ISORC 2008, pp. 363–369, (2008).
- Mazurczyk, W., Caviglione, L.: Steganography in Modern Smartphones and Mitigation Techniques. IEEE Communications Surveys & Tutorials 17 (1), pp. 334 - 357, (2014).
- Mazurczyk, W., Wendzel, S., Zander, S. et al.: Information Hiding in Communication Networks, Wiley / IEEE Comp. Soc. Press, (2016).
- Mileva, A., Velinov, A., Stojanov, D.: New Covert Channels in Internet of Things. SECURWARE 2018 (acc).
- Petitcolas, F.A.P., Anderson, R., Kuhn, M.G.: Information Hiding – A Survey, Proc. IEEE, (1999).
- Pfitzmann, B.: Information Hiding Terminology. 1st Information Hiding Workshop, Springer, (1996).

References

- Reshad, P., Hernandez-Castro, J.: Steganography using the Extensible Messaging and Presence Protocol (XMPP). In Computing Research Repository arXiv:1310.0524 (2013).
- Salman, T., Jain, R.: A Survey of Protocols and Standards for Internet of Things. Advanced Computing and Communications 1(1), (2017).
- Schlegel, R., Zhang, K., Zhou, X., Intwala, M., Kapadia, A., Wang, X.: Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones. In NDSS '11, pp. 17–33, (2011).
- Simmons, G. J., The prisoners problem and the subliminal channel, In Crypto '83, Advances in Cryptography, pp. 51-67, Springer, (1984).
- Tuptuk, N., Hailes, S.: Covert channel attacks in pervasive computing. In IEEE PerCom, pp. 236–242, (2015).
- Wendzel, S.: Covert and Side Channels in Buildings and the Prototype of a Building-aware Active Warden. IEEE ICC, pp. 6753-6758, (2012).
- Wendzel, S., Kahler, B., Rist, T.: Covert Channels and their Prevention in Building Automation Protocols – A Prototype Exemplified Using BACnet, GreenCom 2012 / iThings 2012 / CPSCom 2012, part of 2nd Workshop on Security of Systems and Software Resiliency, pp. 731-736, Besançon, France, IEEE, 2012.
- Wendzel, S., Zander, S., Fechner, B., Herdin, C.: Pattern-based Survey and Categorization of Network Covert Channel Techniques. Computing Surveys 47(3), pp. 50:1-26, ACM, (2015).
- Wendzel, S., Mazurczyk, W., Haas, G.: Don't You Touch My Nuts: Information Hiding in Cyber-physical Systems. IEEE SPW 2017, pp. 29-34, (2017).
- Yin, J.H.J., Fen, G.M., Mughal, F., Iranmanesh, V.: Internet of Things: securing data using image steganography. In 3rd International Conference on Artificial Intelligence, Modelling and Simulation, (2015).
- Zielinska, E., Mazurczyk, W., Szczypiorski, K.: Trends in Steganography. Communications of the ACM, 57 (2) pp. 86-95, (2014).

Thank you for your attention!!!