UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Lecture 3- Introduction to Security & Privacy for IoT

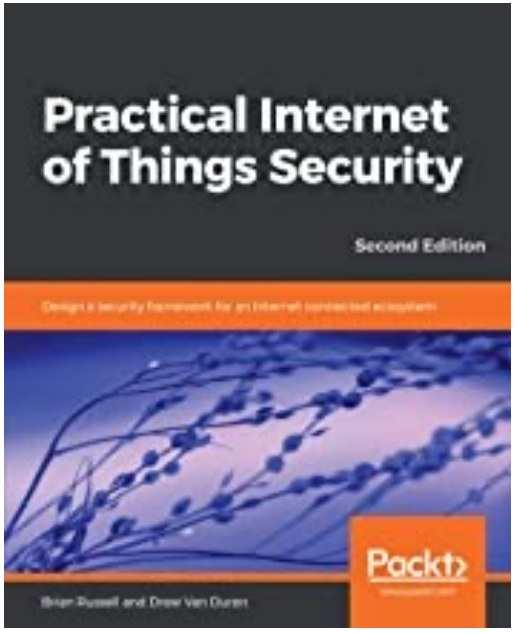
Prof. Esposito Christian

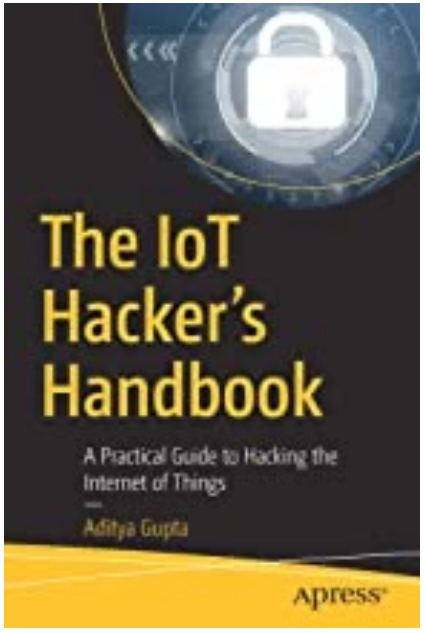
::.. Summary

- Definitions of Security and Privacy, and their Properties
- Introduction to IoT Vulnerabilities and Attacks
- Privacy Issues
- IoT Forensics

::.. References

- Brian Russell, Drew Van Duren, “Practical Internet of Things Security: Design a security framework for an Internet connect-ed ecosystem”, Packt Publishing; 2ª edizione - Novembre 2018;
- Aditya Gupta, “The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things”, Apress - Aprile 2019.





::.. Key Lectures (1/4)

- Neshenko, Nataliia, et al., "Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations", IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2702-2733, thirdquarter 2019.
- Alaba, Fadele Ayotunde, et al., "Internet of Things security: A survey", Journal of Network and Computer Applications, vol. 88, pp. 10-28, Giugno 2017.
- Yang, Yuchen, et al., "A survey on security and privacy issues in Internet-of-Things", IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, Ottobre 2017.
- Mosenia, Arsalan, and Niraj K. Jha, "A comprehensive study of security of internet-of-things", IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586-602, Ott.-Dic. 2016.

::.. Key Lectures (2/4)

- Lin, Jie, et al., "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications", IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, Ottobre 2017.
- Ammar, Mahmoud, Giovanni Russello, and Bruno Crispo, "Internet of Things: A survey on the security of IoT frameworks", Journal of Information Security and Applications, vol. 38, pp. 8-27, Febbraio 2018.
- Porambage, Pawani, et al., "The quest for privacy in the internet of things", IEEE Cloud Computing, vol. 3, no. 2, pp. 36-45, Mar.-Apr. 2016.

::.. Key Lectures (3/4)

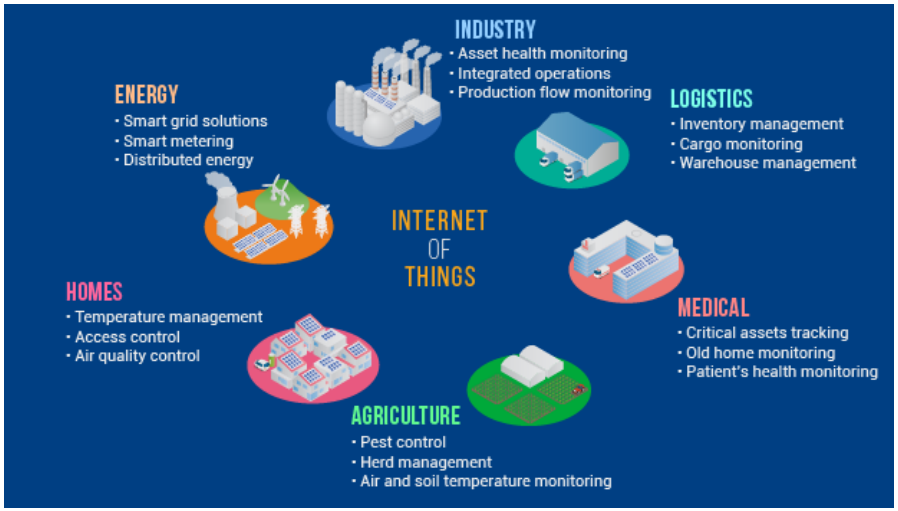
- Stellios, Ioannis, et al. "A survey of Iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services", IEEE Communications Surveys & Tutorials, vol. 20, n. 4, pp. 3453-3495, 2018.
- Alnaeli, Saleh M., et al. "Vulnerable C/C++ code usage in IoT software systems", Proceedings of the IEEE 3rd World Forum on Internet of Things (WF-IoT), 2016.
- Alnaeli, S., et al. "Source Code Vulnerabilities in IoT Software Systems», *Advances in Science, Technology and Engineering Systems Journal, vol.* 2, no. 3, pp. 1502-1507, 2017.

::.. Key Lectures (4/4)

- M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues", in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1191-1221, Secondquarter 2020.
- H. M. A. van Beek, E. J. van Eijk, R. B. van Baar, M. Ugen, J. N. C. Bodde, A. J. Siemelink, "Digital forensics as a service: Game on", Digital Investigation, vol. 15, pp. 20-38, December 2015

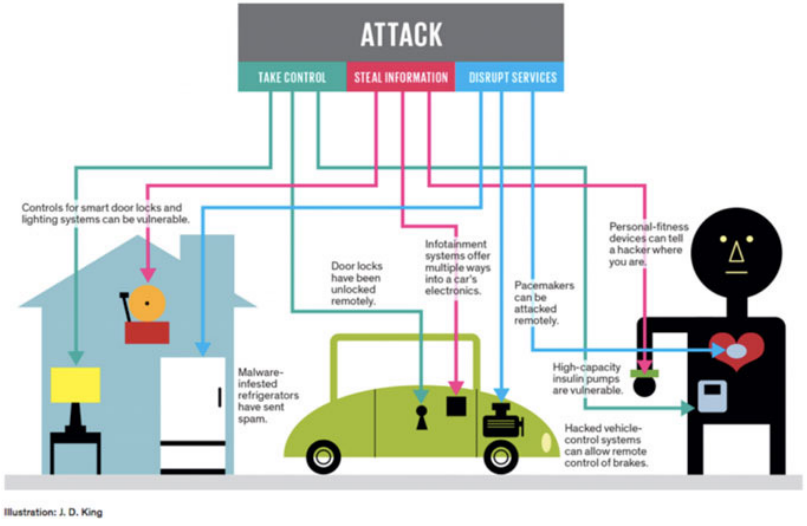
Security & Privacy

::.. Introduction (1/9)



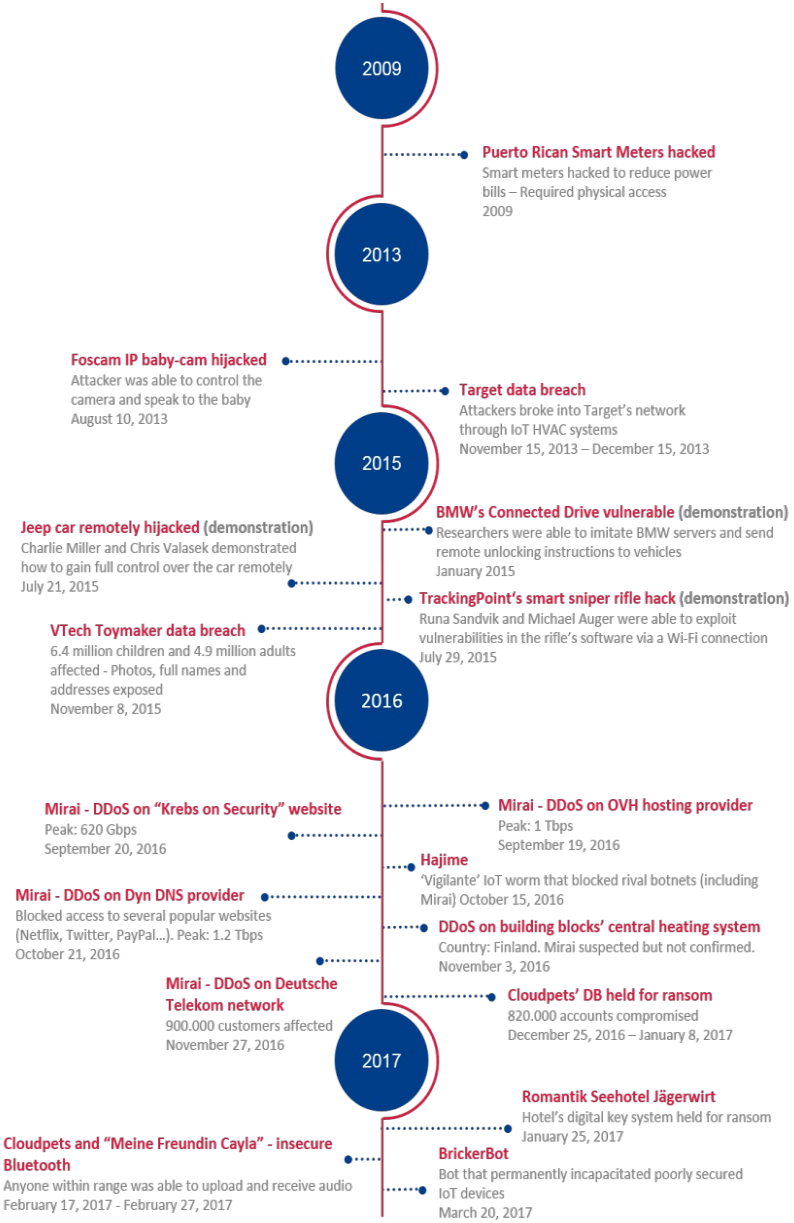
IoT-based systems may manage a huge amount of information and be used for services ranging from industrial management to health monitoring.

This has made the IoT paradigm an interesting target for a multitude of attackers and adversaries.



Potential attackers might be interested in stealing sensitive information and/or compromising IoT components. It can exploit the infected devices to spy on a person of interest or to conduct an attack on a large scale.

::.. Introduction (2/9)



The number of security threats targeting IoT devices has increased over the last years.

- Given the ever wider penetration of IoT across the entire spectrum of daily activities and critical infrastructures, the occurrence of cybersecurity incidents is bound to have an increasing rate.

::.. Introduction (2/8)

It is important to understand the characteristics that define security. Traditionally, security requirements are broken down into three main categories:

1. **Confidentiality** entails applying a set of rules to limit unauthorized access to certain information. It is crucial for IoT devices because they might handle critical personal information.
2. **Integrity** is also necessary for providing a reliable service. The device must ensure that the received commands and collected information are legitimate.
3. **Availability** is essential for providing a fully-functioning Internet-connected environment. It ensures that devices are available for collecting data and prevents service interruptions.

::.. Introduction (3/8)

The CIA-triad does not cover new threats that emerge in the collaborative de-perimeterised environments. The IAS-octave has been proposed as an extension to CIA triad:

1. **Confidentiality** - Ensuring that only authorized users access the information;
2. **Integrity** - Ensuring completeness, accuracy, and absence of unauthorized data manipulation;
3. **Availability** - Ensuring that all system services are available, when requested by an authorized user;
4. **Accountability** - An ability of a system to hold users responsible for their actions;
5. **Auditability** - An ability of a system to conduct persistent monitoring of all actions;

::.. Introduction (4/8)

6. **Trustworthiness** - An ability of a system to verify identity and establish trust in a third party;
7. **Non-repudiation** - An ability of a system to confirm occurrence/non-occurrence of an action;
8. **Privacy** - Ensuring that the system obeys privacy policies and enabling individuals to control their personal information.

Secure thing: A thing that meets all of the abovementioned security requirements.

::.. Introduction (4/8)

6. **Trustworthiness** - An ability of a system to verify identity and establish trust in a third party;
7. **Non-repudiation** - An ability of a system to confirm occurrence/non-occurrence of an action;
8. **Privacy** - Ensuring that the system obeys privacy policies and enabling individuals to control their personal information.

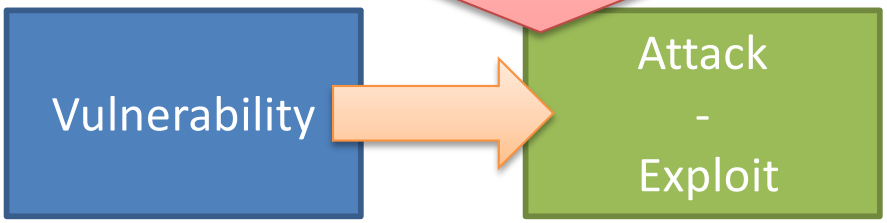
A weakness in some aspects or features of a system that makes an exploit or damage possible. This may be because of poor design, configuration mistakes, or inappropriate and insecure coding techniques. It can be identified and corrected.

Vulnerability

::.. Introduction (4/8)

6. **Trustworthiness** - An ability of a system to verify identity and establish trust in a third party;
7. **Non-repudiation** - An ability of a system to confirm occurrence/non-occurrence of an action;
8. **Privacy** - Ensuring that the system obeys privacy policies and enabling individuals to control their personal information.

An action taken by using one or more vulnerabilities to realize a threat.



::.. Introduction (4/8)

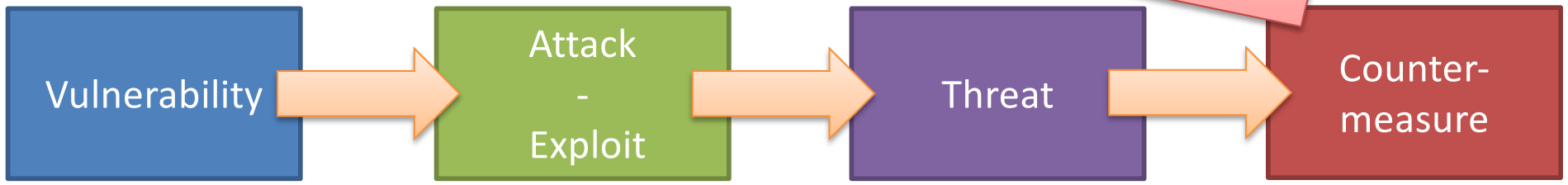
6. **Trustworthiness** - An ability of a system to verify identity and establish trust in a third party;
7. **Non-repudiation** - An ability of a system to confirm occurrence/non-occurrence of an action;
8. **Privacy** - Ensuring that the system obeys privacy policies and enabling individuals to control their personal information.

A negative effect or undesired event. A potential occurrence, often best described as an effect that might damage or compromise an asset or objective. It may or may not be malicious in nature, and can be identified but cannot be controlled.

::.. Introduction (4/8)

6. **Trustworthiness** - An ability of a system to verify identity and establish trust in a third party;
7. **Non-repudiation** - An ability of a system to confirm occurrence/non-occurrence of an action;
8. **Privacy** - Ensuring that the system obeys privacy policies and enabling individuals to control their personal information.

Addresses a vulnerability to reduce the probability of an attack or the impact of a threat. They do not directly address threats; instead, they address the factors that define the threats.



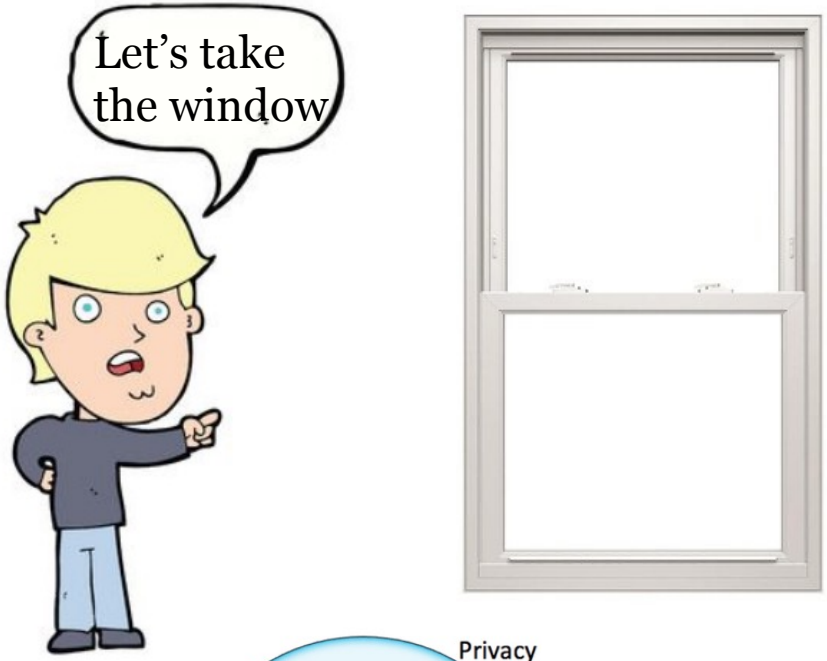
::.. Introduction (5/8)

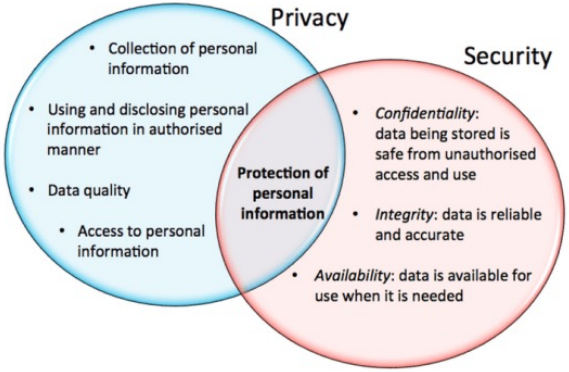
Privacy is one's right to freedom from intrusion and prying eyes. It's the state of being free from unwanted attention and secret surveillance.

SECURITY	PRIVACY
Security refers to protection against unauthorized access.	Privacy defines the ability to protect personally identifiable information.
Security provides protection for all types of data and information including the ones that are stored electronically.	Privacy means protecting sensitive information related to individuals and organizations.
Security can be achieved without privacy.	Privacy cannot be achieved without security.
Security program focuses on all sorts of information assets that an organization collects.	Privacy program focuses on personal information such as names, addresses, social security numbers, log in credentials, financial accounts information, etc.
It implements security protocols to provide confidentiality, integrity and availability of information assets.	It refers to protection of privacy rights with respect to processing of personal data.

VERSUS

DifferenceBetween.net

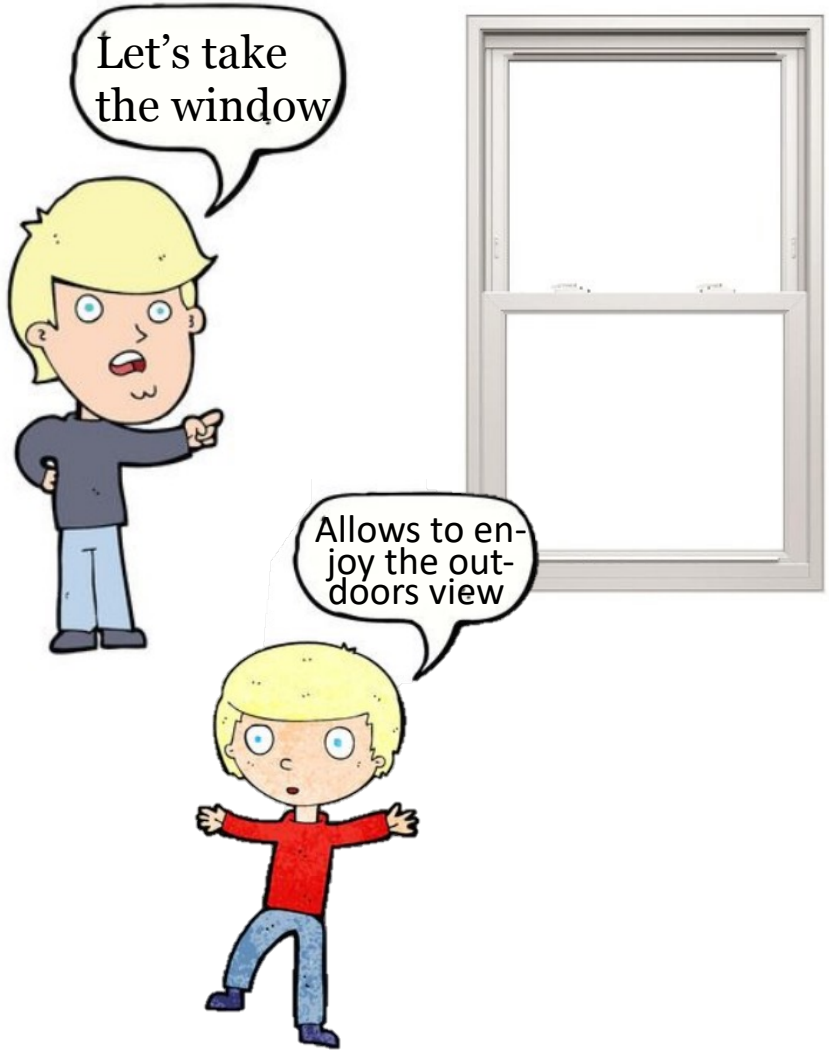




::.. Introduction (5/8)

Privacy is one's right to freedom from intrusion and prying eyes. It's the state of being free from unwanted attention and secret surveillance.

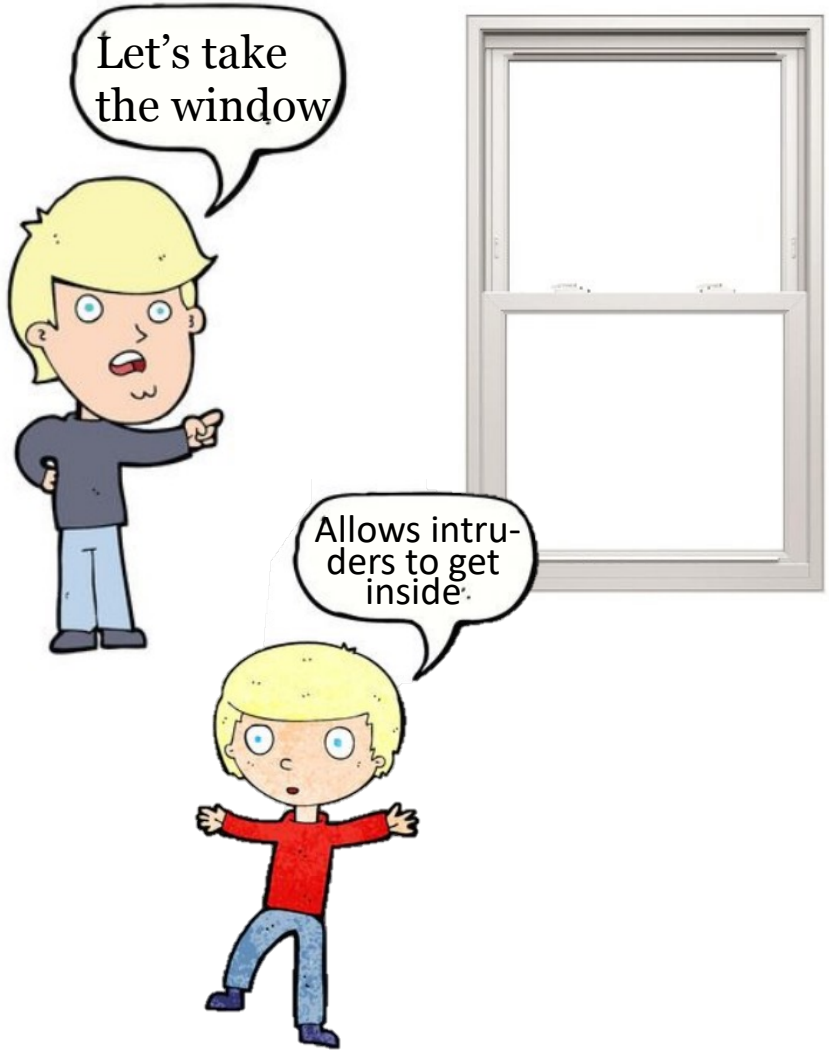
SECURITY	PRIVACY
Security refers to protection against unauthorized access.	Privacy defines the ability to protect personally identifiable information.
Security provides protection for all types of data and information including the ones that are stored electronically.	Privacy means protecting sensitive information related to individuals and organizations.
Security can be achieved without privacy.	Privacy cannot be achieved without security.
Security program focuses on all sorts of information assets that an organization collects.	Privacy program focuses on personal information such as names, addresses, social security numbers, log in credentials, financial accounts information, etc.
It implements security protocols to provide confidentiality, integrity and availability of information assets.	It refers to protection of privacy rights with respect to processing of personal data.



::.. Introduction (5/8)

Privacy is one's right to freedom from intrusion and prying eyes. It's the state of being free from unwanted attention and secret surveillance.

SECURITY	PRIVACY
Security refers to protection against unauthorized access.	Privacy defines the ability to protect personally identifiable information.
Security provides protection for all types of data and information including the ones that are stored electronically.	Privacy means protecting sensitive information related to individuals and organizations.
Security can be achieved without privacy.	Privacy cannot be achieved without security.
Security program focuses on all sorts of information assets that an organization collects.	Privacy program focuses on personal information such as names, addresses, social security numbers, log in credentials, financial accounts information, etc.
It implements security protocols to provide confidentiality, integrity and availability of information assets.	It refers to protection of privacy rights with respect to processing of personal data.



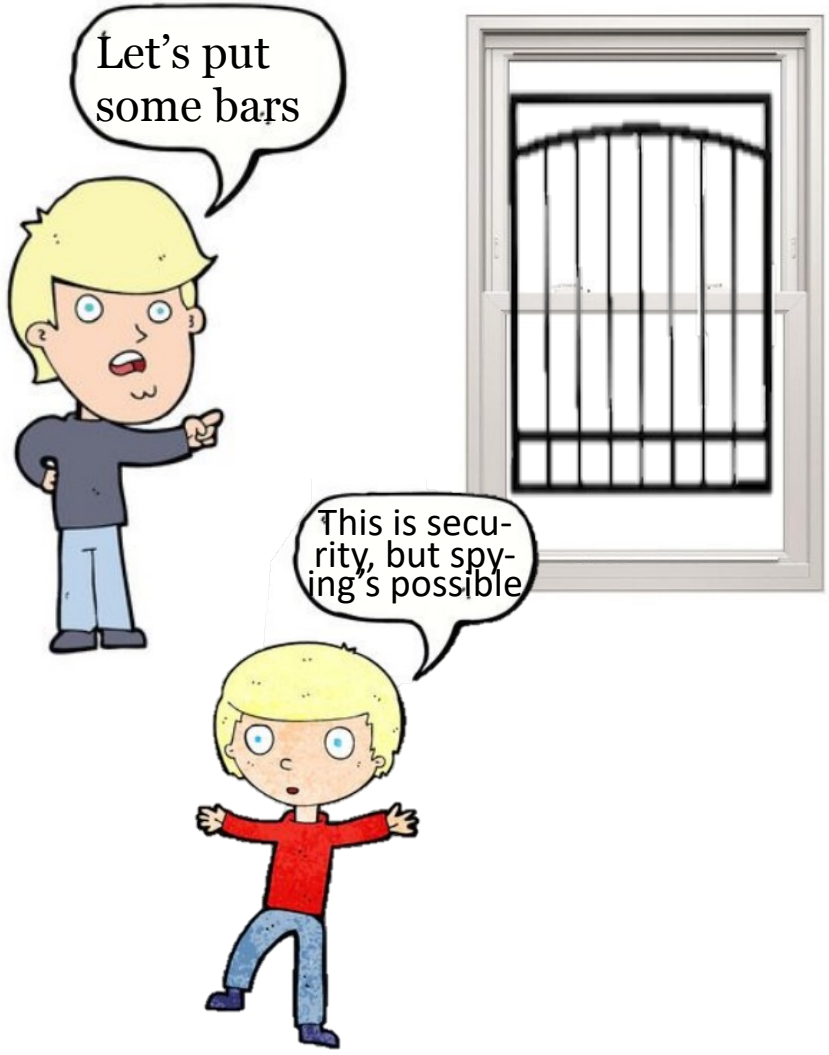
::.. Introduction (5/8)

Privacy is one's right to freedom from intrusion and prying eyes. It's the state of being free from unwanted attention and secret surveillance.

SECURITY	PRIVACY
Security refers to protection against unauthorized access.	Privacy defines the ability to protect personally identifiable information.
Security provides protection for all types of data and information including the ones that are stored electronically.	Privacy means protecting sensitive information related to individuals and organizations.
Security can be achieved without privacy.	Privacy cannot be achieved without security.
Security program focuses on all sorts of information assets that an organization collects.	Privacy program focuses on personal information such as names, addresses, social security numbers, log in credentials, financial accounts information, etc.
It implements security protocols to provide confidentiality, integrity and availability of information assets.	It refers to protection of privacy rights with respect to processing of personal data.

VERSUS

DifferenceBetween.net



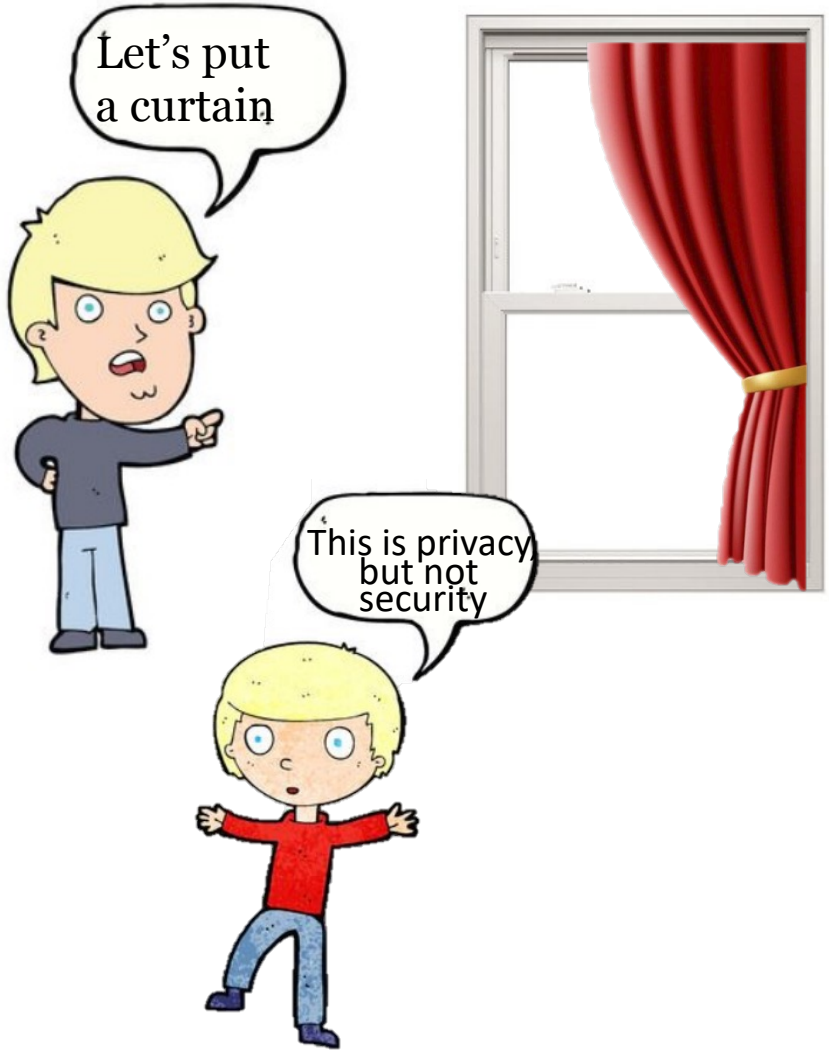
::.. Introduction (5/8)

Privacy is one's right to freedom from intrusion and prying eyes. It's the state of being free from unwanted attention and secret surveillance.

SECURITY	PRIVACY
Security refers to protection against unauthorized access.	Privacy defines the ability to protect personally identifiable information.
Security provides protection for all types of data and information including the ones that are stored electronically.	Privacy means protecting sensitive information related to individuals and organizations.
Security can be achieved without privacy.	Privacy cannot be achieved without security.
Security program focuses on all sorts of information assets that an organization collects.	Privacy program focuses on personal information such as names, addresses, social security numbers, log in credentials, financial accounts information, etc.
It implements security protocols to provide confidentiality, integrity and availability of information assets.	It refers to protection of privacy rights with respect to processing of personal data.

VERSUS

DifferenceBetween.net



::.. Introduction (6/8)

In Europe the EU Regulation 2016/679 (GDPR) states the key factors to protect the Union citizens from uncontrolled use of their personal data, explained in Chapter II (Article 5.1):

- The **lawfulness** of the hold data – The data is treated in a lawful, correct and transparent way w.r.t. the interested party;
- **Limited purpose** - The data is collected for specific, explicit and legitimate purposes;
- **Minimization** – The collected data must be relevant and limited to what is necessary w.r.t. the purposes for which they have been collected and processed;
- **Accuracy** - The collected personal data will be accurate and, if necessary, updated;

::.. Introduction (7/8)

- **Limited retention** - The requested data must be kept for a limited period of time not exceeding the achievement of the purposes for which they are treated;
- **Integrity and confidentiality** – The data is treated in a way to guarantee an adequate security, including the protection, through adequate technical and organizational measures, from unsecured or illicit treatments and from loss, destruction or accidental damage.

GDPR points out the application of

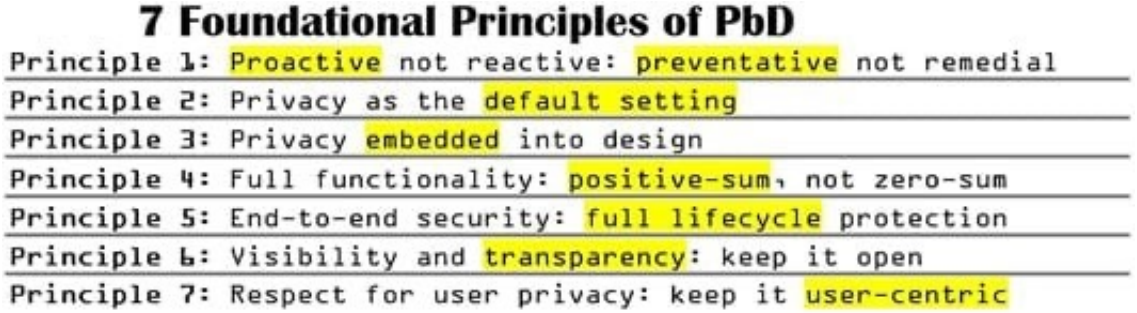
- "**Privacy by Design**" is a concept of risk prevention and means data protection through technology design, or data protection in data processing procedures is best adhered to when it is already integrated in the technology when created.

::.. Introduction (8/8)

7 Foundational Principles of PbD

Principle 1: Proactive not reactive: preventative not remedial
Principle 2: Privacy as the default setting
Principle 3: Privacy embedded into design
Principle 4: Full functionality: positive-sum, not zero-sum
Principle 5: End-to-end security: full lifecycle protection
Principle 6: Visibility and transparency: keep it open
Principle 7: Respect for user privacy: keep it user-centric

::.. Introduction (8/8)



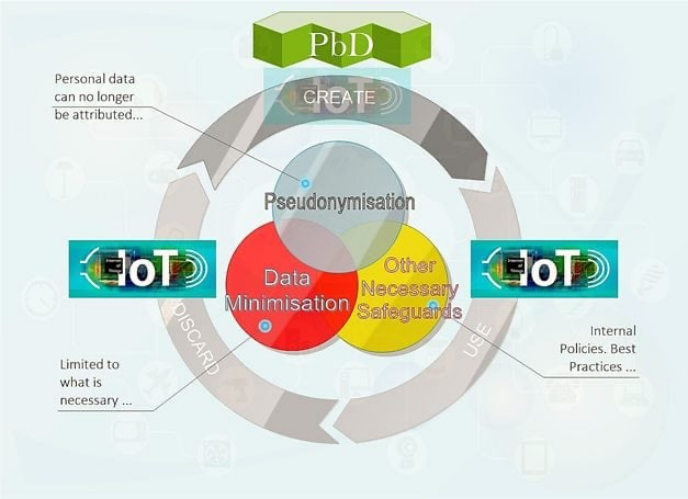
- "**Privacy by Default**" establishes that by default companies should only process personal data to the extent necessary and sufficient for the purposes envisaged and for the period strictly necessary for these purposes.

::.. Introduction (8/8)

7 Foundational Principles of PbD

Principle 1: Proactive not reactive: preventative not remedial
Principle 2: Privacy as the default setting
Principle 3: Privacy embedded into design
Principle 4: Full functionality: positive-sum, not zero-sum
Principle 5: End-to-end security: full lifecycle protection
Principle 6: Visibility and transparency: keep it open
Principle 7: Respect for user privacy: keep it user-centric

- "**Privacy by Default**" establishes that by default companies should only process personal data to the extent necessary and sufficient for the purposes envisaged and for the period strictly necessary for these purposes.



Art. 25 of the GDPR makes mention of which methods data controllers/processors may choose to use in order to apply the PbD approach: "pseudonymization," "data minimization" and other "necessary safeguards [that] protect the rights of data subjects."

IoT Vulnerabilities & Attacks

::.. Vulnerabilities of IoT (1/5)

- **Deficient physical security** - With little effort, an adversary might obtain unauthorized physical access to IoT devices and thus take control over them. Consequently, an attacker would cause physical damage to the devices, possibly unveiling employed cryptographic schemes, replicating their firmware using malicious node, or simply corrupting their control or cyber data.

::.. Vulnerabilities of IoT (1/5)

- **Deficient physical security** - With little effort, an adversary might obtain unauthorized physical access to IoT devices and thus take control over them. Consequently, an attacker would cause physical damage to the devices, possibly unveiling employed cryptographic schemes, replicating their firmware using malicious node, or simply corrupting their control or cyber data.

Hardware Trojan is a malicious modification of an integrated circuit, which enables the attacker to use the circuit or to exploit its functionality to obtain access to data or software running on the integrated circuits (ICs).

Tampering consists in the attacker, with a physical access to the device, extracting valuable cryptographic information, tamper with the circuit, modify programming, or change the operating system.

::.. Vulnerabilities of IoT (1/5)

- **Deficient physical security** - With little effort, an adversary might obtain unauthorized physical access to IoT devices and thus take control over them. Consequently, an attacker would cause physical damage to the devices, possibly unveiling employed cryptographic schemes, replicating their firmware using malicious node, or simply corrupting their control or cyber data.

- **Insufficient energy harvesting** - IoT devices characteristically have limited energy and do not necessary possess the technology or mechanisms to renew it automatically. An attacker might drain the stored energy by generating flood of legitimate or corrupted messages, rendering the devices unavailable for valid processes or users.

::.. Vulnerabilities of IoT (2/5)

- **Inadequate authentication** - The unique constraints of limited energy and computational power challenge the implementation of complex authentication mechanisms. Under such circumstances, the exchanged and employed authentication keys are also always at risk of being lost, destroyed, or corrupted. To this end, an attacker might exploit ineffective authentication approaches to append spoofed malicious nodes or violate data integrity, thus intruding on IoT devices and network communications.
- **Improper encryption** - Resource limitations of the IoT affects the robustness, efficiency and efficacy of encryption algorithms. To this end, an attacker might be able to circumvent the deployed encryption techniques to reveal sensitive information or control operations with limited, feasible effort, as wireless communications are easy to be eavesdropped.

::.. Vulnerabilities of IoT (2/5)

- **Inadequate authentication** - The unique constraints of limited energy and computational power challenge the implementation of complex authentication mechanisms. Under such circumstances, the exchanged and employed authentication keys are also always at risk of being lost, destro cker might exploit to append spoofe grity, thus intrudi ons.

Security mechanism	Effect on energy consumption
Encryption	⇑15 – 30%
Channel assignment	⇑10%
Power control	⇑4%
All three above	⇑230%

- **Improper encryption** - Resource limitations of the IoT affects the robustness, efficiency and efficacy of encryption algorithms. To this end, an attacker might be able to circumvent the deployed encryption techniques to reveal sensitive information or control operations with limited, feasible effort, as wireless communications are easy to be eavesdropped.

::.. Vulnerabilities of IoT (3/5)

- **Unnecessary open ports** - Various IoT devices have un-necessarily open ports while running vulnerable services, permitting an attacker to connect and exploit a plethora of vulnerabilities.

- **Insufficient access control -** The majority of IoT devices in conjunction with their cloud management solutions do not force a password of sufficient complexity. Moreover, after installation, numerous devices do not request to change the default user credentials. Further, most of the users have elevated permissions. Hence, an adversary could gain unauthorized access to the device, threaten data and the entire Internet.

::.. Vulnerabilities of IoT (4/5)

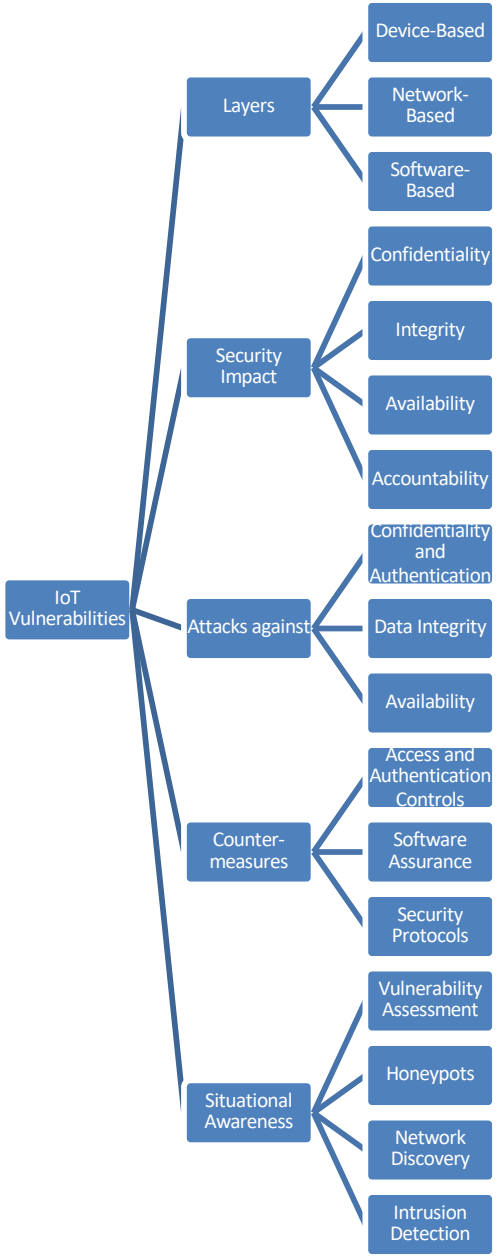
- **Improper patch management capabilities** - IoT operating systems and embedded firmware/software should be patched appropriately to continuously minimize attack vectors and augment their functional capabilities. However, many manufacturers either do not recurrently maintain security patches or do not have in place automated patch-update mechanisms. Moreover, even available update mechanisms lack integrity guarantees, rendering them susceptible to being maliciously modified and applied at large.

- **Weak programming practices** - Countless firmware are released with known vulnerabilities such as backdoors, root users as prime access points, and the lack of Secure Socket Layer (SSL) usage. Hence, an adversary might easily exploit known security weaknesses to cause buffer overflows, information modifications, or gain unauthorized access to the device.

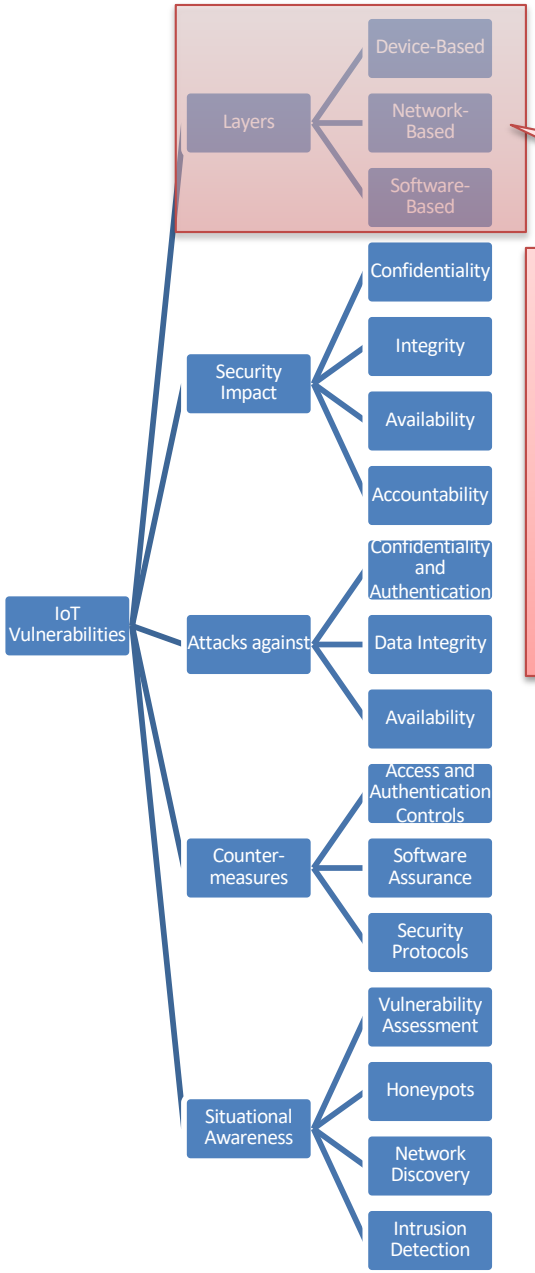
::.. Vulnerabilities of IoT (5/5)

- **Insufficient audit mechanisms** - A plethora of IoT devices lack thorough logging procedures, rendering it possible to conceal IoT-generated malicious activities.

::.. Vulnerability Taxonomy



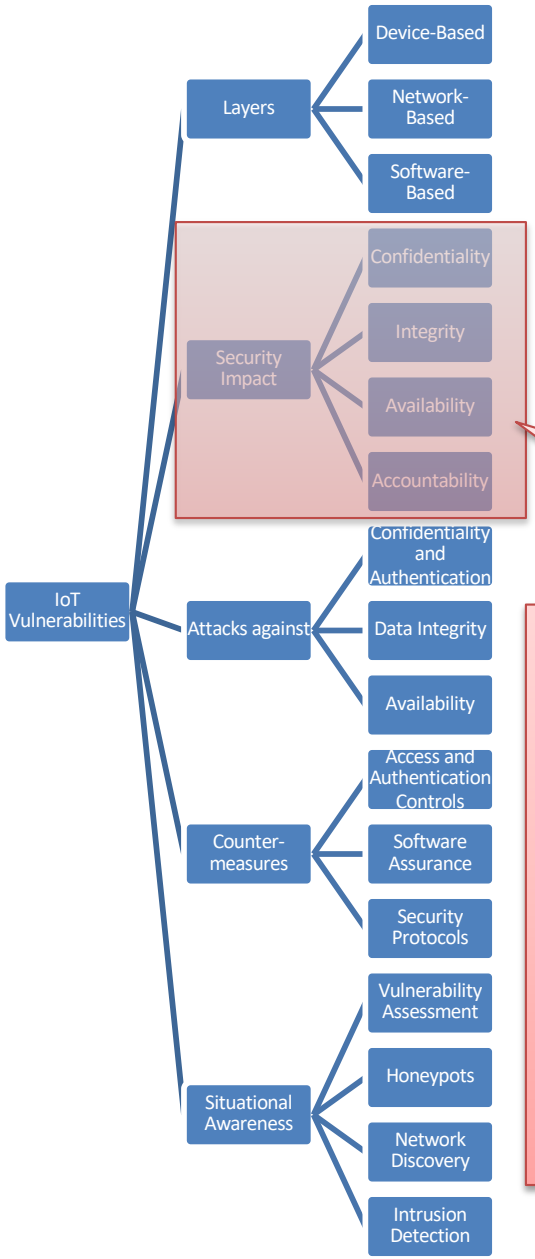
::.. Vulnerability Taxonomy



It represents where the vulnerabilities occurs: those within the hardware elements of the IoT, those from communication protocols, and/or those related to the firmware and/or the software of IoT devices.

Layers	Vulnerabilities
Device-based	Deficient physical security Insufficient energy harvesting
Network-based	Inadequate authentication Improper encryption Unnecessary open ports
Software-based	Insufficient access control Improper patch management capabilities Weak programming practices (e.g. root user, lack of SSL, plain text password, backdoor, ect.) Insufficient audit mechanism

::.. Vulnerability Taxonomy



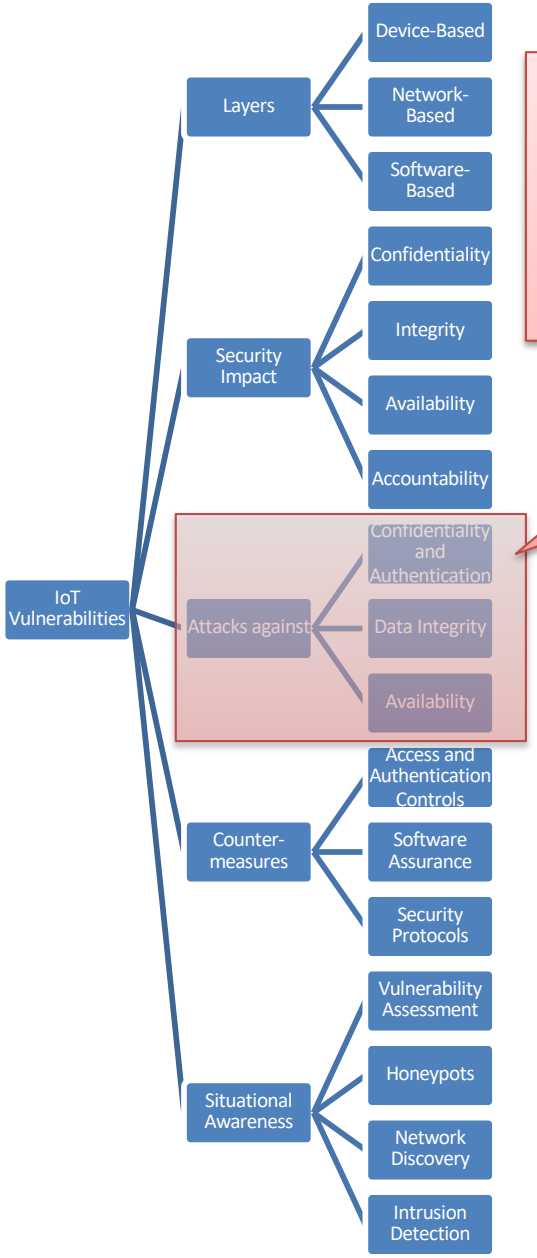
Layers	Vulnerabilities	Security Impact			
		Confidentiality	Integrity	Availability	Accountability
Device-based	Deficient physical security	○	●	●	○
	Insufficient energy harvesting	○	○	●	○
Network-based	Inadequate authentication	●	●	○	○
	Improper encryption	●	●	○	○
	Unnecessary open ports	●	○	●	○
Software-based	Insufficient access control	●	●	●	○
	Improper patch management capabilities	○	○	●	○
	Weak programming practices (e.g. root user, lack of SSL, plain text password, backdoor, ect.)	●	●	○	○
	Insufficient audit mechanism	○	●	○	●

Legend: ● vulnerability has significant impact on particular security concept,
○ vulnerability does not have significant impact on a particular security concept

Security Impact evaluates the vulnerabilities based on the threats they pose on core security objectives.

It is clear that, given the cross-dependencies among the various security requirements, each identified IoT vulnerability might affect more than one security objective.

::.. Vulnerability Taxonomy

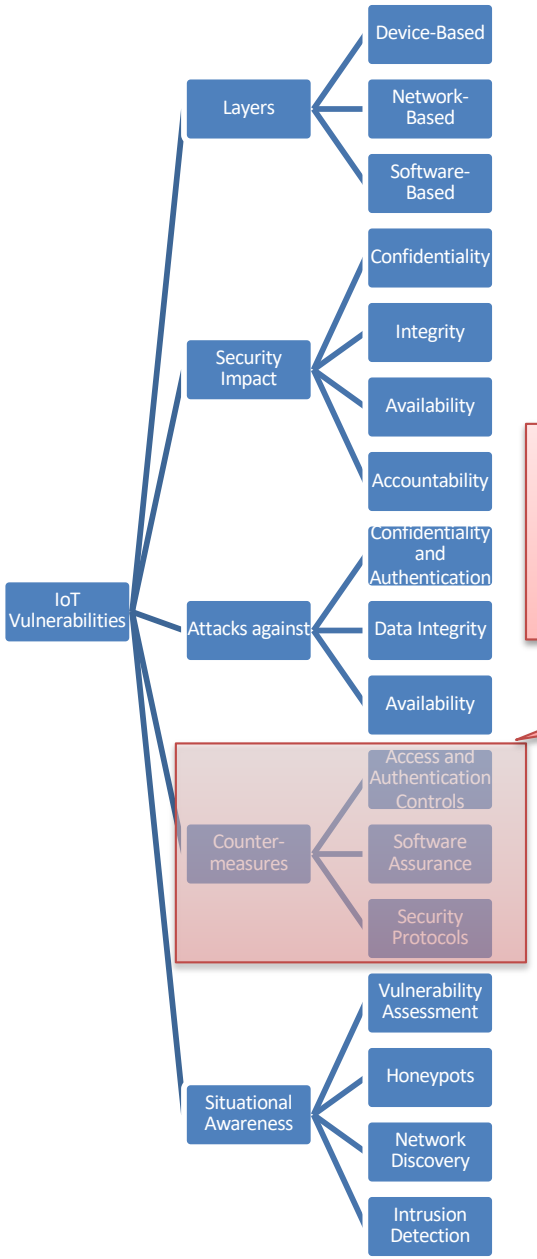


Attacks describe the security flaws categorized by the approach in which the inferred IoT vulnerabilities could be exploited.

	Dictionary Attack	Side-Channel Attack	Sybil Attack	False Data Injection	Firmaware Modification Attack	Device Capture	Sinkhole Attack	Battery Draining Attack	Jumming Attack
Deficient physical security	○	●	○	○	●	●	○	○	○
Insufficient energy harvesting	○	○	○	○	○	○	●	●	●
Insufficient authentication	●	○	●	●	○	●	●	○	○
Improper encryption	○	●	○	○	○	○	○	○	○
Unnecessary open ports	●	○	○	○	○	○	○	○	○
Insufficient access control	●	○	○	○	○	○	○	○	○
Improper software update capabilities	○	○	○	○	●	○	○	○	○
Weak programming practice (e.g. root user, lack of SSL, plain text password, back-door, ect.)	●	○	○	●	●	○	○	○	○
Insufficient audit mechanism	●	○	○	●	●	●	○	○	○

Legend: ● an attack leverages particular vulnerability, ○ an attack does not leverages particular vulnerability

::.. Vulnerability Taxonomy



Attack	Remediation Strategy		
	Access and Authentication Controls	Software Assurance	Security Protocols
Dictionary attack	●	○	○
Side-Channel attack	○	○	○
Sybil attack	○	○	●
False Data Injection	○	●	○
Firmaware modification attack	○	●	○
Device capture	●	○	●
Sinkhole Attack	●	○	○
Battery draining attack	●	○	●
Selective-forwarding	○	○	○

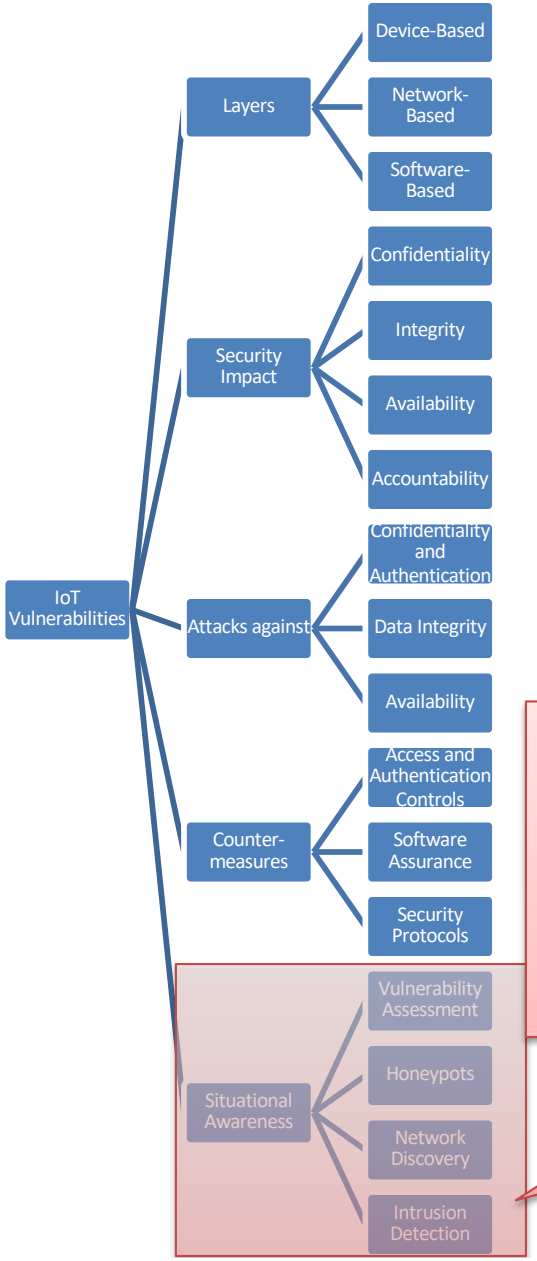
Legend: ● strategy covers particular vulnerability, ○ strategy does not cover particular vulnerability

The available remediation techniques needed to mitigate the identified IoT vulnerabilities.

Vulnerability	Remediation Strategy		
	Access and Authentication Controls	Software Assurance	Security Protocols
Deficient physical security	●	○	○
Insufficient energy harvesting	●	○	●
Inadequate authentication	●	○	○
Improper encryption	○	○	●
Unnecessary open ports	○	○	○
Insufficient access control	●	●	●
Improper patch management capabilities	○	○	○
Weak programming practices (e.g. root user, lack of SSL, plain text password, backdoor, ect.)	○	●	○
Insufficient audit mechanism	●	○	○

Legend: ● strategy covers particular vulnerability, ○ strategy does not cover particular vulnerability

::.. Vulnerability Taxonomy



Vulnerability	Situational Awareness Capabilities			
	Vulnerability Assessment	Honeypots	Network Discovery	Intrusion Detection
Deficient physical security	●	○	○	●
Insufficient energy harvesting	○	○	○	●
Inadequate authentication	●	○	●	●
Improper encryption	●	○	○	○
Unnecessary open ports	●	●	○	○
Insufficient access control	●	●	●	○
Improper patch management capabilities	●	○	○	○
Weak programming practices (e.g. root user, lack of SSL, plain text password, backdoor, etc.)	●	○	○	●
Insufficient audit mechanism	○	○	○	●
IoT device identification	○	○	●	●

Legend: ● capability covers particular vulnerability, ○ capability does not cover particular vulnerability

The available techniques used for capturing accurate and sufficient information regarding generated malicious activities in the context of the IoT.

::.. Attacks against IoT (1/5)

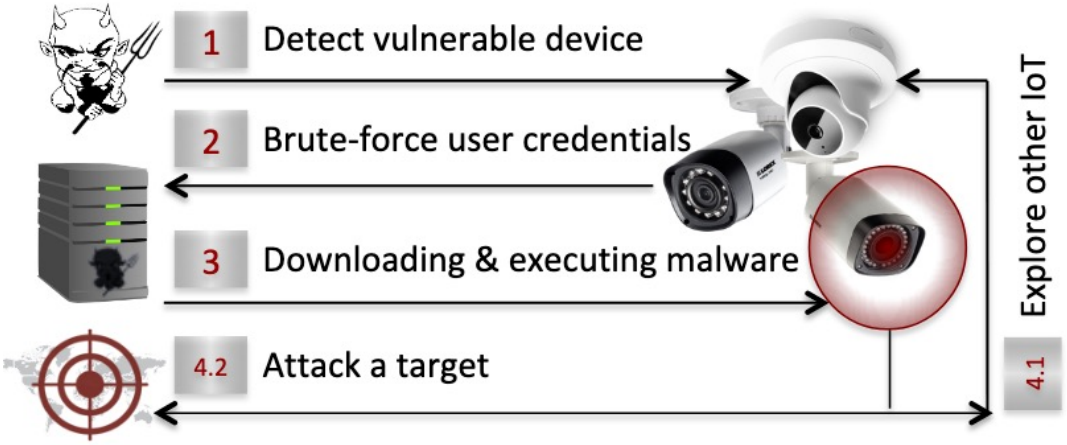
Attacks against Confidentiality and Authentication aims at gaining unauthorized access to IoT resources and data to conduct further malicious actions. This type of attack is often induced by executing brute force events, eavesdropping IoT physical measurements, or faking devices identities.

::.. Attacks against IoT (1/5)

Attacks against Confidentiality and Authentication aims at gaining unauthorized access to IoT resources and data to conduct further malicious actions. This type of attack is often induced by executing brute force events, eavesdropping IoT physical measurements, or faking devices identities.

- **Dictionary attacks** consists in variants of brute force events, leading to illicit modifications of settings or even full control of device functions.

Example: Mirai (Japanese: 未来, lit. 'future') is a malware that turns networked devices running Linux into remotely controlled bots that can be used as part of a botnet in large-scale network attacks.



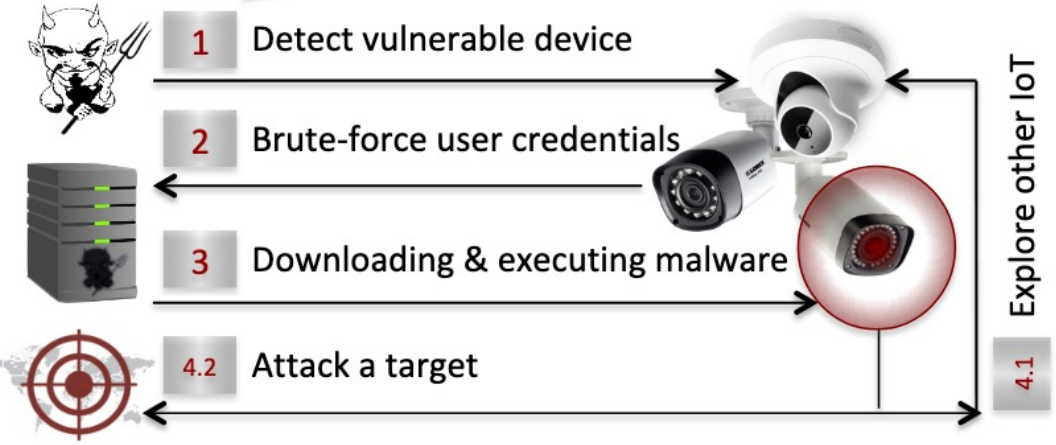
::.. Attacks against IoT (1/5)

Attacks against Confidentiality and Authentication aims at gaining unauthorized access to IoT resources and data to

Devices infected by Mirai continuously scan the internet for the IP address of IoT devices. Mirai then identifies vulnerable IoT devices using a table of more than 60 common factory default usernames and passwords, and logs into them to infect them with the Mirai malware. Infected devices will continue to function normally, except for occasional sluggishness, and an increased use of bandwidth.

of device functions.

Example: Mirai (Japanese: 未来, lit. 'future') is a malware that turns networked devices running Linux into remotely controlled bots that can be used as part of a botnet in large-scale network attacks.



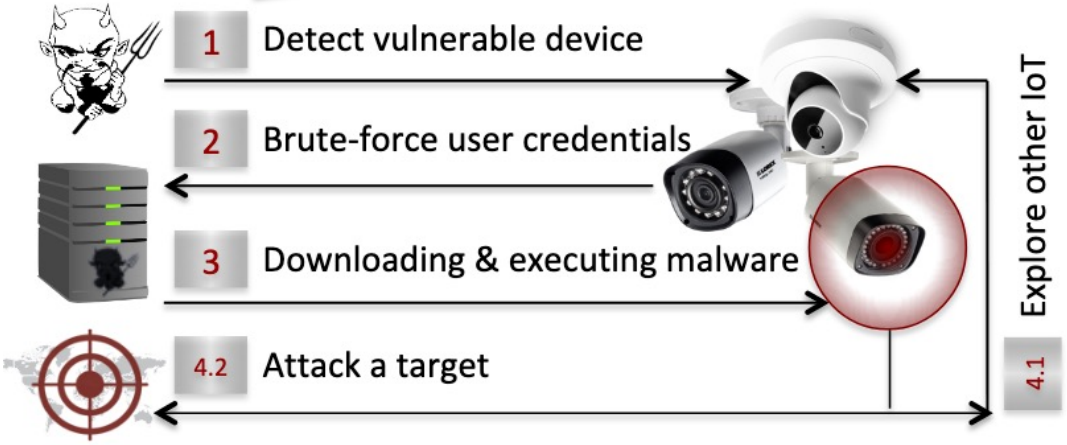
::.. Attacks against IoT (1/5)

Attacks against Confidentiality and Authentication aims at gaining unauthorized access to IoT resources and data to

A device remains infected until it is rebooted, which may involve simply turning the device off and after a short wait turning it back on. After a reboot, unless the login password is changed immediately, the device will be reinfected within minutes. Upon infection Mirai will identify any "competing" malware, remove it from memory, and block remote administration ports.

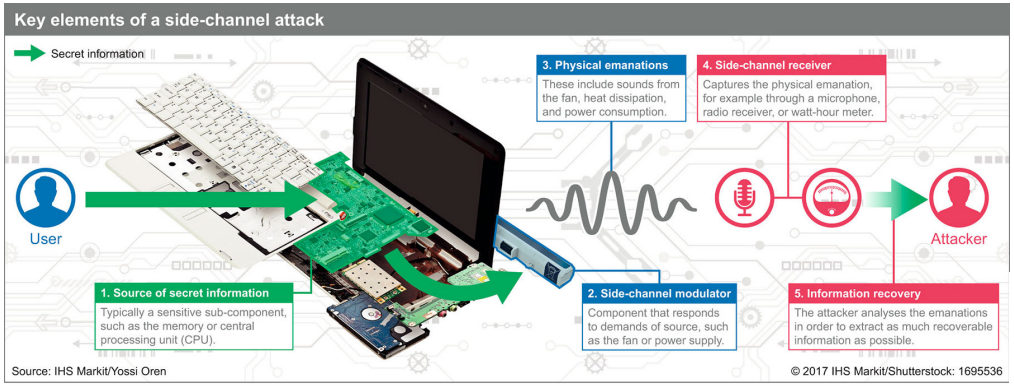
of device functions.

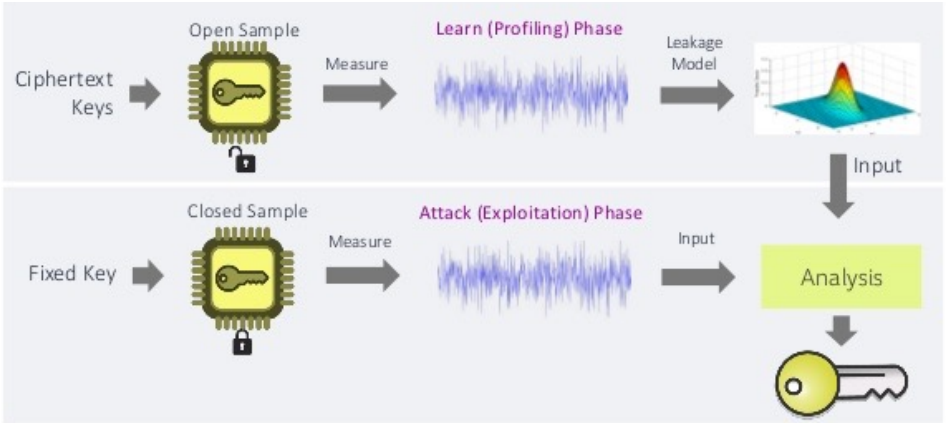
Example: Mirai (Japanese: 未来, lit. 'future') is a malware that turns networked devices running Linux into remotely controlled bots that can be used as part of a botnet in large-scale network attacks.



::.. Attacks against IoT (2/5)

- **Side-channel attacks** (i.e., power analysis) endeavour to recover devices cryptographic keys by leveraging existing correlations between physical measurements and the internal states of IoT devices, rather than weaknesses in the implemented algorithm itself (e.g. **cryptanalysis**).



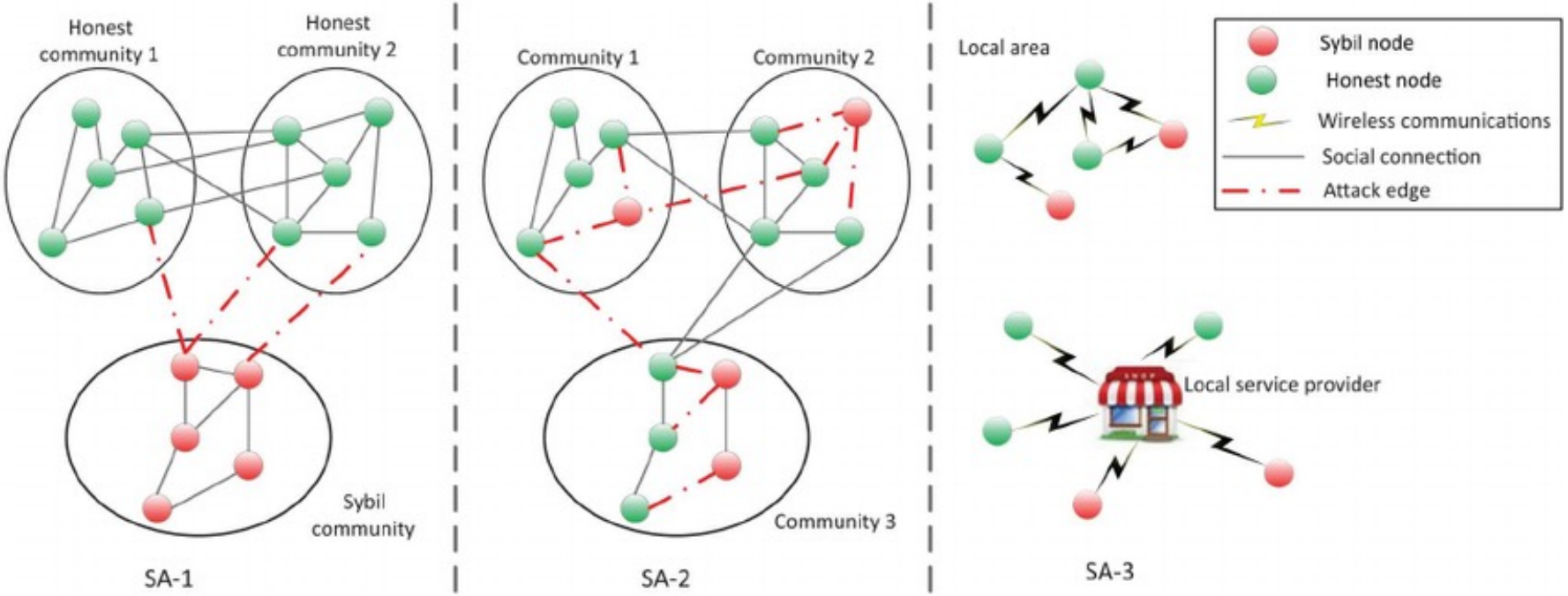


::.. Attacks against IoT (2/5)

- **Side-channel attacks** (i.e., power analysis) endeavour to recover devices cryptographic keys by leveraging existing correlations between physical measurements and the internal states of IoT devices, rather than weaknesses in the implemented algorithm itself (e.g. **cryptanalysis**).

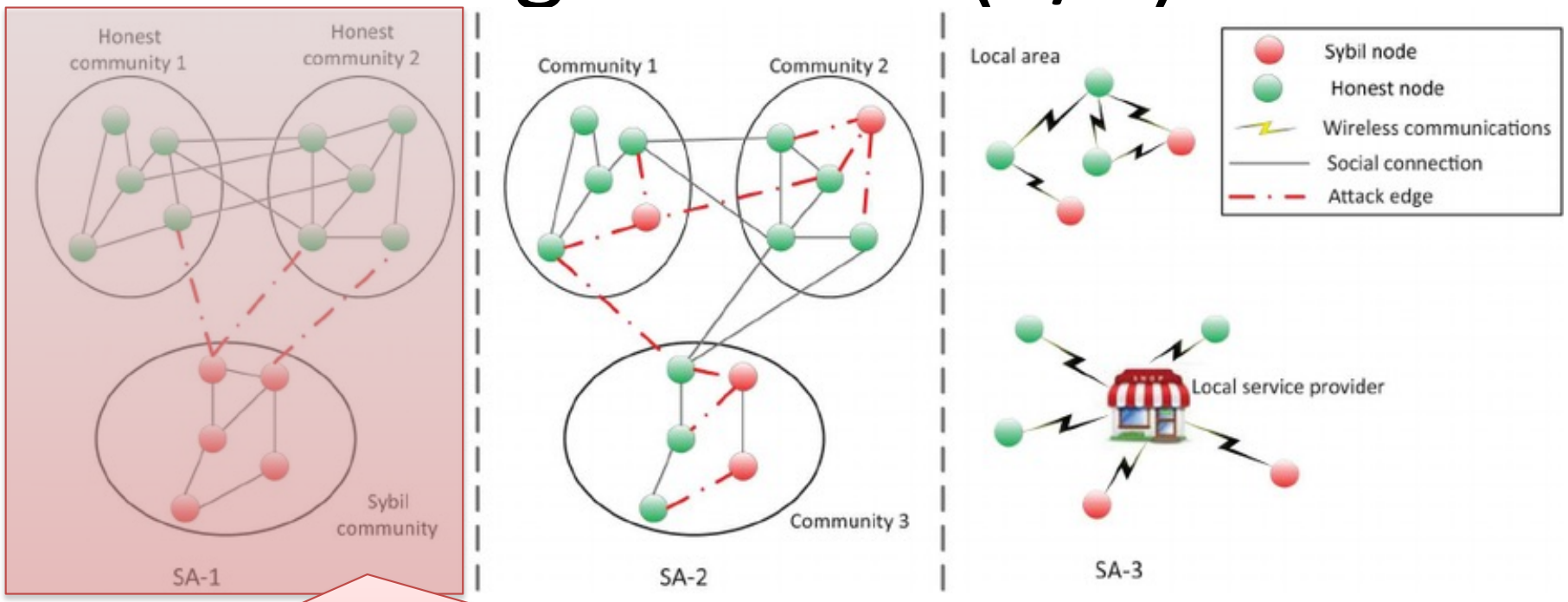
- **Sybil attacks** consists in the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities and uses them to gain a disproportionately large influence.

::.. Attacks against IoT (2/5)



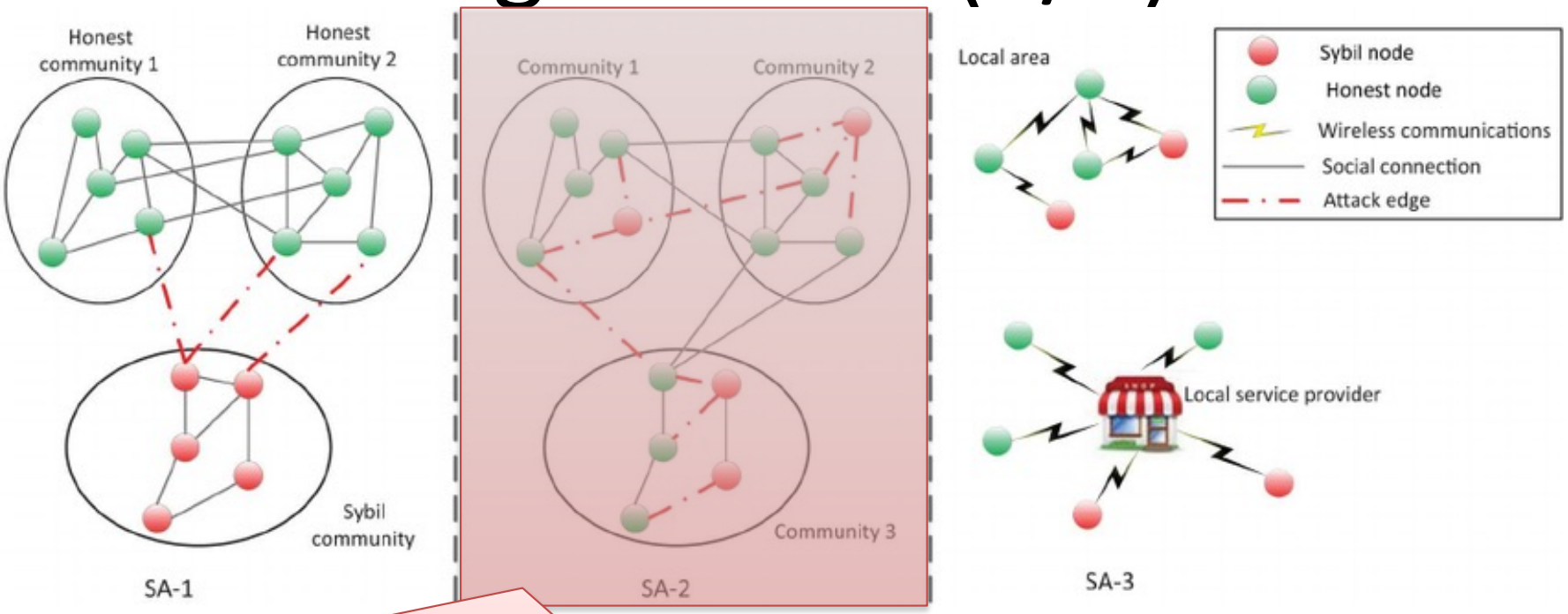
- **Sybil attacks** consists in the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities and uses them to gain a disproportionately large influence.

::.. Attacks against IoT (2/5)



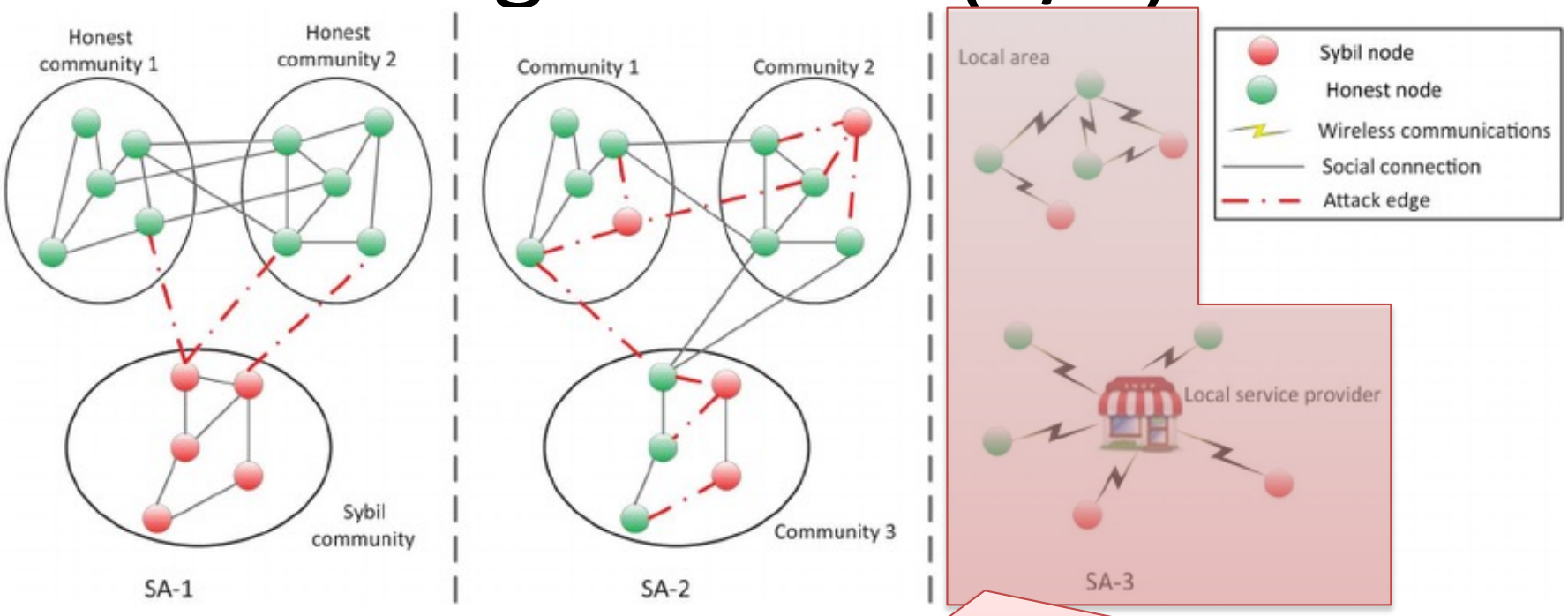
The SA-1 attackers usually build connections within the Sybil community, while Sybil nodes do not build strong social connections with honest nodes. The SA-1 attackers usually exist in sensing domain and social domain, i.e., OSN, voting, or mobile sensing systems. The main goal is to manipulate the overall option or popularity.

::.. Attacks against IoT (2/5)



SA-2 is able to build the social connections not only among Sybil identities but also with the normal users. SA-2 has strong capabilities of mimicing the normal user's social structures from the perspective of social graph. The goal of SA-2 is to disseminate spam, advertisements, and malware; steal and violate user's privacy; and maliciously manipulate the reputation system.

::.. Attacks against IoT (2/5)

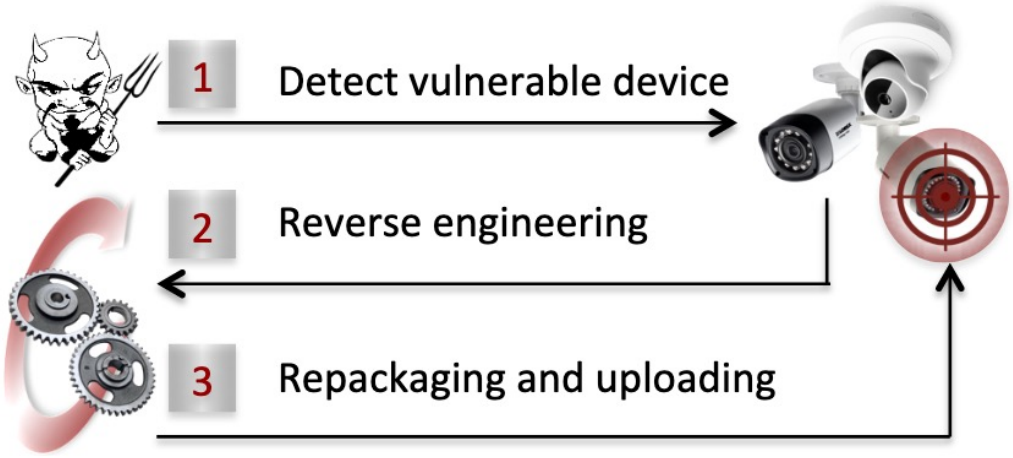


SA-3 has an impact only in a local area or within a short period. Mobile users cannot keep connections with others for the long time, or the connections are intermittent, so a centralized authority cannot exist making Sybil defense hard.

::.. Attacks against IoT (3/5)

Attacks against Data Integrity consists in the sabotage of IoT data, which is quite damaging to the IoT paradigm.

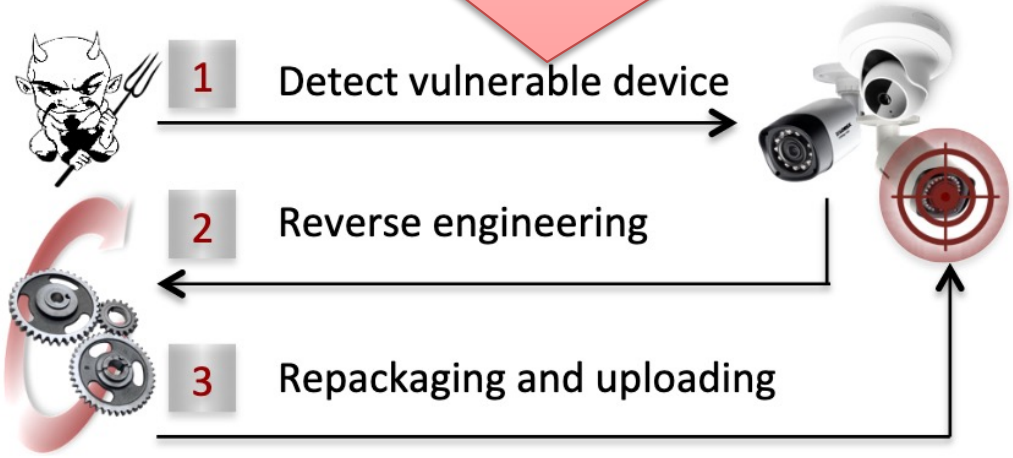
- **False Data Injection** (FDI) attacks fuse legitimate or corrupted input towards IoT sensors to cause various integrity violations. Lunching such attacks could mislead the state estimation process of a IoT device, causing dramatic economic impact or even loss of human life.



- **Firmware modification** aims at maliciously altering the firmware and inducing a functional disruption of the targeted device.

::.. Attacks against IoT (3/5)

Many firmware are released with known vulnerabilities and about 80% of firmware images rely on third-party libraries that contain known vulnerabilities. Update mechanisms typically do not require authentication, facilitating a firmware modification attack. In addition, the rate of current IoT firmware patches is significantly low, and IoT devices lack defense/integrity mechanisms, which can prevent firmware modification attacks.



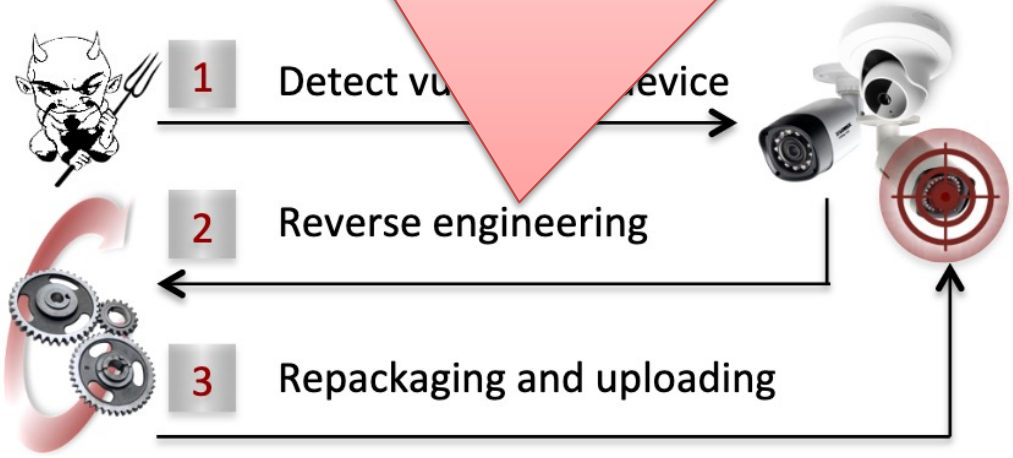
- **Firmware modification** aims at maliciously altering the firmware and inducing a functional disruption of the targeted device.

::.. Attacks against IoT (3/5)

Attacks against Data Integrity consists in the sabotage of IoT data, which is quite damaging to the IoT paradigm.

- **False Data Injection** (FDI) attacks fuse legitimate or corrupted input towards IoT sensors to cause various

By conducting reverse engineering, the attacker can determine the details of the operating system, extract the functionality of various critical routines, and locate key structures to be modified.



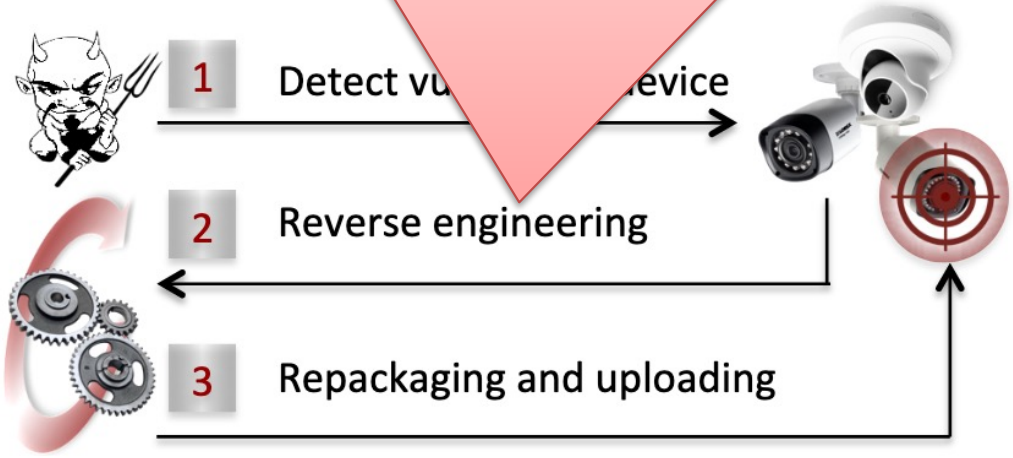
- **Firmware modification** aims at maliciously altering the firmware and inducing a functional disruption of the targeted device.

::.. Attacks against IoT (3/5)

Attacks against Data Integrity consists in the sabotage of IoT data, which is quite damaging to the IoT paradigm.

- **False Data Injection** (FDI) attacks fuse legitimate or corrupted input towards IoT sensors to cause various

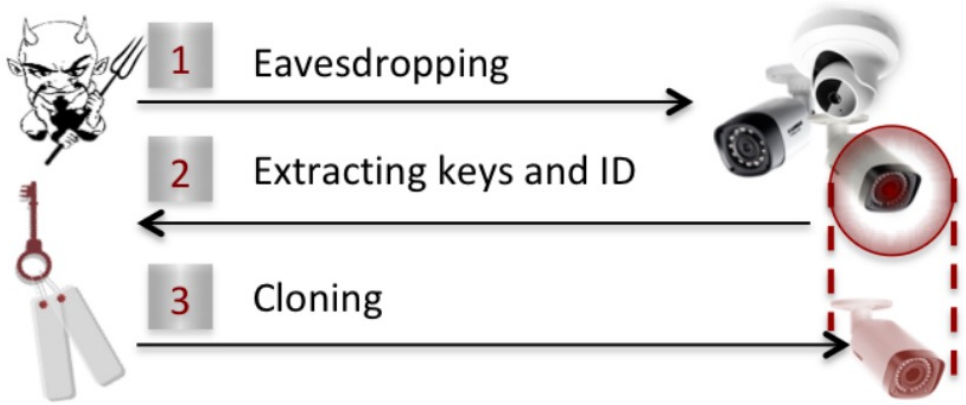
The uploading is not a complex task as IoT devices typically employ weak update validation means, as a simplistic checksum, which can be easily circumvented.



- **Firmware modification** aims at maliciously altering the firmware and inducing a functional disruption of the targeted device.

::.. Attacks against IoT (4/5)

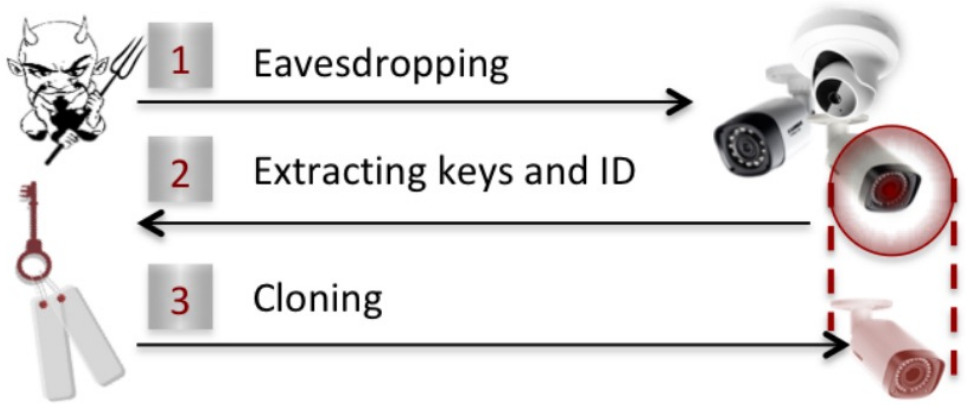
Attacks against Availability, or **Denial of Service** (DoS) attacks against IoT, is to prevent the legitimate users' timely access to IoT resources. This is often induced by revoking device from the network or draining IoT resources until their full exhaustion.



- **Device capture** capture, alter or destroy a device to retrieve stored sensitive information, including secret keys.

::.. Attacks against IoT (4/5)

Attacks against Availability, or **Denial of Service** (DoS) attacks against IoT, is to prevent the legitimate users' timely access to IoT resources. This is often induced by revoking device from the network or draining IoT resources until their full exhaustion.

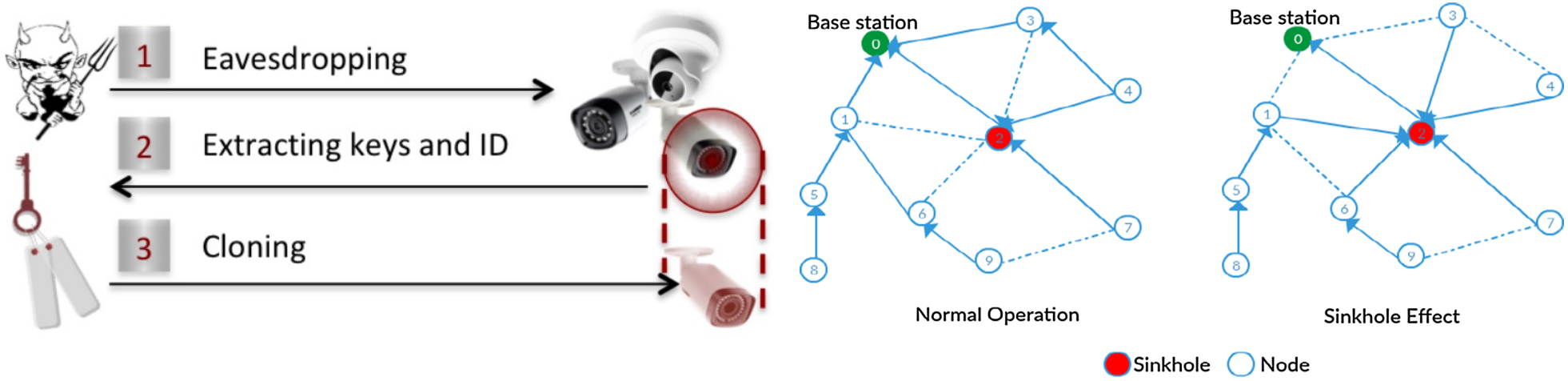


- **Device capture** capture, alter or destroy a device to retrieve stored sensitive information, including secret keys.

- **Sinkhole** attacks is conducted by the malicious nodes having the ability to advertise artificial routing paths where they act as mediators among honest nodes. Malicious nodes can drop packets or send them over longer paths.

::.. Attacks against IoT (4/5)

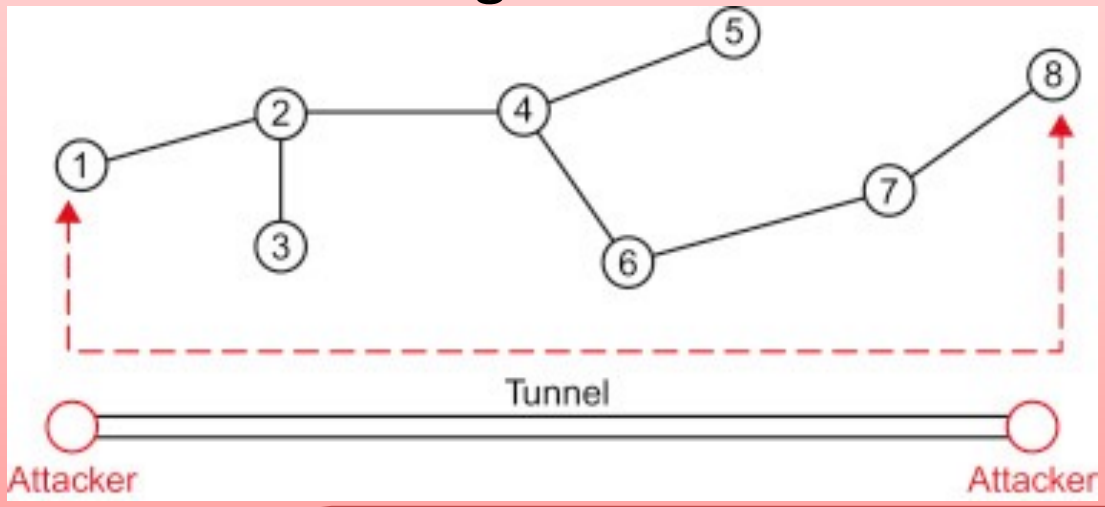
Attacks against Availability, or **Denial of Service** (DoS) attacks against IoT, is to prevent the legitimate users' timely access to IoT resources. This is often induced by revoking device from the network or draining IoT resources until their full exhaustion.



- **Sinkhole** attacks is conducted by the malicious nodes having the ability to advertise artificial routing paths where they act as mediators among honest nodes. Malicious nodes can drop packets or send them over longer paths.

::.. Attacks against IoT (4/5)

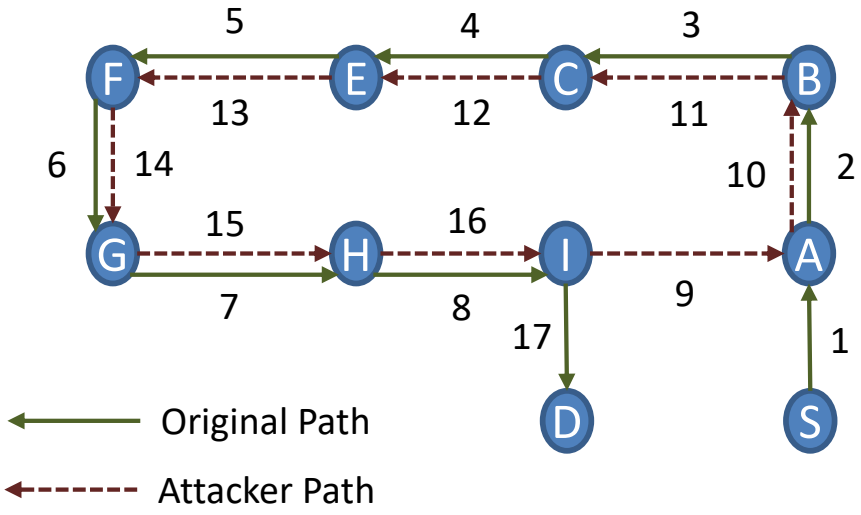
In **wormhole attacks**, two malicious nodes located at different places of the network exchange routing information by tunneling to obtain a false one-hop transmission, even if they are placed far away between each other. More data is conveyed through these two nodes, so that these attacks lead to similar damages as the sinkhole.



- **Sinkhole** attacks is conducted by the malicious nodes having the ability to advertise artificial routing paths where they act as mediators among honest nodes. Malicious nodes can drop packets or send them over longer paths.

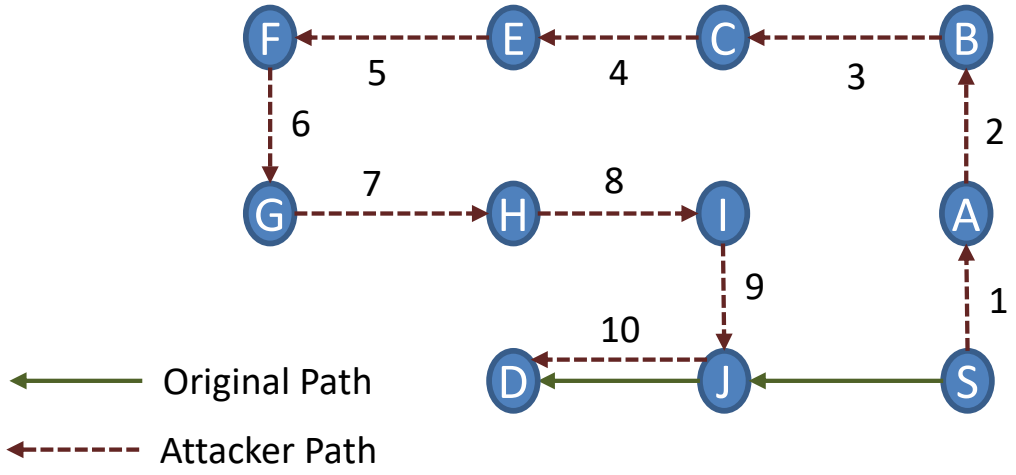
::.. Attacks against IoT (5/5)

- The **Battery Draining**, or vampire, attacks are broadly defined as the transmission of a message in a way which demands significantly more energy from the network and its nodes to be employed and acted upon in contrast with typical messages.
  - **Carousel attacks** permit an adversary to send messages as a series of loops such that the same node appears in the route several times.



::.. Attacks against IoT (5/5)

- The **Battery Draining**, or vampire, attacks are broadly defined as the transmission of a message in a way which demands significantly more energy from the network and its nodes to be employed and acted upon in contrast with typical messages.
  - **Stretch attacks** allow malicious nodes to artificially construct long routes so that the packets traverse through a larger, inversely optimal number of IoT nodes.



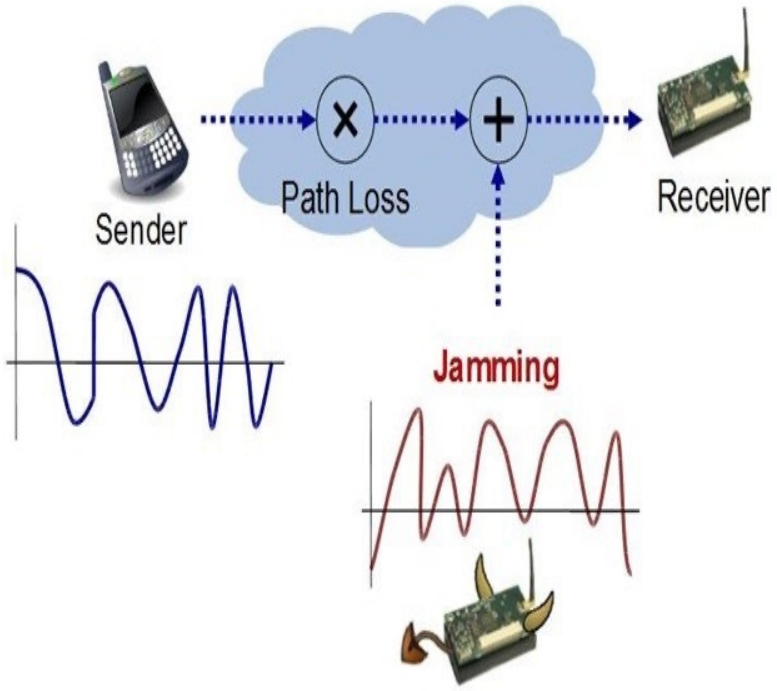
::.. Attacks against IoT (5/5)

- The **Battery Draining**, or vampire, attacks are broadly defined as the transmission of a message in a way which demands significantly more energy from the network and its nodes to be employed and acted upon in contrast with typical messages.

Most IoT devices extend their life cycle by following a sleep routine to reduce power consumption. The **sleep deprivation** attack can break such routines and keep the devices awake all the time.

::.. Attacks against IoT (5/5)

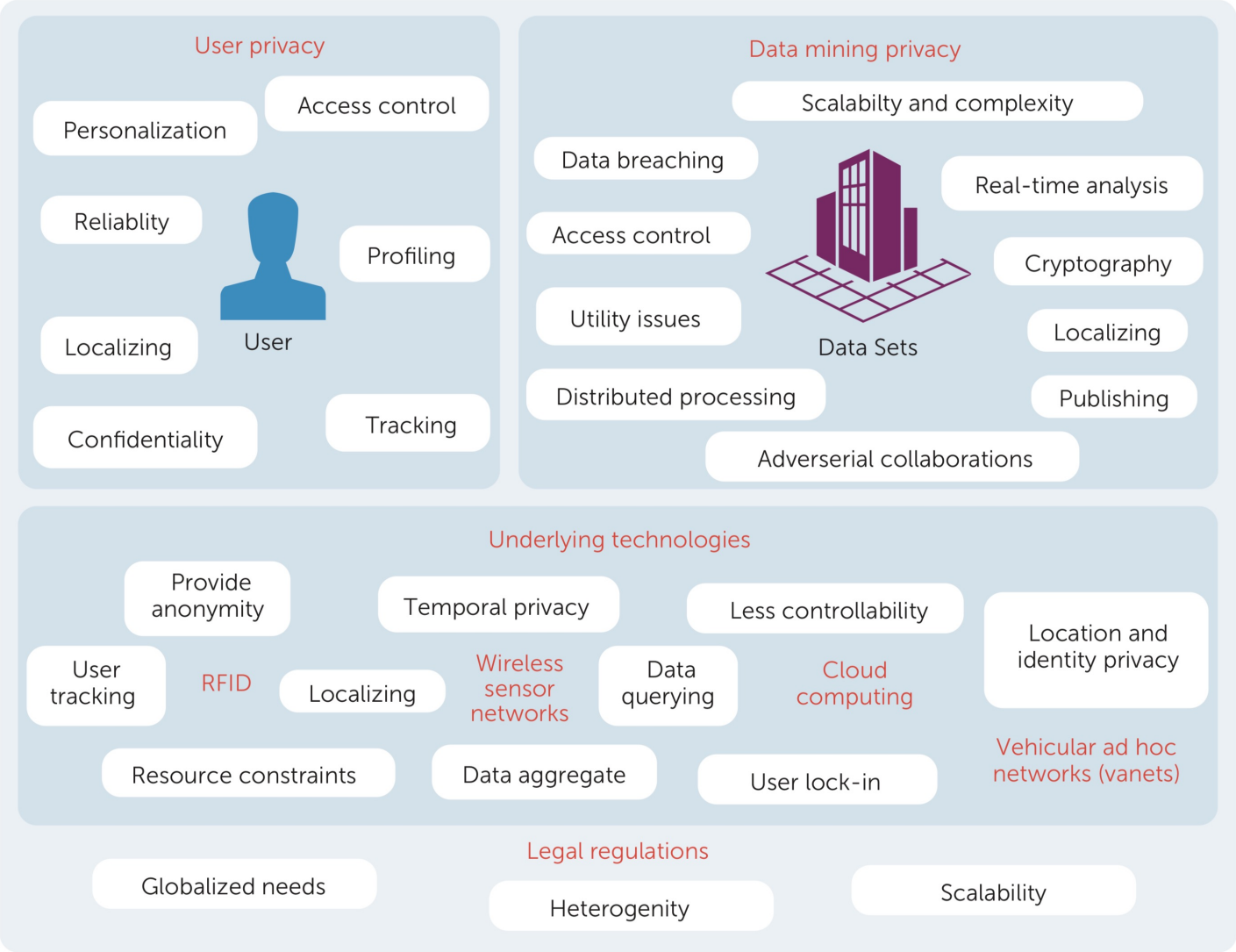
- The **Battery Draining**, or vampire, attacks are broadly defined as the transmission of a message in a way which demands significantly more energy from the network and its nodes to be employed and acted upon in contrast with typical messages.



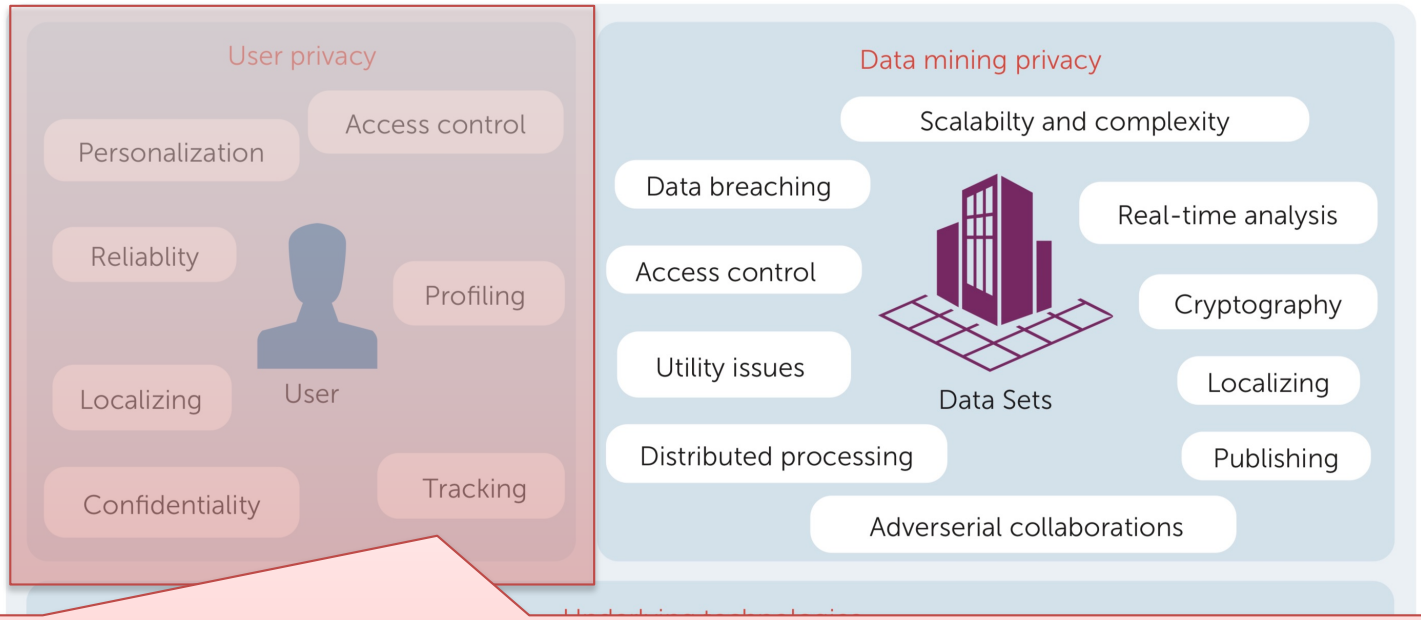
- **Jamming** attacks aim at disrupting IoT network communications and reducing the lifetime of energy-constrained nodes by creating interference and causing packet collisions.

Privacy Issues

:... Privacy Issues

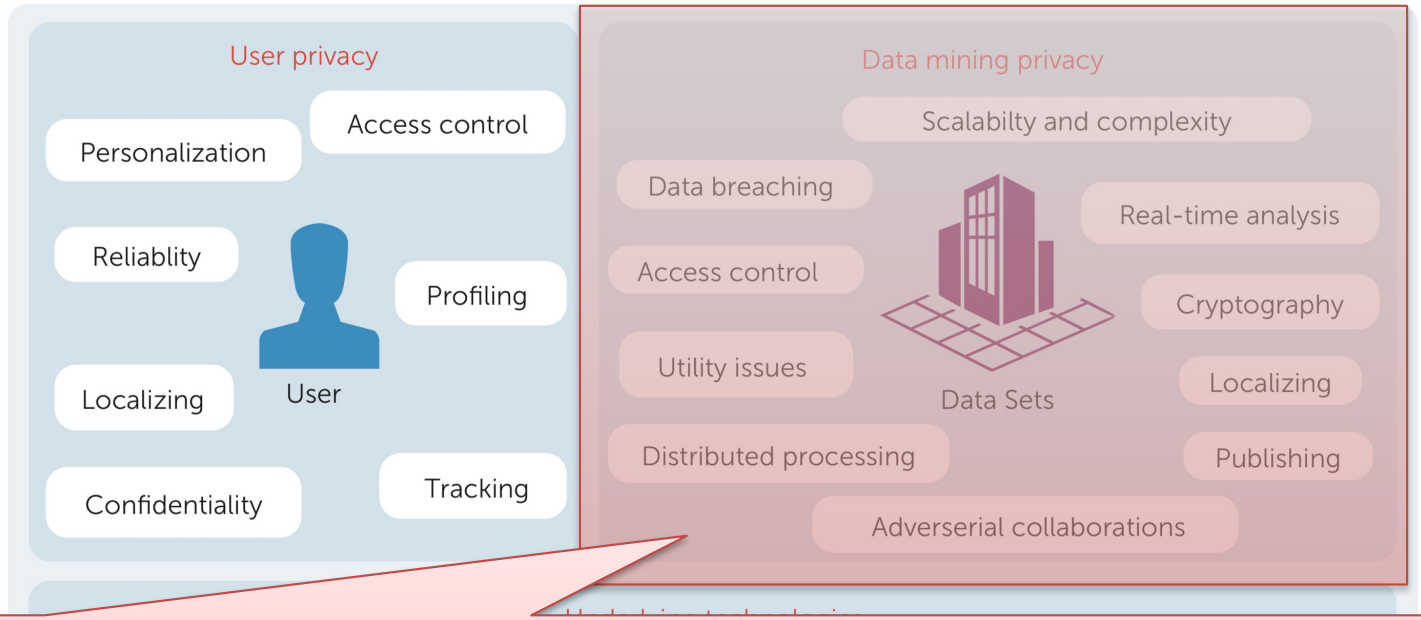


::.. Privacy Issues



The identification of personal information during transmission over the Internet is a serious concern. Possible user information leakage can lead to privacy threats in terms of tracking, localizing, and personalization, as it allows user profiling and tracking. IoT devices connected to the Internet could disclose the user's geographic location and compromise privacy.

::.. Privacy Issues



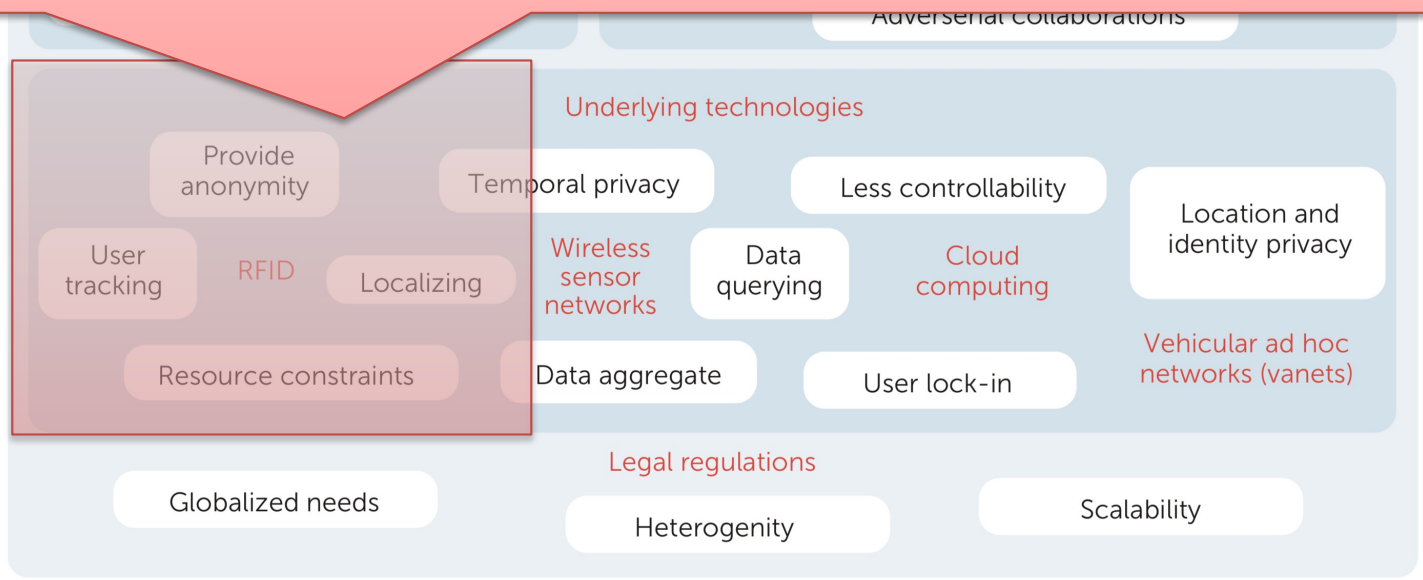
Three critical enablers of IoT privacy from a data-centric perspective are scalability, distributed processing, and real-time analytics. Other privacy issues in this area relate to data publishing, the context of applications, utility issues, cryptography, and adversarial collaboration.

::.. Privacy Issues

1. While collecting large sets of raw data, it's challenging to balance the privacy preservation in data cleaning and the intentional reduction of data quality and original purpose without losing information needed for data mining and analysis.
2. Limitations can be associated with privacy preservation over high-dimensional datasets. Because cooperative users have different privacy constraints, the records should be treated differently for anonymization purposes.
3. The collected data might be used and published for purposes other than the original objective without user consent.
4. Because computer storage mediums can store large volumes of data, they offer high availability at low cost. Consequently, once information is generated, it's most likely stored infinitely, and thus "digital forgetting" can lead to privacy violations from the data owners' perspective.

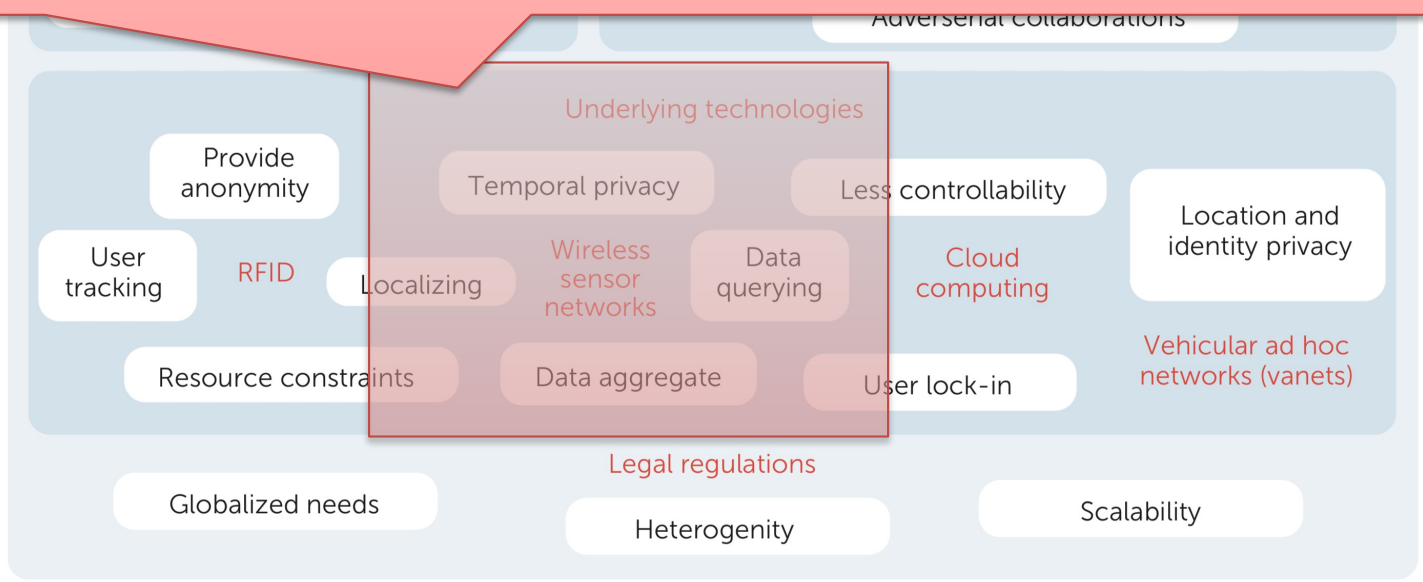
::.. Privacy Issues

RFID / NFC within an IoT environment can be exploited by powerful adversaries who can monitor all communications, trace tags within a limited time period, corrupt tags, and get side channel information on the reader output. Privacy relate to user tracking and localizing, which permit the creation and misuse of detailed user profiles. Thus, it's important to provide anonymity, even when the state of a tag has been disclosed.



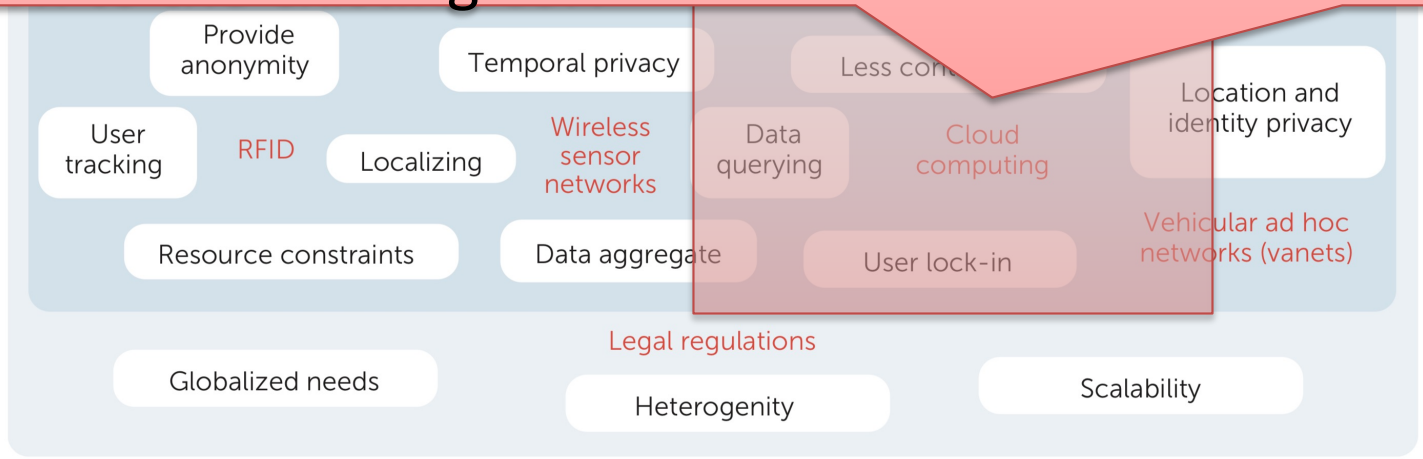
::.. Privacy Issues

WSNs have inherent challenges in protecting privacy and prevent existing techniques (such as public-key ciphers) from being directly transplanted in resource-constrained devices. Privacy in WSNs can be addressed through data orientation (i.e., querying data and aggregating sensed data without violating privacy) and context orientation (i.e., protecting location and temporal privacy).

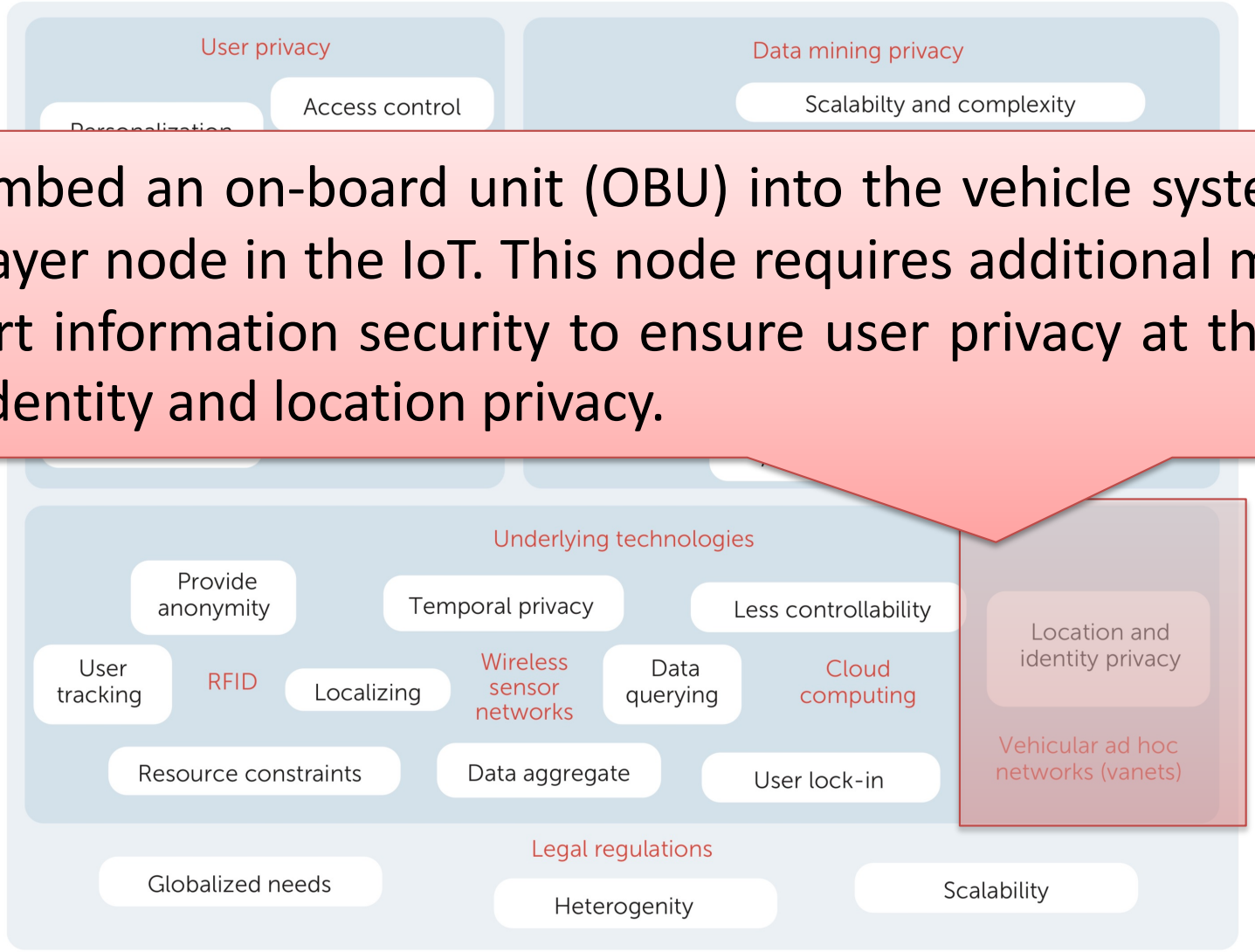


::.. Privacy Issues

With cloud computing, privacy violations can occur, as users might lack control over the data processing. Therefore, identity information, the policy components (during negotiation), and transaction histories of the consumers must be protected, as well as providing a high degree of transparency in the applied operations.
User lock-in scenarios can also occur when consumers are too dependent on a particular IoT CSP, and may be intimidated to migrate to another CPS, as that they've already revealed important information to the existing CSP.

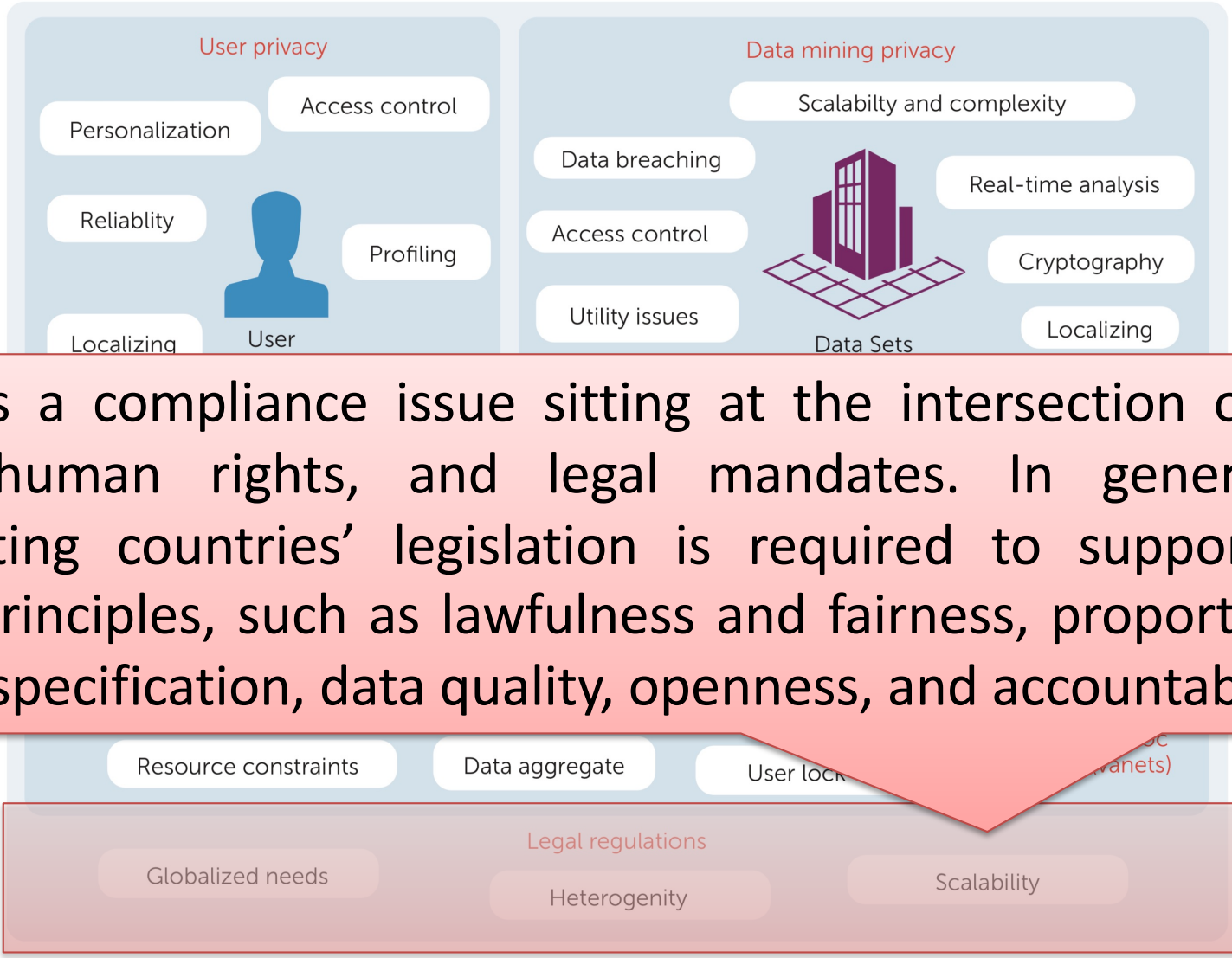


::.. Privacy Issues



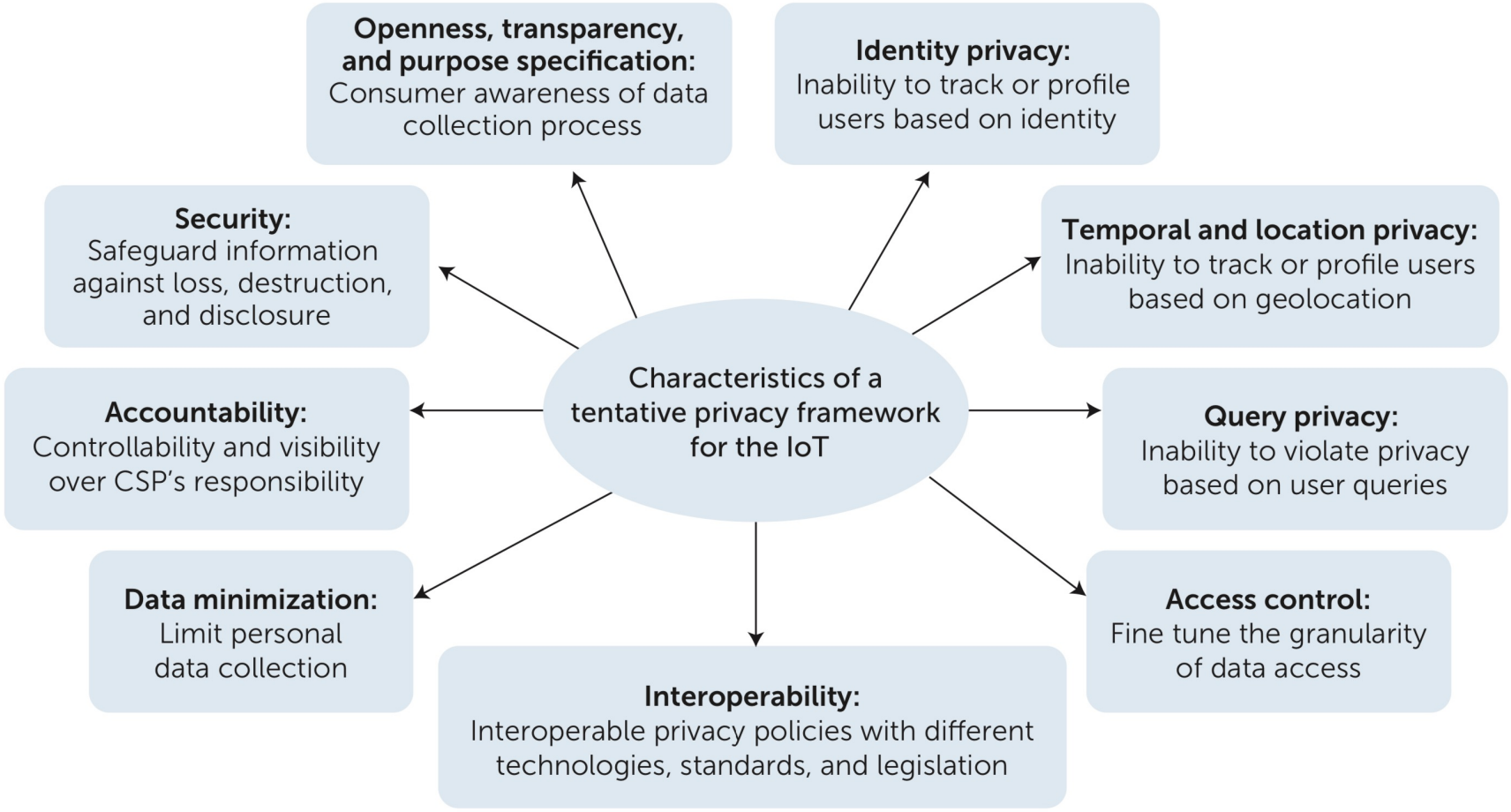
Vanets embed an on-board unit (OBU) into the vehicle system as a sensing layer node in the IoT. This node requires additional modules to support information security to ensure user privacy at the same level as identity and location privacy.

::.. Privacy Issues



Privacy is a compliance issue sitting at the intersection of social norms, human rights, and legal mandates. In general, the participating countries' legislation is required to support basic privacy principles, such as lawfulness and fairness, proportionality, purpose specification, data quality, openness, and accountability.

::.. Privacy Framework



The relevance of these principles might vary depending on the contexts of the IoT application scenarios and user requirements.

IoT Forensics

::.. Recent Cases

With the proliferation of connected devices bringing about new avenues to track and collect data, the lines between "serving justice" and protecting privacy has become blurred. The thing about IoT devices is that in order to function properly and meet the needs of their users, the devices need to collect and process large amounts of sensitive personal data about our lives, preferences, and daily activities. Needless to say, if that data is somehow compromised or ends up in the wrong hands, it would obviously be an enormous invasion of personal privacy.

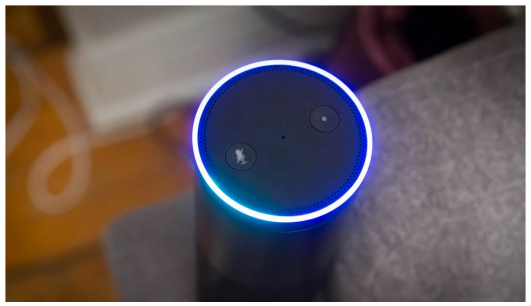
But what happens if the data stored on our devices could potentially hold key evidence in a criminal case? Can authorities demand access to the personal data collected and processed by IoT devices? Who is to decide under what circumstances such access to sensitive personal data should be authorised?

Alexa, Play My Alibi: The Smart Home Gets Taken to Court

t *WIRED*, a look at how data from smart speakers and other connected devices is used to solve crimes.

Judge orders Amazon to turn over Echo recordings in double murder case

Zack Whittaker @zackwhittaker / 5:46 PM GMT+1 • November 14, 2018 Comment



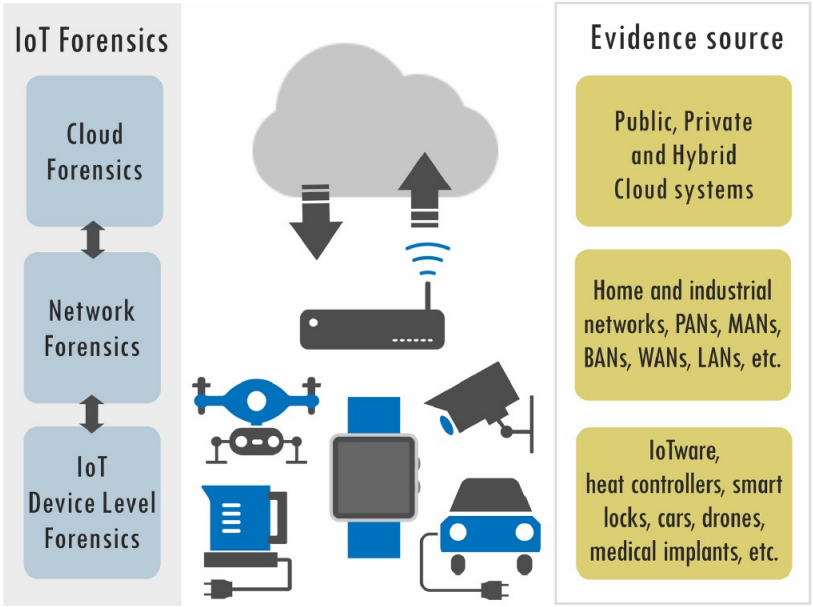
::.. Introduction (1/5)

The discipline of Digital Forensics (DF) is a branch of the traditional forensics science. It concerns the uncovering and interpretation of electronic data. DF professionals deal with the identification, collection, recovery, analysis, and preservation of digital evidence, found on various types of electronic devices.

Although there are some variations in the way different scholars divide the investigation cycle into phases, one important detail should never be missed: the whole cycle should be executed using validated tools and scientifically proven methodology.

The IoT Forensics could be perceived as a subdivision of the DF and a relatively new and unexplored area, to identify and extract digital information in a legal and forensically sound manner.

::.. Introduction (2/5)



Besides from a particular IoT device or sensor, forensic data could be gathered from the internal network (e.g., a firewall or a router) or from the cloud. Following this, IoT Forensics could be divided into three categories: IoT device level, network forensics and cloud forensics.

A fundamental difference between DF and IoT Forensics could be seen in terms of evidence source. Unlike traditional DF, where the usual objects of examination are computers, smartphones, tablets, servers or gateways, in IoT Forensics the sources of evidence could be much more wide-ranging, including infant or patient monitoring systems, In-Vehicle Infotainment (IVI) systems, traffic lights, and even medical implants in humans and animals.

::.. Introduction (3/5)

IoT Security	*IoT Forensics*
Provides security insurance for both physical and logical security issues	Determines and reconstructs the chain of events by analyzing physical evidence and electronic data
Applies diverse security techniques to minimize the scope of the attack and prevent further damage	Applies investigative techniques to identify, extract, preserve, and analyze digital information
Real-time response: implements different techniques in order to confront the threats during a live incident	Post-mortem investigation: identifies deficits after the incident occurred or while the system is inactive (however, when applying live forensics techniques, forensics professionals acquire digital evidence during a real-time incident)
Generalized: looking for any possible harmful behavior	Case-centered: reconstructing a given criminal scenario
Continuous process: keeps alert 24 hours a day	Time-restricted process: after a crime is alleged to have occurred (notitia criminis)
Security training and awareness: applies a set of security procedures, processes and standards, in order to have a securely-ready system, and prevent future cyber-threats from happening	Forensics Readiness: meets the forensics requirements and applies forensics standards, in order to be ready to undertake an investigation; takes measurements to maximize the forensic value of the potential evidence, and minimize the amount of resources spent on the investigation
Specifies the judicial region and legal aspects in service legal agreements regarding the security	Specify the judicial region and legal aspects in service legal agreements regarding the forensics issues
Well-established computer science field	Young and unexplored branch of the Digital Forensics

To secure every single sensor, communication device and cloud storage within the IoT network, is nearly impossible. If an incident happens, one of the first tasks that forensics professionals execute is to define the scope of the compromise.

However, unlike IoT security practices, forensics techniques do not aim to minimize the damage, but to identify the attack/deficit origin or the liabilities of the different parties.

IoT Forensics is motivated by the wide Attack Surface, and the advent of novel Cyber-Physical Security Threats, where some of the existing digital risks are turned them from privacy and digital security threats to physical security ones.

::.. Introduction (4/5)

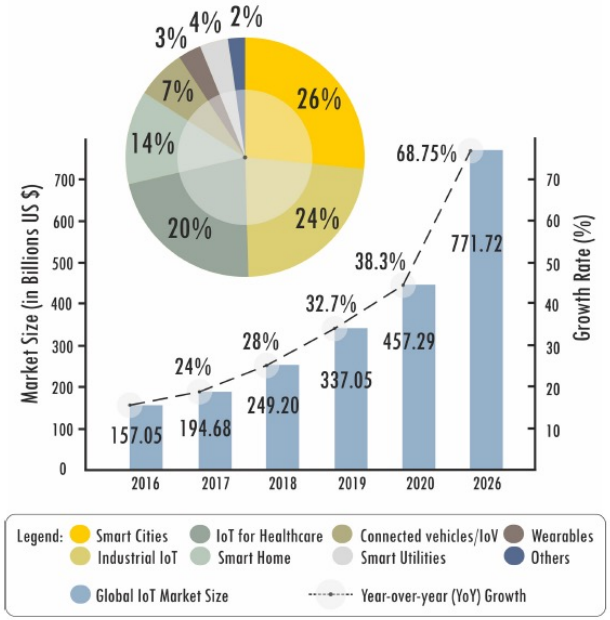
On the one hand the IoT forensics can support the analysis of the threats and improve the security and privacy efforts. Moreover, IoT installations can host a set of digital evidences to support crime investigation and judgement.

Digital traces describe a piece of information, able to prove or disprove certain hypothesis, and could therefore help the forensics professionals find answers and reconstruct the crime scene.

- Digital traces may give information about when a smart home alarm was disabled and a certain door was opened.
- The information gathered from a smoke or carbon monoxide detector could determine the exact moment and place where the fire in the building started.

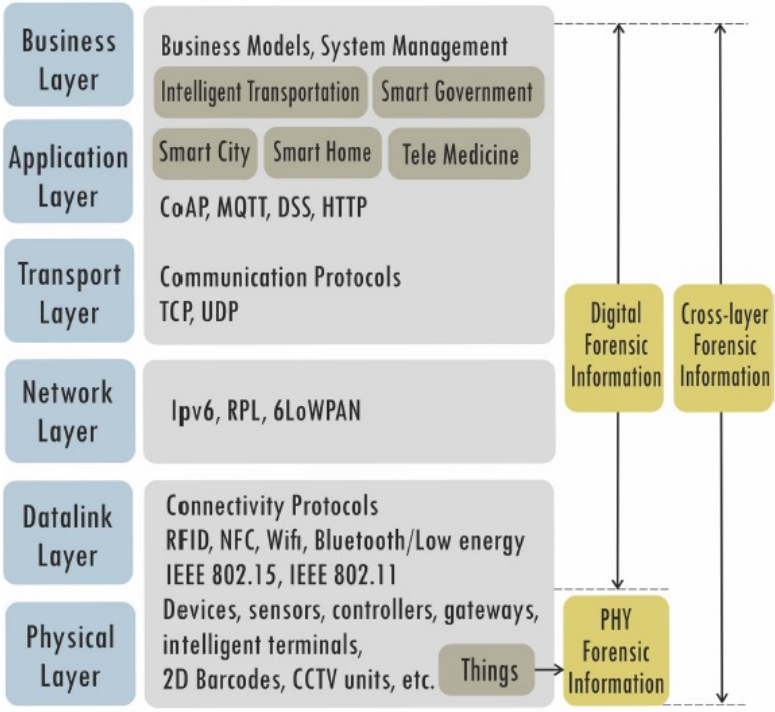
These files include sensitive information about users' identity, location, activity, as well as general linkages and chronology, and therefore must be gathered and analyzed with special attention to ethics and privacy.

::.. Introduction (5/5)

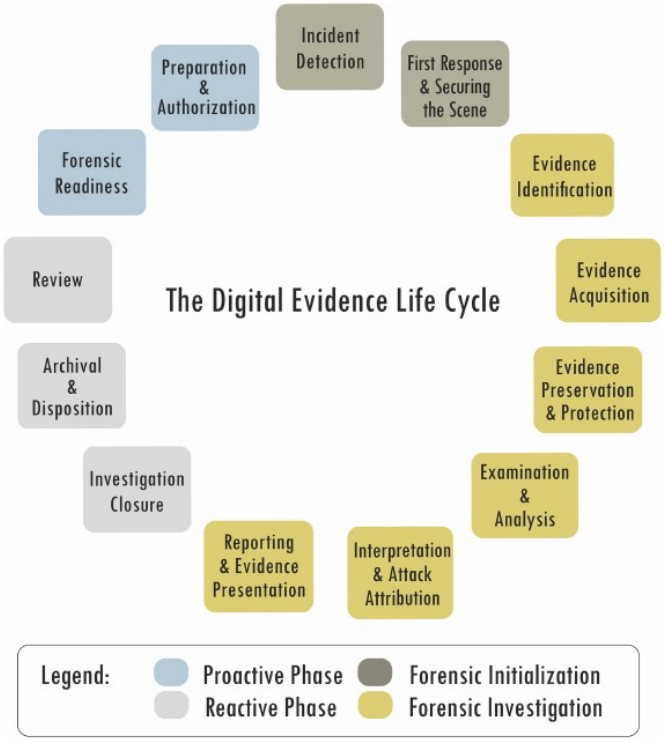


The IoT market has and will continue to experience an exponential growth over the current decade. Cloud service providers have seen this as an opportunity to establish new business models. Thereby, the ongoing Forensics-as-a-Service (FaaS) paradigm has started.

Unlike conventional computing devices which rely on traditional network security suites like endpoint protection and fire-walls, IoT communication consists of endless number of protocols, device capa-bilities and standards. Thus, IoT security relies upon securing each and every layer.



::.. Challenges (1/15)



The IoT Forensics field is encountering an array of challenges, none of which has a simple solution. A comprehensive list provided by the U.S. National Institute of Standards and Technology (NIST) identifies 65 challenges associated with cloud and IoT Forensics.

These problematic issues are grouped into seven categories, the most prominent of which is the multi-tenant nature of the cloud, followed by the complicated evidence acquisition procedure.

According to forensics practitioners, legal aspects represent another significant challenge, while researchers believe that automation in forensics is the third most important topic.

Based on the literature, the most challenging forensics aspects are divided into six groups: identification, collection, preservation, analysis and correlation, attack attribution, and finally, evidence presentation.

::.. Challenges (2/15)

The first and probably the most essential part of any forensic examination is the search for evidence. The identification in the IoT context is especially difficult, since the examiners may not even know where the investigated data is physically stored. Even a simple task like finding the compromised IoT device and reconstructing the crime scene could be challenging.

1. Scope of the Compromise and Crime Scene Reconstruction: In traditional (digital) forensics, boundary lines could be easily defined: investigators could determine the number of devices that have to be confiscated, or the number of people that were using a compromised device. The IoT context, however, implies real-time and autonomous interaction between various nodes, which makes it almost impossible to reconstruct the crime scene and to identify the scope of the damage, due to the highly dynamic nature of the communication. The data could be stored on different virtual machines (VMs), which means that important forensic data such as registry entries or temporary files could be completely erased as soon as the VM gets rebooted or turned off.

::.. Challenges (3/15)

2. Device and Data Proliferation: The increasing number of interconnected devices and the amount of digital forensic data requiring analysis, has been discussed over many years. Hence, the traditional digital forensics tools are incapable of handling such tremendous increase in volume, variety and velocity. Forensics professionals not only have to identify what is useful for the investigation, but also to discard the irrelevant data, which makes the timely analysis difficult.

3. Data Location: While operating, IoT devices could frequently migrate between different physical locations. Therefore, when attempting to locate evidence, digital forensics professionals face considerable challenges. Even if the location is known, acquiring the system is not without any complications because it could affect other customers who are using the same architecture. Moreover, the resources may be subject to multiple jurisdictions with numerous, and even contradictory regulations on data protection and unauthorized intrusions.

::.. Challenges (4/15)

4. Device Type: In contrast to the traditional digital forensics science, where the objects of forensic interest are usually limited to different types of computer systems or mobile phones, the source of evidence in IoT-centric cases could be heterogeneous. Certain IoT devices could be possibly hard to detect due to lack of battery life or because they could not be distinguished from traditional household appliances like refrigerators, dishwashers, pressing irons and baby monitors.

Assuming that the relevant IoT device has been successfully identified, the second step would be to collect the evidence data. However, at this point the investigators must deal with another problem: until the present moment, there is no guidance or standardized method for evidence collection from an IoT device in a forensically sound manner.

- “in a forensically sound manner” implies that there must be a specific procedure applied while collecting the evidence information in order to make it usable in court. Each step of the investigation process must be carefully documented in order to ensure a proper Chain of Custody.

::.. Challenges (5/15)

1. Lack of Training and Weak Knowledge Management: Law enforcement agencies should organize training programs for their first responders in order to instruct them how to acquire digital evidence in a forensically sound manner. The responding officers often unplug or shut down the system directly, without first creating the necessary forensic image. This makes evidence acquisition from IoT devices one of the most neglected steps in the practice. At the same time, by bridging the borders between decentralized on-scene units and research laboratories, the forensics practice could offer timely and legally appropriate digital and physical evidence analysis.
2. Data Encryption: the percentage of the end-to-end encrypted files has increased. However, by having full control over the cloud infrastructure, users could hide or manipulate information that cannot be recovered by the provider.

::.. Challenges (6/15)

3. Heterogeneous Software and/or Hardware Specifications: each manufacturer adopts different hardware and operating systems. Evidence data may be stored in an encrypted way or in a nonstandard format for which currently there is no applicable viewer. The files have to be decoded and converted to a readable form. In overall, in order to be able to deal with any kind of IoT crime, the investigating unit has to possess knowledge about a huge amount of systems and standards.
4. Privacy and Ethical Considerations by Accessing Personal Data: beyond technical challenges, privacy is a major issue to consider while collecting data. IoT devices deal with sensitive personal information including users' medical records, prescriptions or current health status, and may also hold data of customers who are not related to the investigation. Most of the current forensics models have rather neglected the privacy aspect.

::.. Challenges (7/15)

5. Forensic Value of Evidence: some providers of IoT services stop supporting their frameworks and seize to deliver security updates. Data gathered from such IoT devices is less valuable, because it could be easily manipulated by a hacker who took advantage of the security vulnerabilities. Apart from that, IoT data is often intermittent. In general, data from IoT devices has limited forensics value since IoT devices could work without human interference and adjust to changes in the indoor/outdoor situation accordingly.
6. Lack of a Common Forensic Model in IoT: Depending on the case, the responsible investigative body chooses different methods, but a wrong choice could have many possible complications. On one hand, the evidence gathered can easily be challenged in court. On the other hand, cross-border crimes require co-operation between investigative bodies in two or more countries. Problems are encountered in the absence of supranational agreements.

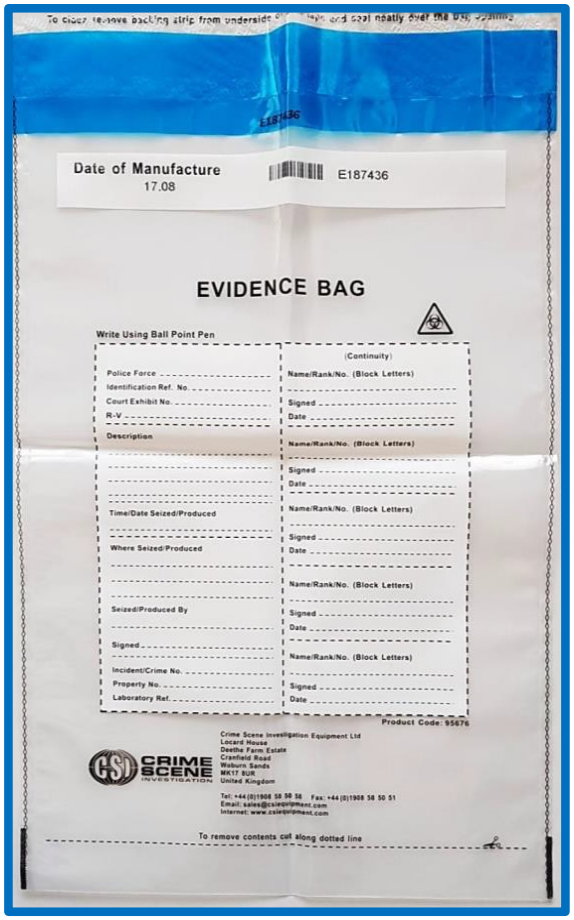
::.. Challenges (8/15)

In case investigators find one possibly compromised device and manage to collect potentially useful data, they will have to face another challenge: how to preserve the gathered data and guarantee its integrity.

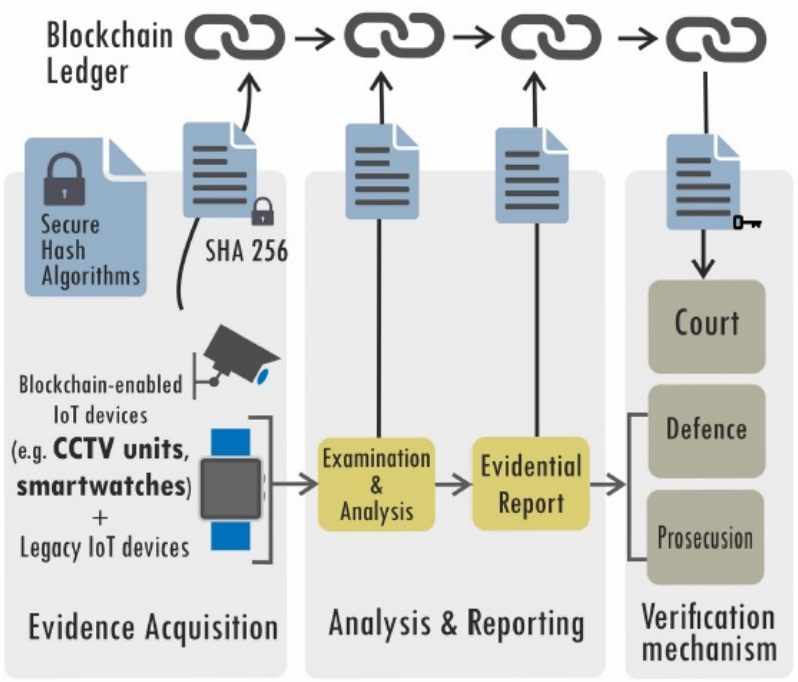
1. Securing the Chain of Custody: The term “Chain of Custody” could be defined as the accurate auditing control of original evidence material. In conventional forensics, it starts when the investigators gather a piece of evidence at the crime scene and ends with the presentation of the evidence material in court. The Chain of Custody provides clear information about when and how the evidence was gathered, preserved, analyzed and presented [97]. Moreover, it proves that the evidence material has not been altered or changed during all steps of the forensic investigation. In the case of IoT Forensics, evidence data must be gathered from multiple remote servers, which significantly complicates the mission of maintaining proper Chain of Custody.

::.. Challenges (9/15)

Due to its immaterial nature, digital evidence is especially vulnerable to manipulation, and therefore, it has to be extensively documented and protected during all steps of the forensic process.



By using blockchain a certain piece of digital information can be preserved and routed towards its final destination, the court of law.



::.. Challenges (10/15)

2. Lifespan Limitation: IoT devices have limited space, but IoT systems are running continuously, so data could be easily overwritten, resulting in the possibility of missing evidence.
3. The Cloud Forensic Problem(s): The synergy between cloud and IoT has emerged because the cloud possesses attributes which enable and benefit the IoT expansion. However, the cloud consists of a huge amount of security issues. Therefore, data preserved in the cloud has limited forensic value, since it could have been altered by a malicious user who took advantage of the vulnerabilities. Of course, no system is immune to attacks. However, cloud systems have one particular weakness that has not yet been resolved, namely the “Cloud forensic problem”: once the intruders gain access to the victim’s system, they can modify and delete whatever data they want, including completely erasing all traces of the attack. However, the distributed nature of the cloud may also be an advantage as it makes harder to erase the traces left by criminals. Digital evidence is usually mirrored in multiple places, or already hashed and indexed, which makes the collection of artefacts possible.

::.. Challenges (11/15)

4. Securing Evidence Depending on the Deployment and/or the Service Model of the Cloud (PaaS, SaaS, IaaS): From a forensics perspective, obtaining evidence in SaaS and PaaS primarily involves the service providers, while in IaaS forensics, investigators have to deal with both service providers and clients. Therefore, investigating data of an IaaS user may require less restrictions, but in the case of SaaS the access evidence information might be minimal or completely missing.
5. Data Protection and Lack of Transparency in Cloud Services: In the cloud, storage and data protection are typically performed by the IaaS vendor. Most vendors declare to encrypt users' data, but they neglect other issues such as: i) restricting the amount of data protected by a given key, ii) decreasing the amount of exposure if a certain key has been compromised, iii) limiting the time available for a physical, logical and procedural penetration attempt.

::.. Challenges (12/15)

The lack of transparency regarding the internal infrastructure of the cloud poses another challenge in the investigation process. If a user becomes involved in a criminal action, the access to the case-related information will be governed by the laws of the country where the CSP data center is located. All this could have unexpected consequences, as every state institution is allowed to acquire control over the data and freeze access to it, even if the investigation is not brought against the user from their own country of residence.

6. Data Storage Period in the Cloud: The data storage period is determined by the service provider. Legislation in different countries determines whether to store data and for how long.

Evidence Analysis and Correlation:

1. the end-to-end analysis of the existing IoT information exceeds the abilities of a single investigator or even of an investigating unit.

::.. Challenges (13/15)

2. the data provenance provides examiners with information about ownership and modification history of data objects. In IoT Forensics there is less certainty about where the data came from, as well as who or what created and/or modified the data object.
3. Time Lining and Limited Correlation of Evidence: The vast majority of IoT devices do not store any metadata. This practically makes the correlation and logical consistency of evidence, collected from multiple IoT nodes, almost impossible. Without temporal information, investigators could only speculate on the causal links.
4. Legal Issues: the legal guidance is conflicting with cross-border crimes, including the absence of clear procedural and contractual agreements. A single file could be broken down into multiple blocks located on different nodes, and thereby fall within different jurisdictions. In the worst case, this leads to a breach of the law in the state where the forensic practice is actually carried out.

::.. Challenges (14/15)

All investigation procedures aim to identify criminal parties. However, even if the evidence supports that a particular IoT node is the cause of the crime, this does not mean that the identified device will lead the investigators to the criminals.

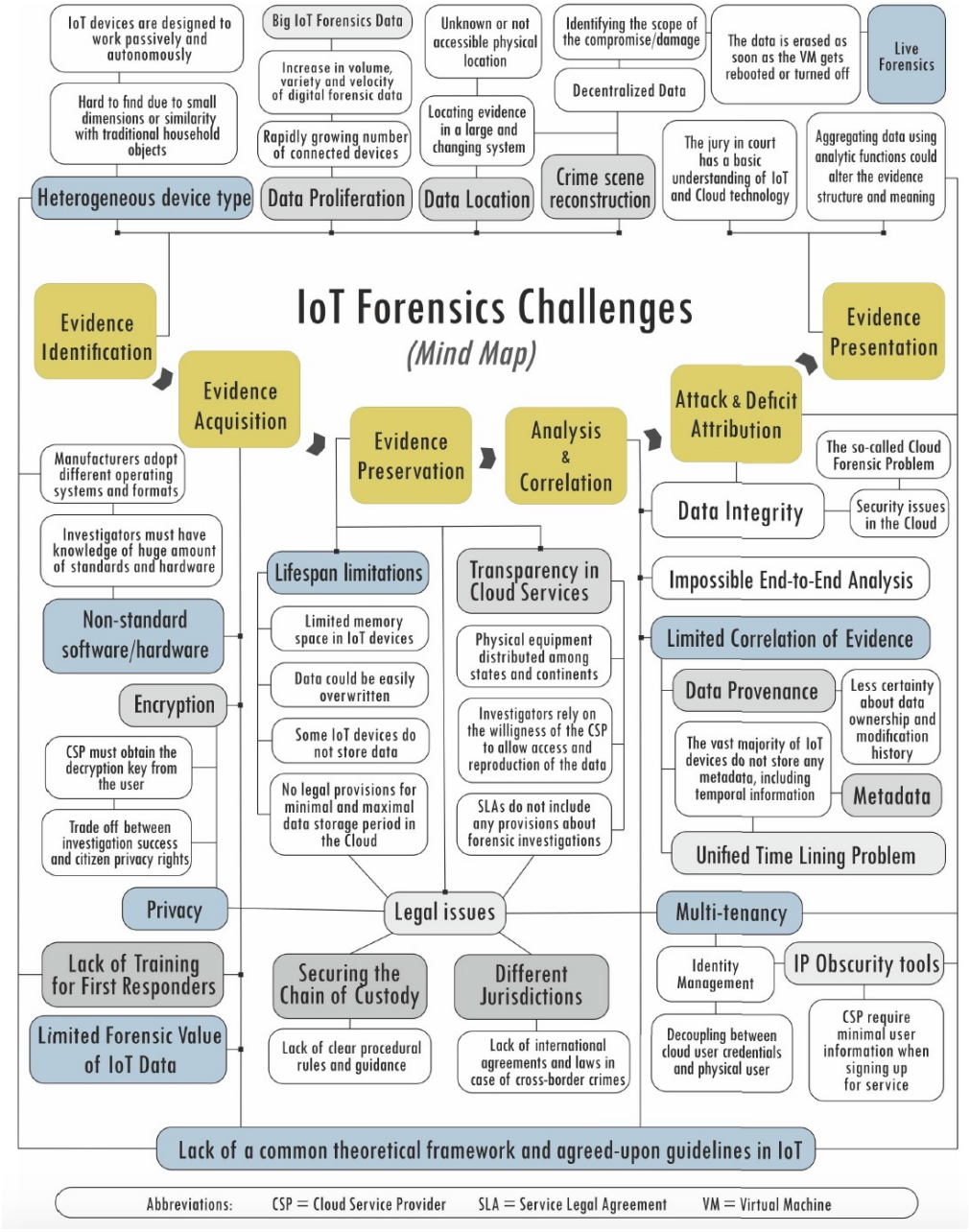
1. Lack of User Information/IP Anonymity: The adoption of IP obscurity tools complicates the tracking down of a criminal.
2. Sharing Resources and Identifying Liabilities: In the case of IoT multiple users share a physical server simultaneously. If one of the users performs an illegal activity, in a subsequent investigation, it would be very difficult to establish the truth. Therefore, forensics professionals have to pay special attention when confirming the link between digital and physical identity. Incorrect assumptions could seriously bias the investigation process. Certain presence indication events (e.g., motion detection or door opening) do not necessarily reveal someone's identity.

::.. Challenges (14/15)

If the geolocation information extracted from a certain IoT device suggests that it was present at the crime scene in the moment of the incident, forensics examiners have to make sure that the device location and time settings were set accurately. Furthermore, the investigators should determine if the device was also used by another person at the same time.

Presenting the findings of an IoT-centric case poses some new challenges. There are legal systems that require presentation of the evidence in front of a panel of jurors in the courtroom. Before being questioned and chosen by the judge and/or the attorneys, the potential jurors (also known as the “voir dire”) were picked among the community using a reasonably random method. The jury most probably has only basic understanding of involved technologies, based on the media or their personal experience with IoT technology.

:.. Challenges (15/15)



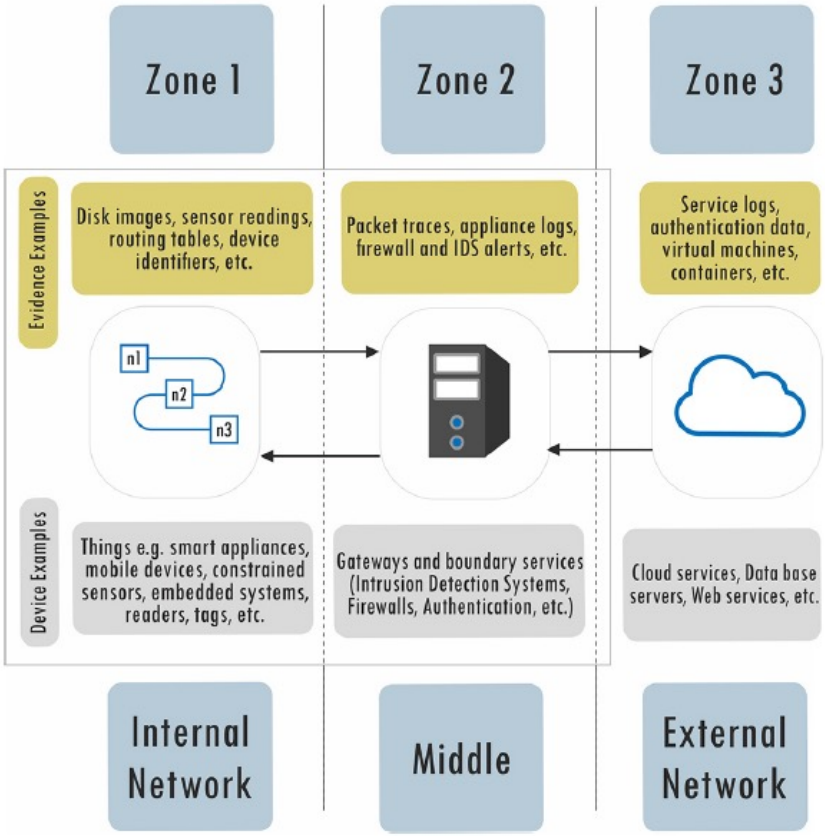
::.. IoT Forensics Approaches (1/8)

Within the IoT, traditional investigative techniques have a very low success rate. There are various theoretical frameworks to choose from, even though they all adopt similar major stages. In the end, the choice of approach mainly depends on the assessment of the investigative body.

Over the last 25 years, many forensic frameworks have been proposed and evolved based on the ever-changing technology, cybercrime attack patterns, experience on evidence admissibility, and government/public interest.

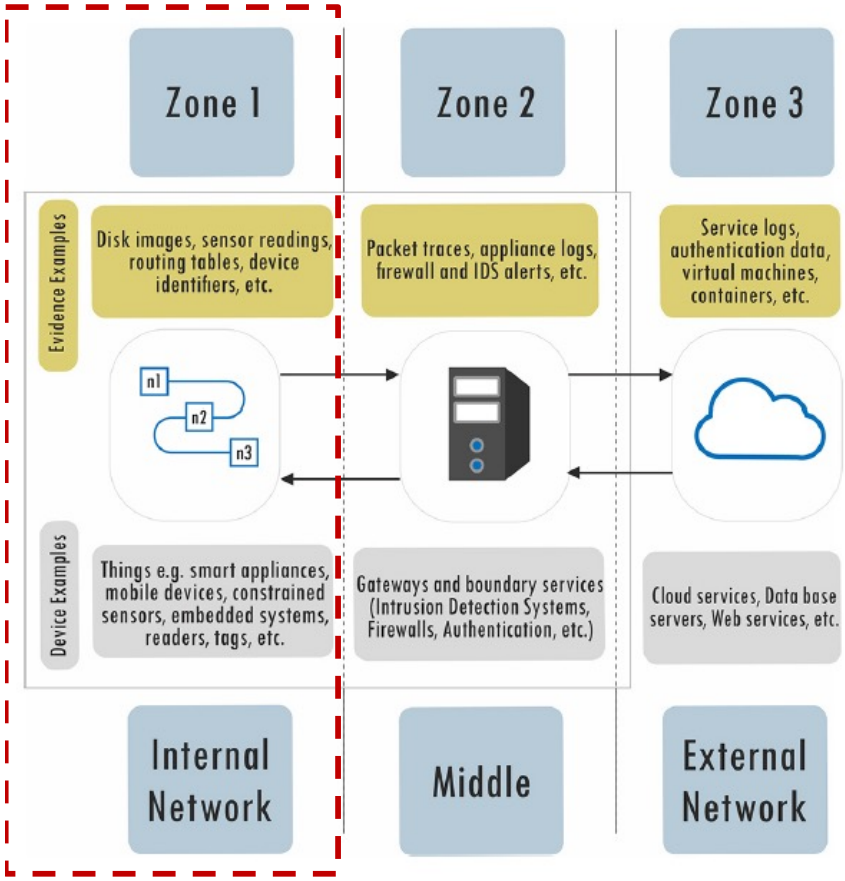
The 1-2-3 Zones Approach may not be among the most recent developments, but it is perhaps the most cited theoretical framework in the Digital Forensics science. The method reduces the complexity and the timing of investigations, which means that the authorities can focus their attention on substantial tasks and by doing so, achieve greater efficiency.

::.. IoT Forensics Approaches (2/8)



The method divides the IoT Forensics into three zones.

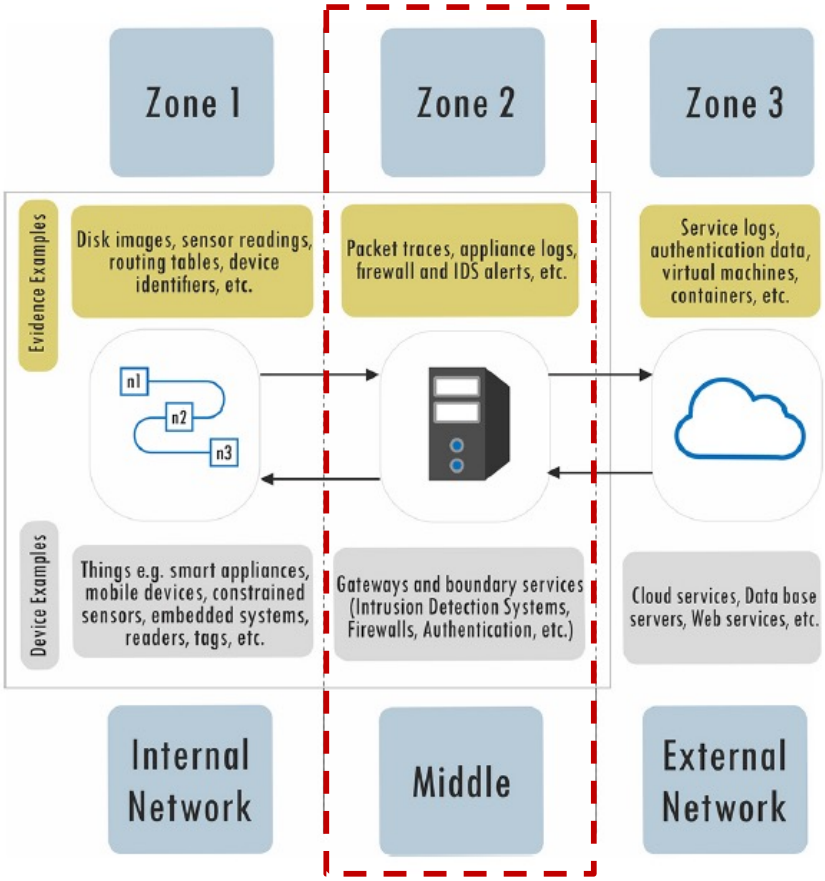
::.. IoT Forensics Approaches (2/8)



The method divides the IoT Forensics into three zones:

- The first zone covers the entire internal area consisting of hardware, software and networks. Here, the initial evidence is collected. One can also identify tag identities and their state. The investigator may decide to pay special attention to this area, if there is access to sites of forensic interest and/or open physical devices.

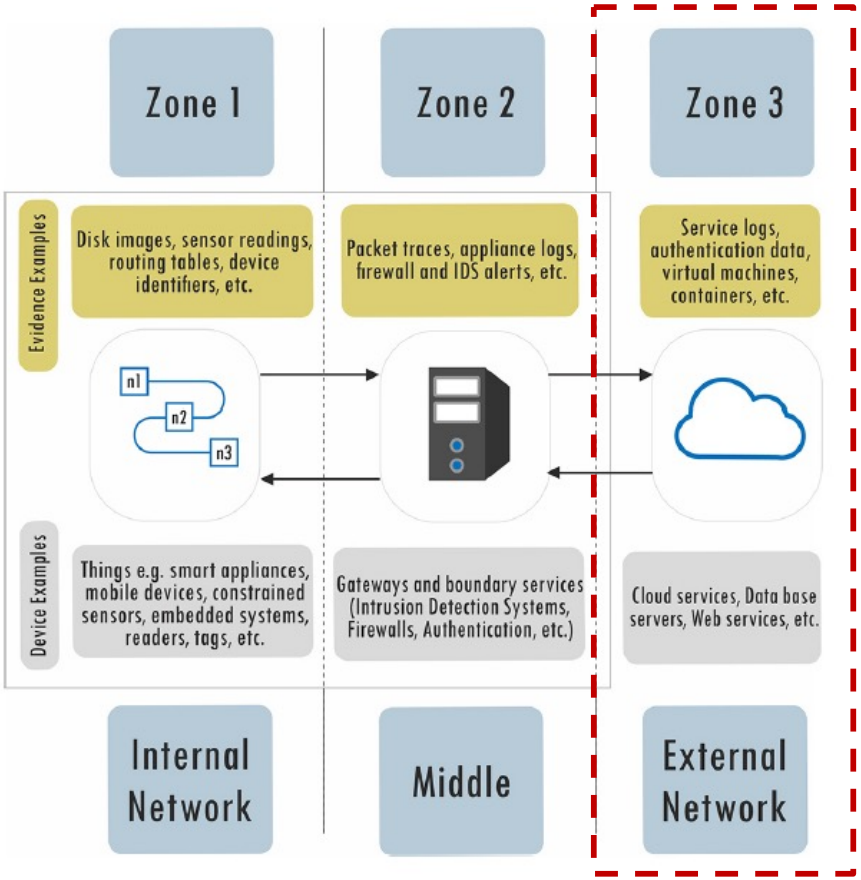
::.. IoT Forensics Approaches (2/8)



The method divides the IoT Forensics into three zones:

- The second zone includes all the devices and software that connect the internal (Zone 1) to the external area (Zone 3). This area includes mainly public devices and infra-structure, intrusion prevention and detection systems, and network firewalls. During the investigation, it is necessary to gather maximum evidence by requiring assistance from the respective providers.

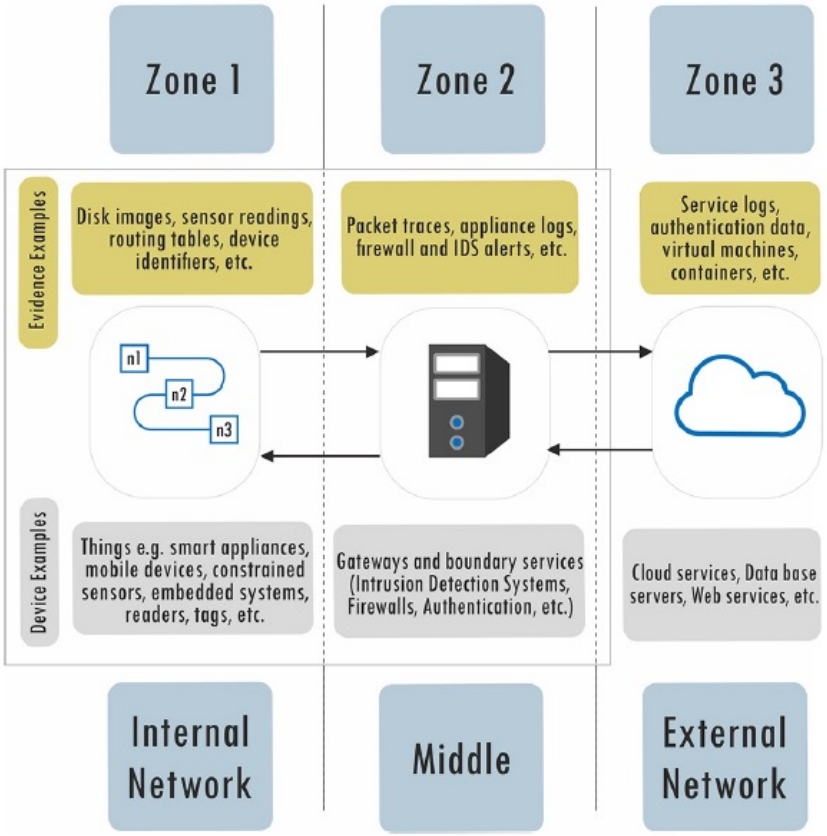
::.. IoT Forensics Approaches (2/8)



The method divides the IoT Forensics into three zones:

- The third zone covers all hardware and software that is outside of the network in question. E.g., all cloud, social network, Internet Service Provider (ISP) and mobile network providers' data, or Internet and Web-based services, virtual online identities, edge network, inter-network evidence, device-based evidence, Gateway or edge devices, etc..

::.. IoT Forensics Approaches (2/8)

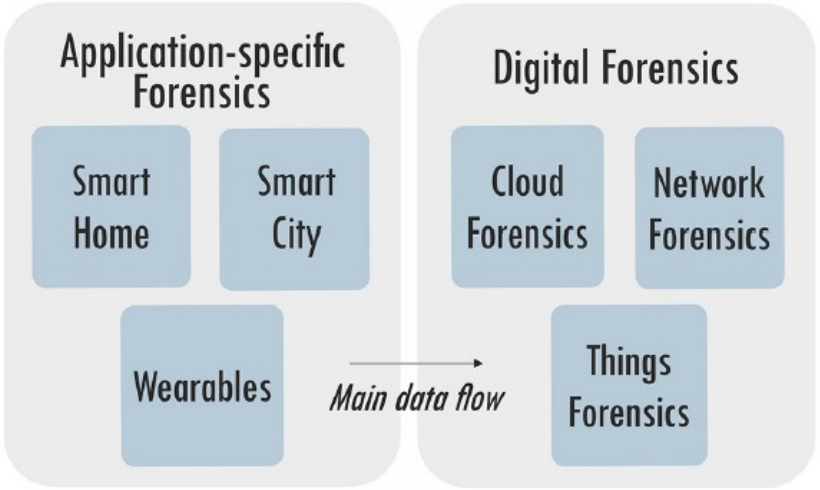


The method divides the IoT Forensics into three zones.

Another well-established Digital Forensics model is the Next-Best-Thing Triage (NBT) Model, which is highly likely to prove that data originated from a device that is no longer physically available. It helps the investigators to "arrange the puzzle" and gather enough evidence of a crime.

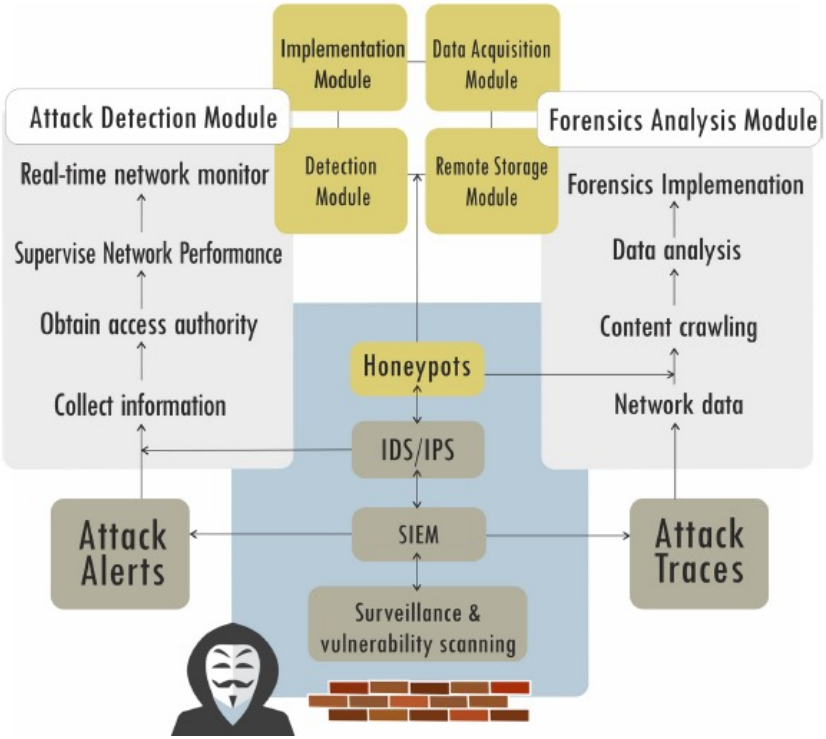
The Digital Forensics Investigation Framework for IoT (DFIF-IoT) is a generic framework complaint with ISO/IEC 27043: 2015, a still valid, internationally recognized standard on incident investigation principles.

::.. IoT Forensics Approaches (3/8)



The Application-Specific Digital Forensics consists of three independent components: Application specific Forensics, Digital Forensics and Forensics Process. Each of them comprises several other topics.

Security and forensics practices are treated as completely separated processes, which could result in lag of forensic response and loss of evidence. A possible solution to this problem may be a hybrid incident detection and forensics model



::.. IoT Forensics Approaches (4/8)

The Digital Forensics Readiness (DFR) term represents the capability to "collect, preserve, protect and analyze Digital Evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or in a Court of law"

Digital forensics approaches should not only be used in post-incident activities, but also to increase the chances of obtaining good results or spending less resources in future investigations. Ergo, DFR could be understood as the proactive phase in a cyber investigation.

Many modern-day organizations have already recognized the need for being forensically ready. Even though it has been acknowledged as a highly recommended objective, the integration of Forensics Readiness into IoT systems remains challenging.

::.. IoT Forensics Approaches (5/8)

One of the main factors that minimize the potential value of the evidence and, at the same time, double the recourses needed to conduct a forensic investigation, is the rise of antiforensics techniques.

Cybercriminals are aware of the way digital forensics tools work. As the defensive mechanisms become increasingly efficient, even more sophisticated encryption and obfuscation techniques should be expected.

In order to deal with the aggressive deployment of anti-forensics methods, researchers and investigators need to come up with improved, proactive and standardized IoT Forensics tools.

::.. IoT Forensics Approaches (6/8)

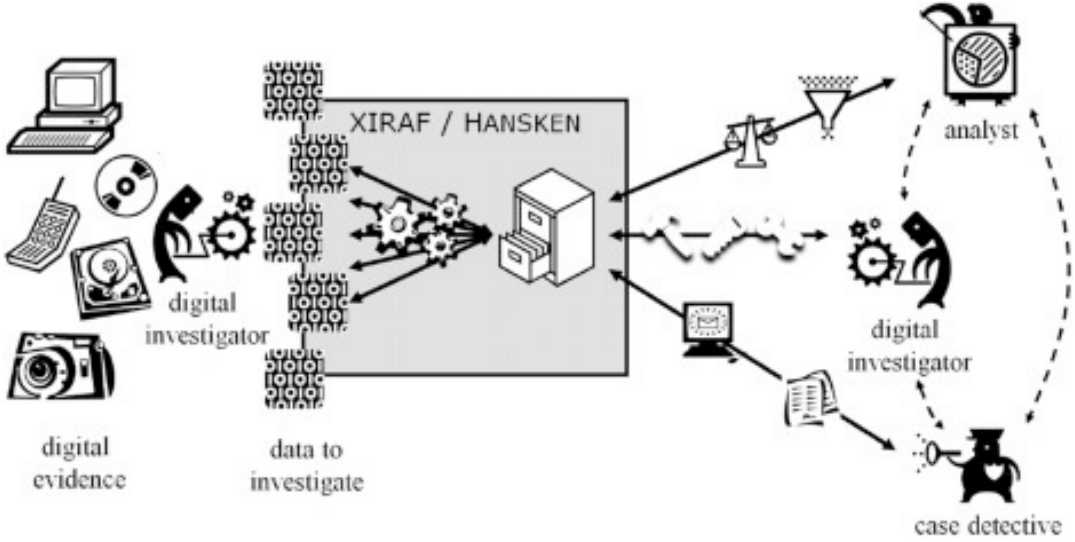
Law enforcement agencies, legal authorities and governments struggle to address all resulting open legal problems and multi-jurisdictional disputes. Within the context of IoT, it is unclear under which law the case should be prosecuted: the device jurisdiction, the attacker jurisdiction, or the data storage jurisdiction. It is necessary to create an international commission, to define uniform procedures.

Collaboration deficiencies could be found not only on international level, but also between local law enforcement agencies, incident responders and forensic laboratories. Some problems may arise, especially if the forensics investigators have to deal with an IoT device unknown to the practice.

An automated technical solution for bridging this knowledge gap between incident responders and forensic laboratories is to “codify” the digital forensics process and make it easily accessible to the police officers at the crime scene via a secure Web-based interface.

::.. IoT Forensics Approaches (7/8)

The Hansken system, developed by the Netherlands Forensics Institute, is a successful example of an automated processing and reporting system for digital traces, available to review remotely during fieldwork.

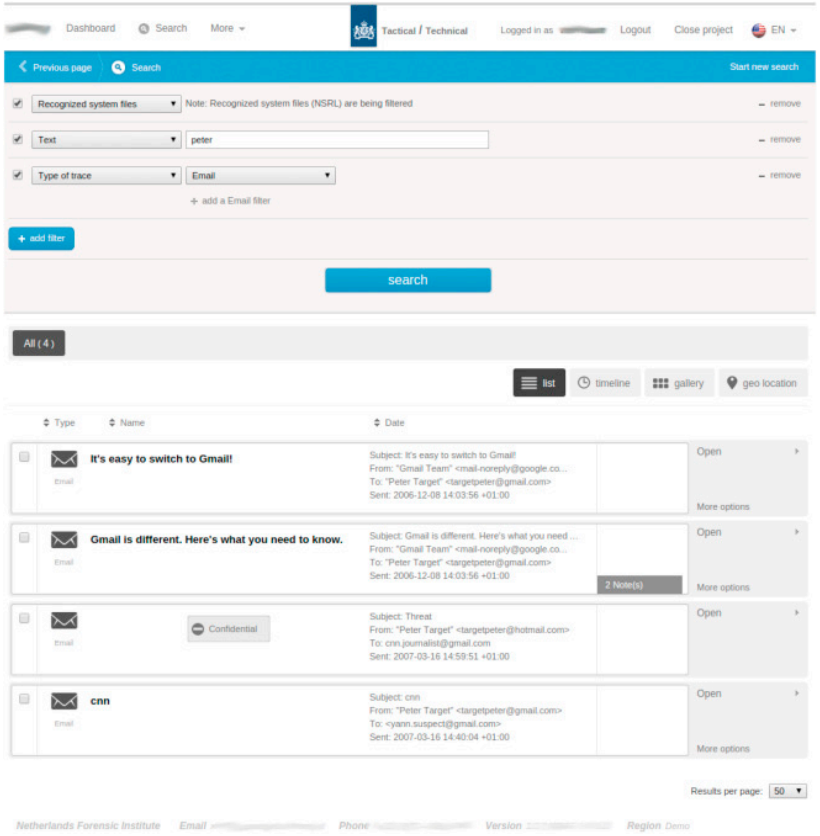


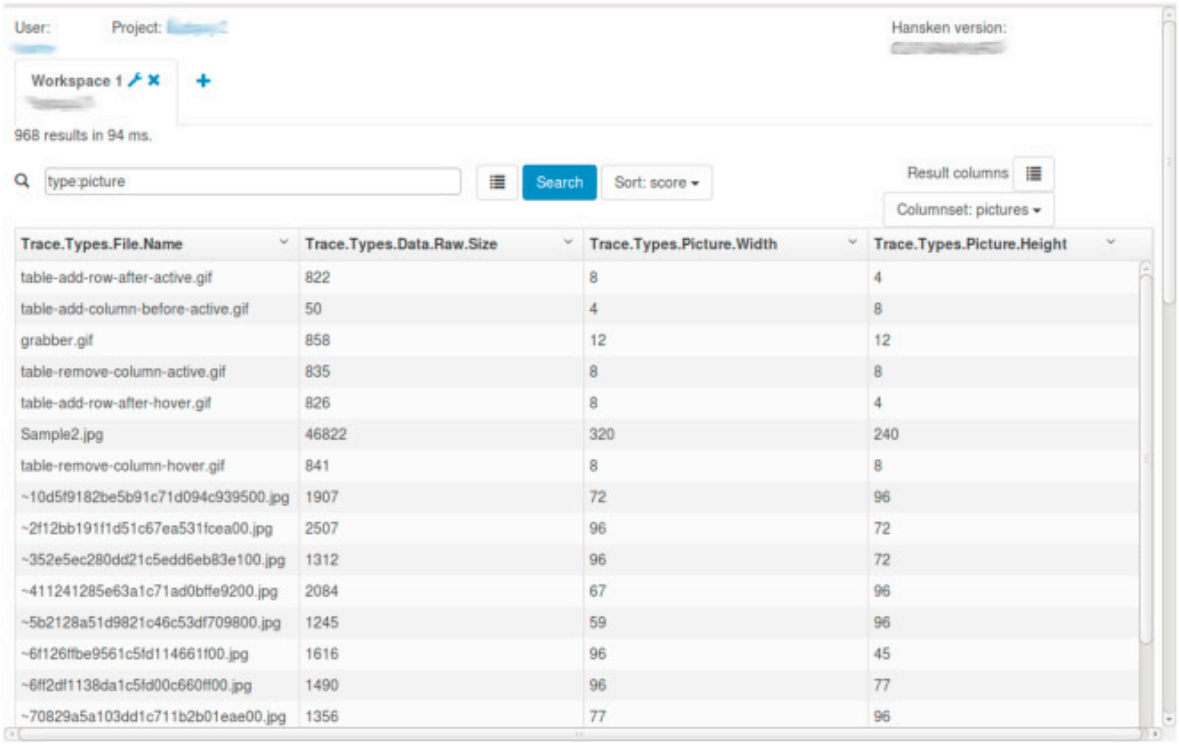
It provides Digital Forensics as a Service to the Dutch law enforcement organizations. The digital evidences are copied to a central storage and processed using a standard set of tools.

The results of these tools, i.e. the extracted metadata, are stored in a centralized database and queried using multiple methods. Digital investigators can use the programming interface to run automated tools and scripts written in their favorite programming language. Analysts may want to retrieve all information and analyze the results using data visualization tools, integrate additional data sources or build a network of contacts, for example.

::.. IoT Forensics Approaches (8/8)

Two graphical user interfaces have been developed: a tactical user interface, aimed at detectives, and a technical interface, aimed at digital investigators. Both interfaces provide the same functionality, however the tactical interface is more explicit in the possible queries that can be performed and shows less technical details.





Trace.Types.File.Name	Trace.Types.Data.Raw.Size	Trace.Types.Picture.Width	Trace.Types.Picture.Height
table-add-row-after-active.gif	822	8	4
table-add-column-before-active.gif	50	4	8
grabber.gif	858	12	12
table-remove-column-active.gif	835	8	8
table-add-row-after-hover.gif	826	8	4
Sample2.jpg	46822	320	240
table-remove-column-hover.gif	841	8	8
~10d5f9182be5b91c71d094c939500.jpg	1907	72	96
~2f12bb191f1d51c67ea531fcea00.jpg	2507	96	72
~352e5ec280dd21c5edd6eb83e100.jpg	1312	96	72
~411241285e63a1c71ad0bffe9200.jpg	2084	67	96
~5b2128a51d9821c46c53df709800.jpg	1245	59	96
~6f126ffbe9561c5fd114661f00.jpg	1616	96	45
~6ff2df1138da1c5fd00c660ff00.jpg	1490	96	77
~70829a5a103dd1c711b2b01eae00.jpg	1356	77	96