SEOULTECH

Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations

2019.10.01

Presented by:
Mikail Mohammed Salim
Jin Seong Park

SeoulTech UCS Lab
Ubiquitous Computing & Security Laboratory

SEOULTECH

Abstract

- The security issue affecting the Internet-of-Things (IoT) has attracted significant attention from the research community.
- The paper presents a taxonomy to discuss IoT vulnerabilities, their attack vectors, and impacts on various security objectives.
- The research aims to acquaint us with research related to IoT vulnerabilities, including their technical details and consequences.
- Related remedial methodologies and capabilities to monitor such weaknesses are present.
- Open research issues and challenges are discussed to pave way for future research in IoT security.

SEOULTECH

Contents

SEOULTECH

Introduction

- The concept of IoT device consumption is both people and safety centric. The aim is to improve the quality of life.
- IoT machines with grave security vulnerabilities are sold in the market without basic security protocols.
- Poor security authentication protocols have led to DDoS attacks such as the Mirai based botnet attack on Dyn, a DNS provider.
- The major threat from IoT security based vulnerabilities is upon the human well-being.
- These devices have poor computational capabilities, limited storage and battery power.
- The most basic security flaw is the usage of common security credentials across all devices manufactured by a vendor.

SEOULTECH

Introduction

- This paper addresses the lack of an exhaustive study of IoT vulnerabilities.
- It combines and classifies current IoT-related research literature to highlight research trends.
- The authors propose a taxonomy to discuss IoT vulnerabilities based on research of existing studies.
- Utilizes empirical data to present the spread of infected devices on a worldwide scale, industries that host them and vendors that sell unsecure devices.
- Challenges and open issues are discussed based on the proposed taxonomy to help facilitate future research.

SEOULTECH

Related surveys

Year of publication	2010	2013		2014		2015			2016				2017					2018
Research area	[22]	[23]	[24]	[25]	[26]	[27]	[28]	[29]	[30]	[31]	[32]	[33]	[34]	[35]	[36]	[37]	[38]	[39]
Protocols and Technologies	●	●	○	●	○	●	○	●	●	○	○	○	●	●	○	●	○	●
Application domains	●	●	○	●	○	●	○	○	●	○	○	○	○	○	○	●	○	●
Context awareness	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○
Legal frameworks	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○
Attacks	○	○	●	○	○	○	○	○	○	○	○	●	●	○	●	●	○	●
Access models	○	○	●	○	○	○	●	○	○	○	○	○	○	●	●	●	○	○
Security protocols	○	○	●	○	○	○	●	●	○	○	○	○	●	○	○	●	○	○
Intrusion detection techniques	○	○	○	○	○	○	○	○	○	○	●	○	○	○	●	○	●	○

Legend: ● area has been covered in the survey, ○ area has not been covered

SeoulTech UCS Lab
Ubiquitous Computing & Security Laboratory

SEOULTECH

Related surveys

IoT architectures and corresponding technologies

- Atzoria et al. [1] reviewed application domains, research challenges. The authors discussed the importance of security and highlighted IoT device weaknesses disallow complex security mechanisms.
- Gubbi et al. [2] discussed challenges in IoT-centric application domains and presented a cloud-focused vision for the implementation of the IoT. The authors suggest that cloud security is of prime importance to fully secure IoT environment.
- Da Xu et al. [3] presented core IoT enabling technologies in the context of their industiral application. Characteristics of IoT such as deployment, mobility and complexity suffer from vulnerabilities that make them not ideal for industrial usage.
- Al-Fuqaha et al. [4] reviewed IoT application domains, enabling technologies, their roles and analyzed numerous challenges for IoT security. The authors suggest a lack of common standards among IoT architectures is a major obstacle to protect IoT from cyber attacks.

SEOULTECH

Related surveys

IoT architectures and corresponding technologies

- Atzori et al. [5] discussed the evolution of IoT and suggest that current technological advances help in the next evolutional growth of IoT devices.
- Perera et al. [6] described the IoT from a context-aware perspective and studied 50 different projects to analyze their applicability. The security and privacy functionalities of the projects are discussed. The authors note that there are security and privacy concerns in the middleware layer.

IoT security

- Sicari et al. [7] discussed available solutions for IoT security. Despite these solutions, the authors conclude that many challenges and research questions remain open such as a systematic and a unified vision to guarantee IoT security.
- Mosenia and Jha [8] presented numerous IoT targeted attacks and pinpointed their possible mitigation approaches. The authors suggest a proactive approach to secure the IoT environment.

SEOULTECH

Related surveys

IoT security

- Ouaddah et al. [9] presented a quantitative and a qualitative evaluation of available access control solutions for IoT. The research suggests that centralized and distributed approaches could support each other when designing access control for IoT environment.
- Roman et al. [10] discussed the challenges of a distributed architecture for IoT security. The research concluded that while a distributed architecture may reduce the impact of an attack, it may also increase the number of attack vectors.
- Gendreau and Moorman [11] reviewed intrusion detection techniques proposed for the IoT and suggest that IDS in IoT are still in its infancy. The primary challenge is prevention of unauthorized access in IoT device due to poor computational power.

SEOULTECH

Methodology

- The survey represents findings from 100 research works from 2005-2018.
- Meticulously studies work to investigate relevant, common and impactful IoT vulnerabilities.
- Categorized weaknesses based upon their impact on security objectives such as confidentiality, integrity and availability.
- To identify defense techniques, the authors selected research contributions that analyzed, defined or simulated an attack.
- Analyzed research to study mechanisms which to monitor IoT generated malicious activities and identify attacks against IoT environments.
- IEEE and ACM libraries were explored to accomplish literature work.

SEOULTECH

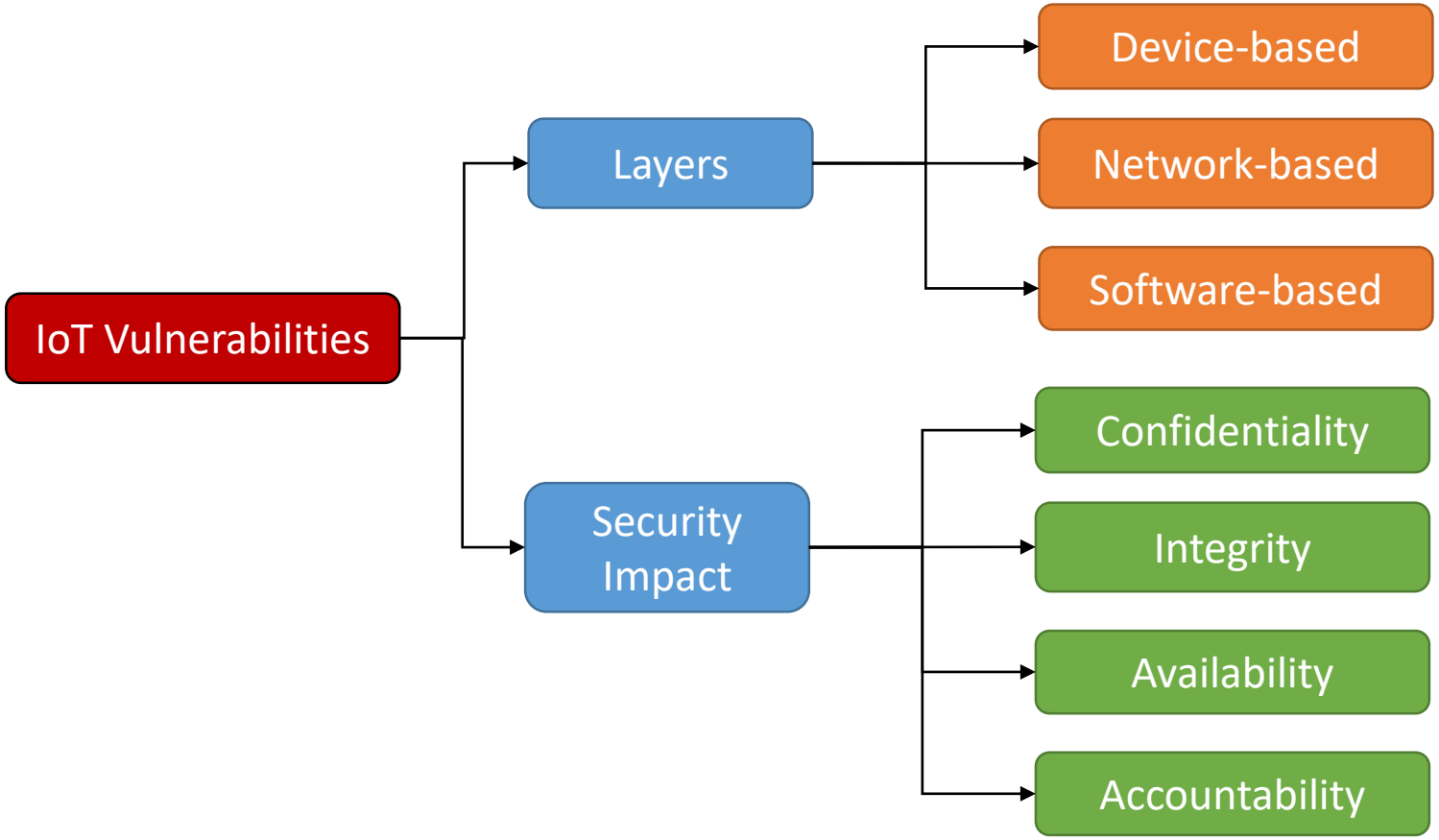
Taxonomy of IoT Vulnerabilities

Identified IoT vulnerabilities:

- Deficient physical security
- Insufficient energy harvesting
- Inadequate authentication
- Improper encryption
- Unnecessary open ports
- Insufficient access control
- Improper patch management capabilities
- Weak programming practices
- Insufficient audit mechanisms

SEOULTECH

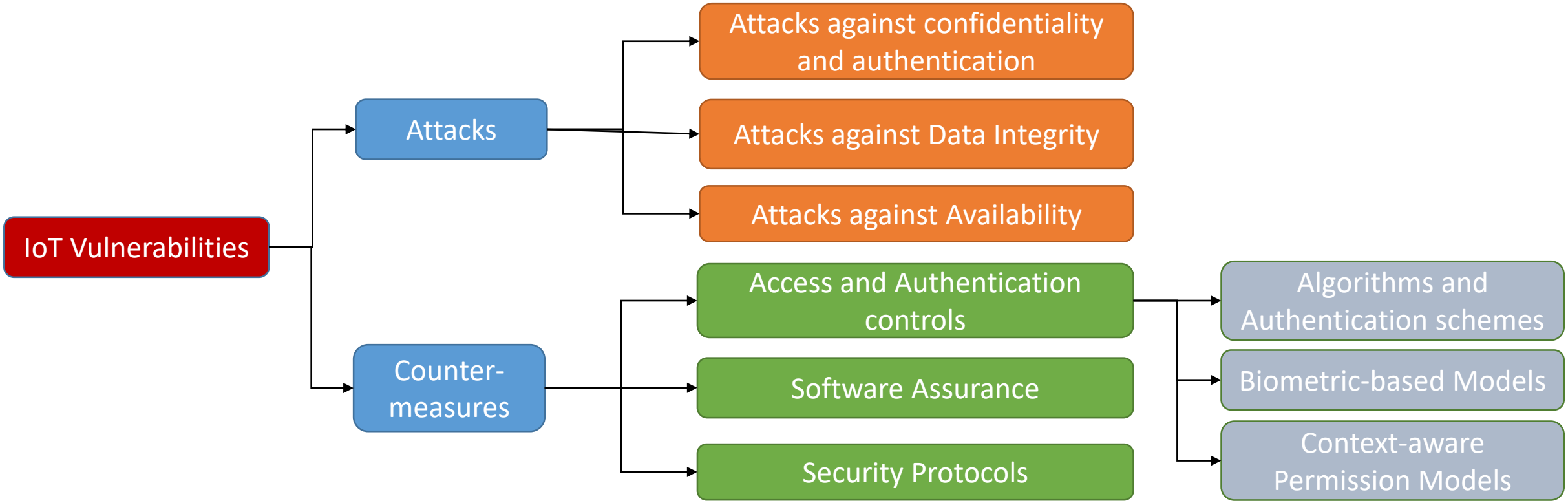
Taxonomy of IoT Vulnerabilities



Categorization of IoT vulnerabilities

SEOULTECH

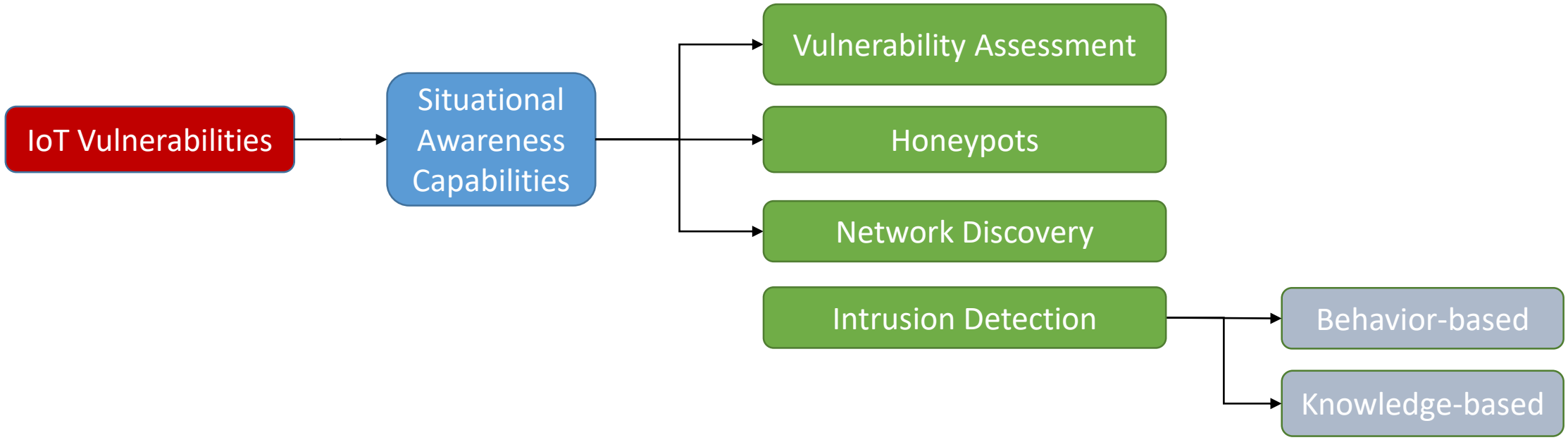
Taxonomy of IoT Vulnerabilities



Categorization of IoT vulnerabilities

SEOULTECH

Taxonomy of IoT Vulnerabilities



Categorization of IoT vulnerabilities

SEOULTECH

Taxonomy of IoT Vulnerabilities

Layers: Device based vulnerabilities:

- IoT devices are generally left to operate without any physical monitoring. An attacker can access data stored in its memory.
- Wurm et al. [12] demonstrated that physical access to device allows an attacker to modify boot parameters, obtain password and private data.
- The authors executed energy theft by modifying ID of the smart meter. Due to lack of encryption at device level, several network attacks were carried out.
- Trappe et al. [13] highlighted device vulnerabilities due to low power of devices. Energy harvesting is proposed to power devices and adopt complex security mechanisms.

SEOULTECH

Taxonomy of IoT Vulnerabilities

Layers: Network based vulnerabilities:

- ZigBee devices establish secure communications by using symmetric keys while the level of sharing of such keys among nodes depends on the security mode.
- Vidgren et al. [14] illustrated how ZigBee-enabled IoT devices are compromised as transmission of keys are unencrypted. Data can be leaked by attacker and device control lost.
- Petroulakis et al. [15] experimentally investigated the correlation between energy consumption and security mechanisms such as encryption.
- Due to low energy in IoT devices, device availability is affected if strong security measures are implemented as shown in the below table:

Security mechanism	Effect on energy consumption
Encryption	$\Uparrow 15-30\%$
Channel assignment	$\Uparrow 10\%$
Power control	$\Uparrow 4\%$
All three above	$\Uparrow 230\%$

SEOULTECH

Taxonomy of IoT Vulnerabilities

Layers: Network based vulnerabilities:

- Simplicio et al. [16] demonstrated that many existing lightweight key agreement schemes have the drawback of key escrow problems.
- The authors evaluated escrow-free alternatives to estimate their suitability for IoT and concluded that the Strengthened MQV (SMQV) protocol is a more efficient alternative for other lightweight solutions.
- Another network based vulnerability is based on port blocking policies. Czyz et al. [17] explored IoT connectivity over IPv4 and IPv6.
- The authors noted that Telnet service in 46% of the cases was accessible over IPv6 than IPv4.
- IoT network operators confirmed that these default set open ports are left open unintentionally. This has a major impact on IoT security.

SEOULTECH

Taxonomy of IoT Vulnerabilities

Layers: Software based vulnerabilities:

- Attackers are able to gain remote access to IoT devices by exploiting software vulnerabilities.
- Angrishi [18] explored IoT-centric malware, which recruited IoT devices into botnets for conducting DDoS attacks.
- The researcher uncovered that 90% of investigated malware injected default or weak user credentials, while only 10% exploited software-specific weaknesses.
- Referring to the Carna botnet, Markowsky and Markowsky [19] noted that it unveiled more than 1.6 million devices throughout the world that used default credentials.
- Patton et al. [20] analyzed the search engine Shodan to index IoT devices that have been deployed in critical infrastructure and executed queries with default credentials to gain access to the devices.

SEOULTECH

Taxonomy of IoT Vulnerabilities

Layers: Software based vulnerabilities:

- Cui and Stolfo [21] uncovered 540,000 devices that were using default credentials in government organizations, ISPs and educational institutions.
- Costin et al. [22] performed a large-scale analysis of embedded firmware. The authors were able to recover plaintext passwords from almost 55% of retrieved password hashes.
- Konstantinou and Maniatakos [23] demonstrated how malicious firmware of power grids could corrupt control signals and cause a cascade of power outages.
- Though public firmware are encoded by certain vendors, however the authors were able to repackage the firmware file and launch two attacks causing physical damage and voltage instability to he device.

SEOULTECH

Taxonomy of IoT Vulnerabilities

Layers

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

SEOULTECH

Taxonomy of IoT Vulnerabilities

Security Impact: Confidentiality

- To ensure data confidentiality, unauthorized access is enforced by strict access control, encryption and strong authentication procedures.
- Copos et al. [24] illustrated how network traffic analysis of IoT thermostats and smoke detectors could be used to learn sensitive information.
- The authors assessed that although traffic is encrypted, the devices still reveal destination IP addresses and communication packet sizes.
- Ronen and Shamir [25] analyzed the leakage of sensitive information such as WiFi passwords and encryption primitives by simulating attacks on smart IoT light bulbs.
- When devices are installed, passwords are transmitted unencrypted allowing them to be used for malicious reasons.
- Wang et al. [26] revealed by learning a user's motion signals and unique movement patterns, an attacker can learn a PIN based access system such as an ATM.

SEOULTECH

Taxonomy of IoT Vulnerabilities

Security Impact: Integrity

- The security objective of safeguarding integrity is to prevent any unauthorized modification. It is enforced by access control, encryption and using IDS.
- Ho et al. [27] investigated a number of integrity attacks by studying smart IoT lock systems.
- The authors demonstrate network architectures and trust models which allow an attacker to achieve authorized physical access to a building.
- Gena et al. [28] performed security evaluation of wireless traffic signals using attack simulations which revealed a lack of encryption and usage of default credentials.
- The authors note that implementation of encryption on the wireless network, modifying default credentials, blocking unnecessary network traffic, and regularly updating device firmware will ensure device security.
- Takeoglu and Tosun's [29] research demonstrated that auditing device security and reducing administrator access helps to reduce integrity issues in IoT security.

SEOULTECH

Taxonomy of IoT Vulnerabilities

Security Impact: Availability

- The security objective of safeguarding availability is to guarantee timely access to data, applications and network infrastructure.
- Availability is enforced by monitoring and adapting the handling capabilities of devices, applying security policies and firmware update patches.
- Costa et al. [30] discussed two groups of availability issues, include hardware and coverage failures.
- Failures include damaged devices, energy depletion and the quality of the information transmitted by the device.
- Schuett et al. [31] demonstrated how firmware modifications could hamper the availability of IoT devices deployed in critical infrastructure.
- The U.S. Department of Homeland Security (DHS) had issued an alert notifying IoT operators of DoS attacks, which target devices with default credentials and open Telnet ports.

SEOULTECH

Taxonomy of IoT Vulnerabilities

Security Impact: Accountability

- The accountability objective typically guarantees the feasibility of tracing actions and events to the respective user or systems aiming to establish responsibility for actions.
- Issues such as open access control, lack of security auditing measures, and non-enforcement of integrity rules.

Layers	Vulnerabilities	Security Impact				References
		Confidentiality	Integrity	Availability	Accountability	
Device-based	Deficient physical security	○	●	●	○	[50]–[52], [57]
	Insufficient energy harvesting	○	○	●	○	[56], [57], [94]
Network-based	Inadequate authentication	●	●	○	○	[60], [61], [86], [88]–[90], [95]
	Improper encryption	●	●	○	○	[66], [96]–[98]
	Unnecessary open ports	●	○	●	○	[67], [91], [100]
Software-based	Insufficient access control	●	●	●	○	[51], [72], [74], [83], [92], [93], [98]–[100]
	Improper patch management capabilities	○	○	●	○	[52], [81], [83]
	Weak programming practices (e.g. root user, lack of SSL, plain text password, backdoor, ect.)	●	●	○	○	[83]
	Insufficient audit mechanism	○	●	○	●	[51], [86]

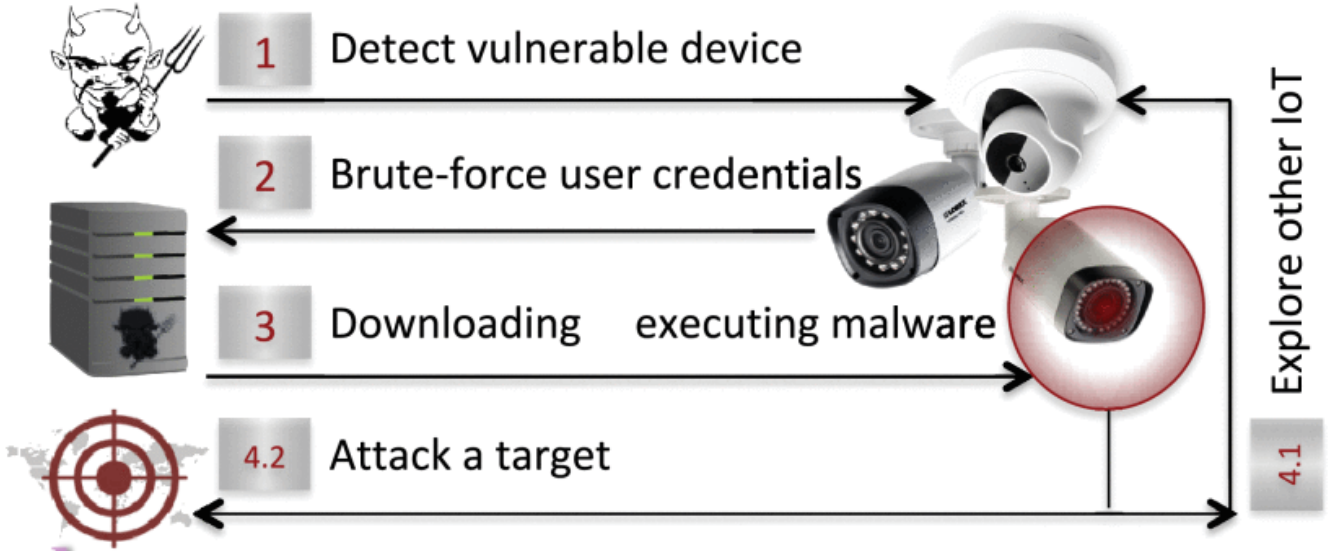
Legend: ● vulnerability has significant impact on particular security concept,
○ vulnerability does not have significant impact on a particular security concept

SEOULTECH

Taxonomy of IoT Vulnerabilities

Attacks: Attacks Against Confidentiality and Authentication

- The primary goal of this class of attack is to gain unauthorized access to IoT resources and data to conduct further malicious actions.
- Dictionary attacks aim at gaining access to IoT devices through executing variants of brute force events.
- Attackers aim to modify device settings or take full control of the device.
- Kolias et al. [32] discussed there are always a number of online and unsecure devices which can be used to launch large scale attacks.



SEOULTECH

Taxonomy of IoT Vulnerabilities

Attacks: Attacks Against Confidentiality and Authentication

- Antonakakis et al. [33] analyzed over 1,000 malware variants to document the evolution of the Mirai malware.
- The authors identified 1.2 million Mirai infected IP addresses associated with various deployment environments and types of IoT devices.
- Mirai-like botnets are now used for crypto-currency mining attacks.
- Using Sybil attacks, an attacker can manipulate the identity of compromised devices aiming to maliciously influence the network.
- Rajan et al. [34] labelled Sybil attacks in two types, stolen and fabricated identities.
- The authors inspected network performance when malicious nodes drop packets or selectively forward them to the server.
- A behavioral profile was proposed to detect sybil nodes. A trust matrix is used to calculate trust.
- Traffic is rerouted from nodes with low trust score to nodes with high trust score.

SEOULTECH

Opinions

- The paper addresses many issues for IoT security, however the lack of secure device credentials is still a concern.
- There is a lack of an immediate response to prevent growth of malware activity in devices once malicious behavior is detected.
- Shodan.io is used to scan for open ports in machines which exposes device vulnerabilities to attackers.
- Defense mechanisms are needed to monitor and restrict access to open ports. Each process running on the device must have access control in place to prevent unauthorized scripts from communicating with the attacker.
- Device manufacturers do not update firmware with known vulnerabilities. There needs to be a defense framework which resets the device operating system to break communication between device and attacker.

SEOULTECH

References

1. L. Atzori, A. Iera, G. Morabito, "The Internet of Things: A survey", Comput. Netw., vol. 54, no. 15, pp. 2787-2805, 2010.
2. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, "Internet of Things (IoT): A vision architectural elements and future directions", Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645-1660, 2013.
3. L. Da Xu, W. He, S. Li, "Internet of Things in industries: A survey", IEEE Trans. Ind. Informat., vol. 10, no. 4, pp. 2233-2243, Nov. 2014.
4. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, "Internet of Things: A survey on enabling technologies protocols and applications", IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347-2376, 4th Quart. 2015.
5. L. Atzori, A. Iera, G. Morabito, "Understanding the Internet of Things: Definition potentials and societal role of a fast evolving paradigm", Ad Hoc Netw., vol. 56, pp. 122-140, Mar. 2016.
6. C. Perera, A. Zaslavsky, P. Christen, D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey", IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 414-454, 1st Quart. 2014.
7. S. Sicari, A. Rizzardi, L. A. Grieco, A. Coen-Porisini, "Security privacy and trust in Internet of Things: The road ahead", Comput. Netw., vol. 76, pp. 146-164, Jan. 2015.
8. A. Mosenia, N. K. Jha, "A comprehensive study of security of Internet-of-Things", IEEE Trans. Emerg. Topics Comput., vol. 5, no. 4, pp. 586-602, Oct./Dec. 2017.
9. A. Ouaddah, H. Mousannif, A. A. Elkalam, A. A. Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities", Comput. Netw., vol. 112, pp. 237-262, Jan. 2017.
10. R. Roman, J. Zhou, J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things", Comput. Netw., vol. 57, no. 10, pp. 2266-2279, 2013.

SEOULTECH

References

11. A. A. Gendreau, M. Moorman, "Survey of intrusion detection systems towards an end to end secure Internet of Things", Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud), pp. 84-90, 2016.
12. J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, Y. Jin, "Security analysis on consumer and industrial IoT devices", Proc. 21st Asia South Pac. Design Autom. Conf. (ASP-DAC), pp. 519-524, 2016.
13. W. Trappe, R. Howard, R. S. Moore, "Low-energy security: Limits and opportunities in the Internet of Things", IEEE Security Privacy, vol. 13, no. 1, pp. 14-21, Jan./Feb. 2015.
14. N. Vidgren, K. Haataja, J. L. Patino-Andres, J. J. Ramirez-Sanchis, P. Toivanen, "Security threats in ZigBee-enabled systems: Vulnerability evaluation practical experiments countermeasures and lessons learned", Proc. 46th Hawaii Int. Conf. Syst. Sci. (HICSS), pp. 5132-5138, 2013.
15. L. Atzori, A. Iera, G. Morabito, "Understanding the Internet of Things: Definition potentials and societal role of a fast evolving paradigm", Ad Hoc Netw., vol. 56, pp. 122-140, Mar. 2016.
16. N. E. Petroulakis, E. Z. Tragos, A. G. Fragkiadakis, G. Spanoudakis, "A lightweight framework for secure life-logging in smart environments", Inf. Security Tech. Rep., vol. 17, no. 3, pp. 58-70, 2013.
17. J. Czyz, M. J. Luckie, M. Allman, M. Bailey, "Don’t forget to lock the back door! A characterization of IPv6 network security policy", Proc. NDSS, 2016.
18. K. Angrishi, "Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT botnets" in arXiv preprint arXiv:1702.03681, 2017.
19. L. Markowsky, G. Markowsky, "Scanning for vulnerable devices in the Internet of Things", Proc. IEEE 8th Int. Conf. Intell. Data Acquisition Adv. Comput. Syst. Technol. Appl. (IDAACS), vol. 1, pp. 463-467, 2015.
20. M. Patton et al., "Uninvited connections: A study of vulnerable devices on the Internet of Things (IoT)", Proc. IEEE Joint Intell. Security Informat. Conf. (JISIC), pp. 232-235, 2014.

SEOULTECH

References

21. A. Cui, S. J. Stolfo, "A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan", Proc. 26th Annu. Comput. Security Appl. Conf., pp. 97-106, 2010.
22. A. Costin, J. Zaddach, A. Francillon, D. Balzarotti, S. Antipolis, "A large-scale analysis of the security of embedded firmwares", Proc. USENIX Security, pp. 95-110, 2014.
23. C. Konstantinou, M. Maniatakos, "Impact of firmware modification attacks on power systems field devices", Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), pp. 283-288, Nov. 2015.
24. B. Copos, K. Levitt, M. Bishop, J. Rowe, "Is anybody home? Inferring activity from smart home network traffic", Proc. IEEE Security Privacy Workshops (SPW), pp. 245-251, 2016.
25. E. Ronen, A. Shamir, "Extended functionality attacks on IoT devices: The case of smart lights", Proc. IEEE Eur. Symp. Security Privacy (EuroS&P), pp. 3-12, 2016.
26. H. Wang, T. T.-T. Lai, R. R. Choudhury, "Mole: Motion leaks through smartwatch sensors", Proc. 21st Annu. Int. Conf. Mobile Comput. Netw., pp. 155-166, 2015.
27. G. Ho et al., "Smart locks: Lessons for securing commodity Internet of Things devices", Proc. 11th ACM Asia Conf. Comput. Commun. Security, pp. 461-472, 2016.
28. B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, J. A. Halderman, "Green lights forever: Analyzing the security of traffic infrastructure", Proc. WOOT, vol. 14, pp. 7, 2014.
29. A. Tekeoglu, A. S. Tosun, "Investigating security and privacy of a cloud-based wireless IP camera: Netcam", Proc. 24th Int. Conf. Comput. Commun. Netw. (ICCCN), pp. 1-6, 2015.
30. D. G. Costa, I. Silva, L. A. Guedes, F. Vasques, P. Portugal, "Availability issues in wireless visual sensor networks", Sensors, vol. 14, no. 2, pp. 2795-2821, 2014.

SEOULTECH

References

31. C. Schuett, J. Butts, S. Dunlap, "An evaluation of modification attacks on programmable logic controllers", Int. J. Crit. Infrastruct. Protect., vol. 7, no. 1, pp. 61-68, 2014.
32. C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, "DDoS in the IoT: Mirai and other botnets", Computer, vol. 50, no. 7, pp. 80-84, 2017.
33. M. Antonakakis et al., "Understanding the Mirai botnet", Proc. 26th USENIX Security Symp. (USENIX Security), pp. 1093-1110, 2017.
34. A. Rajan, J. Jithish, S. Sankaran, "Sybil attack in IoT: Modelling and defenses", Proc. Int. Conf. Adv. Comput. Commun. Informat. (ICACCI), pp. 2323-2327, Sep. 2017.

SEOULTECH

Thank you!

SeoulTech UCS Lab
Ubiquitous Computing & Security Laboratory

Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations - Part 2 -

Jinseong Park, Mikail Mohammed Salim

Department of Computer Science & Engineering

Seoul National University of Science & Technology

CIS (Cryptography and Information Security) Lab

2019-10-01

Table of Contents

IV. TAXONOMY OF IOT VULNERABILITIES

❖ Attacks

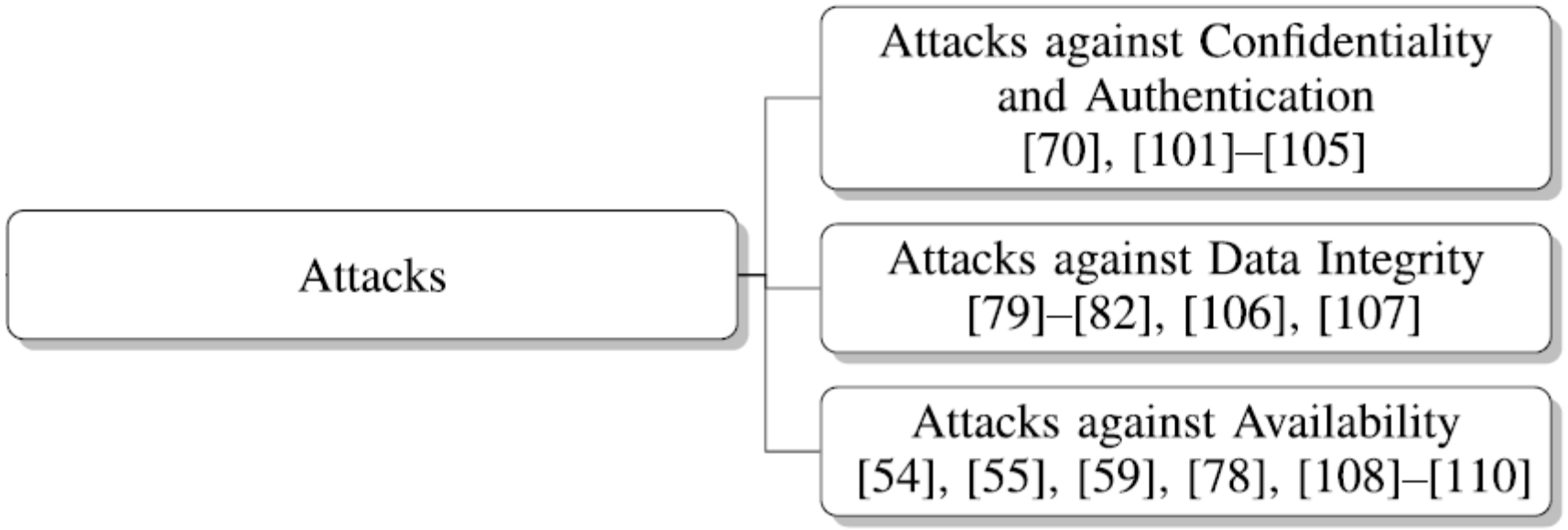
TABLE VI
ATTACKS TARGETING IOT PARADIGM

	Dictionary Attack	Side-Channel Attack	Sybil Attack	False Data Injection	Firmaware Modification Attack	Device Capture	Sinkhole Attack	Battery Draining Attack	Jumming Attack	References
Deficient physical security	○	●	○	○	●	●	○	○	○	[54], [55], [70], [79]–[82], [104], [108]
Insufficient energy harvesting	○	○	○	○	○	○	●	●	●	[59], [109], [110]
Insufficient authentication	●	○	●	●	○	●	●	○	○	[54], [55], [101]–[103], [105]–[109]
Improper encryption	○	●	○	○	○	○	○	○	○	[70], [104]
Unnecessary open ports	●	○	○	○	○	○	○	○	○	[78]
Insufficient access control	●	○	○	○	○	○	○	○	○	[78], [102]
Improper software update capabilities	○	○	○	○	●	○	○	○	○	[79]–[82]
Weak programming practice (e.g. root user, lack of SSL, plain text password, back-door, ect.)	●	○	○	●	●	○	○	○	○	[79]–[82], [102], [106], [107]
Insufficient audit mechanism	●	○	○	●	●	●	○	○	○	[54], [55], [79]–[82], [102], [106]–[108]

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

IV. TAXONOMY OF IOT VULNERABILITIES

❖ Attacks



IV. TAXONOMY OF IOT VULNERABILITIES

- ❖ Attacks
  - ➢ Attacks Against Data Integrity
    - ✓ False Data Injection (FDI) attacks
      - fuse legitimate or corrupted input towards IoT sensors
      - Liu et al. [106] simulated data injection attacks on power utilities.
        - only need to compromise 1% of the IoT meters in the system to severely threaten the resiliency of the entire power grid
      - Liu et al. [107] proposed and validated numerous strategies which allows the proper execution of FDI attacks
        - built a linear programming model that minimized the number of required network characteristics measurements
    - ✓ Firmware modification

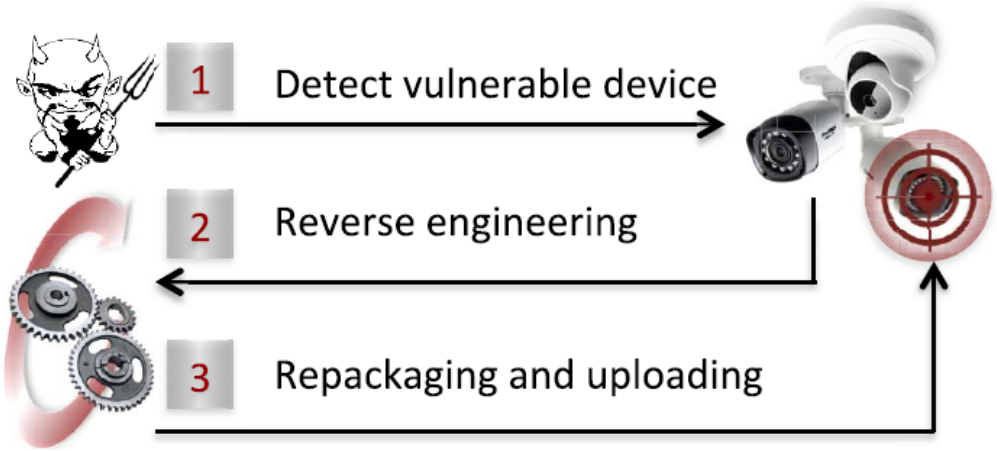


Fig. 5. Stages of firmware modification attack.

IV. TAXONOMY OF IOT VULNERABILITIES

- ❖ Attacks
  - ➢ Attacks Against Data Integrity
    - ✓ Firmware modification
      - Basnight et al. [79] illustrated how firmware could be maliciously modified and uploaded to PLC.
        - By conducting reverse engineering
        - resource limitation of PLC devices hinders the implementation of a robust algorithm that would attempt to verify data integrity
      - Cui et al. [80] analyzed a large number of printer firmware and executed firmware modification attacks by reverse engineering a number of hardware components.
        - rely on third-party libraries that contain known vulnerabilities
        - update mechanisms typically do not require authentication
        - lack of IoT host-based defense/integrity mechanisms
      - Konstantinou and Maniatakos [81] defined firmware modifications as a new class of cyber-physical attacks against the IoT paradigm
        - using simplistic checksum which can be easily circumvented
        - maliciously modified IoT firmware could indeed cause a cascade of power outages within the context of the smart grid.
      - Bencsáth et al. [82] introduced a general framework for Cross-Channel Scripting (CCS) attacks targeting IoT embedded software.

IV. TAXONOMY OF IOT VULNERABILITIES

- Attacks
  - Attacks Against Availability
    - ✓ The goal of this attacks is to prevent the legitimate users' timely access to IoT resources.

    - ✓ Device capture
      - capture, alter or destroy a device to retrieve stored sensitive information
      - IoT devices typically reside in unattended and physically unprotected realms.
      - Smache et al. [54] formalized a model for node capturing attacks, given a secure IoT WSN.

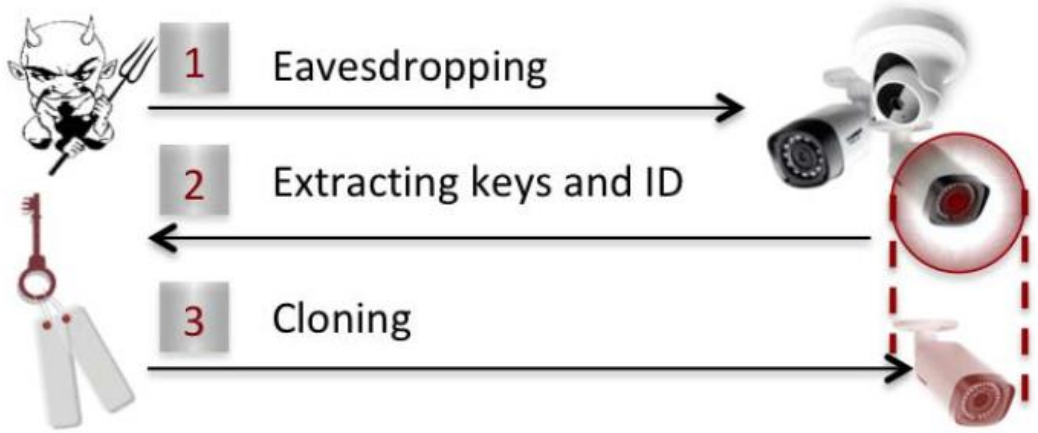


Fig. 6. Node capturing attack phases.

IV. TAXONOMY OF IOT VULNERABILITIES

- ❖ Attacks
  - ➢ Attacks Against Availability
    - ✓ Device capture
      - Zhao [55] analyzed the resiliency to node-capture attacks of random key predistribution IoT schemes, and provided several design guidelines for secure sensor networks by employing such scheme.
      - Bonaci et al. [108] proposed an adversary model of node capture attacks.
        - Proposed an algorithm for identifying corrupted nodes
        - Proposed node revocation methods
        - Proposed key refreshment techniques for node validation
      - Radware [78] recently witnessed and alarmed about nearly 2,000 attempts to compromise IoT honeypots.
    - ✓ Sinkhole Attacks
      - advertise artificial routing paths to include as many nodes as possible in order to obligee them to send packets

IV. TAXONOMY OF IOT VULNERABILITIES

- ❖ Attacks
  - ➢ Attacks Against Availability
    - ✓ Battery draining attacks (= vampire attacks)
      - demands significantly more energy from the network and its nodes to be employed and acted upon in contrast with typical messages.
      - Carousel attack
        - series of loops such that the same node appears in the route several times
      - Stretch attacks
        - construct long routes so that the packets traverse through a larger, inversely optimal number of IoT nodes
    - ✓ Jamming attacks (Pielli et al. [110])
      - disrupting IoT network communications and reducing the lifetime of energy-constrained nodes by creating interference and causing packet collisions
      - trade-off between communication reliability and device lifetime

IV. TAXONOMY OF IOT VULNERABILITIES

❖ Countermeasure

TABLE VII
SUMMARY OF REMEDIATION STRATEGIES

Vulnerability	Remediation Strategy			References
	Access and Authentication Controls	Software Assurance	Security Protocols	
Deficient physical security	●	○	○	[53], [87], [123]
Insufficient energy harvesting	●	○	●	[111], [123]–[126]
Inadequate authentication	●	○	○	[62]–[64], [87], [112]–[115], [180]–[183]
Improper encryption	○	○	●	[68], [69], [128]
Unnecessary open ports	○	○	○	[-]
Insufficient access control	●	●	●	[75], [76], [116]–[119], [129]
Improper patch management capabilities	○	○	○	[-]
Weak programming practices (e.g. root user, lack of SSL, plain text password, backdoor, ect.)	○	●	○	[84], [85], [120]–[122]
Insufficient audit mechanism	●	○	○	[87]

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

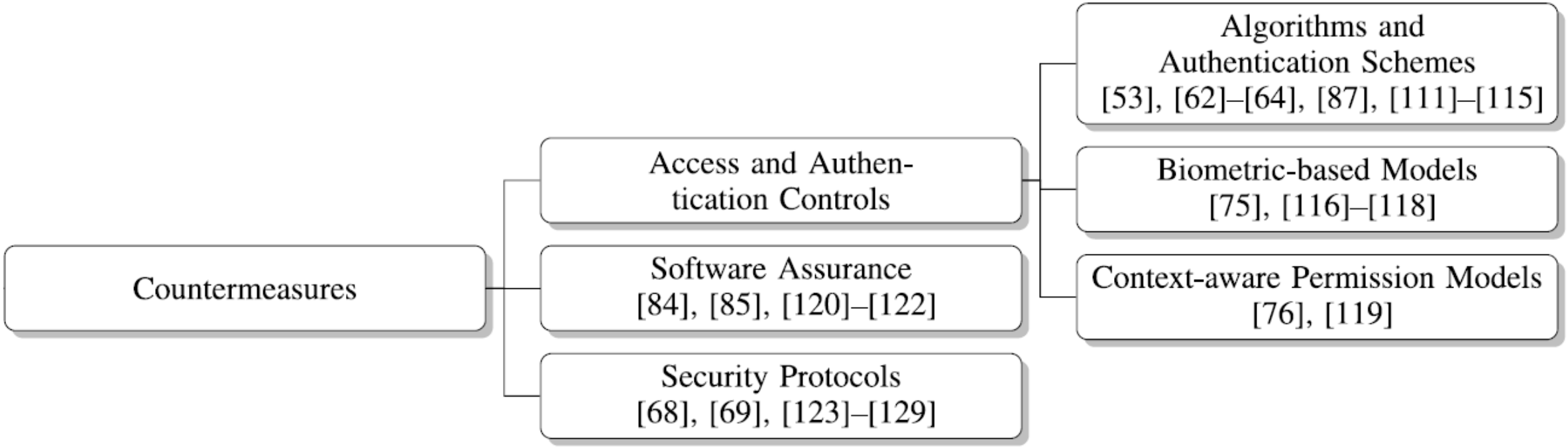
TABLE VIII
SUMMARY OF REMEDIATION STRATEGIES FOR EACH ATTACK

Attack	Remediation Strategy			References
	Access and Authentication Controls	Software Assurance	Security Protocols	
Dictionary attack	●	○	○	[75], [76], [87], [116]–[119]
Side-Channel attack	○	○	○	
Sybil attack	○	○	●	[62], [64], [115]
False Data Injection	○	●	○	[68], [69], [120], [128]
Firmaware modification attack	○	●	○	[84], [85], [122]
Device capture	●	○	●	[53], [63], [87], [123]
Sinkhole Attack	●	○	○	
Battery draining attack	●	○	●	[111], [112], [123], [124]
Selective-forwarding	○	○	○	

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

IV. TAXONOMY OF IOT VULNERABILITIES

❖ Countermeasure



- Countermeasure
  - Access and Authentication Control
    - ✓ Challenge – because of the low computational power of IoT devices
    - ✓ Hafeez et al. [63] proposed Securebox, a platform for securing IoT networks.
      - intercepts any connection request from a connected IoT device to a remote destination and subsequently verifies if various security policies match the requested connection
    - ✓ Qabulio et al. [53] proposed a generic framework for securing mobile wireless IoT networks against physical attacks.
      - techniques by exploiting time differences in inter-arrival rate to detect spoofed packets
    - ✓ Hei et al. [111] proposed a lightweight security scheme to defend against resource depletion attacks.
      - By employing Support Vector Machines (SVM), throttled malicious authentications, thus saving a significant amount of energy
      - the proposed scheme was designed and tested only on one type of IoT device and thus might not be generic enough to be employed for various IoT types.
    - ✓ Yang et al. [87] proposed an RFID-based solution
      - By binding the RFID tags with the control chip of the IoT devices, the authors aimed to prevent stolen, replaced by malicious ones or modified.

- Countermeasure
  - Access and Authentication Control
    - ✓ Jan et al. [112] proposed a lightweight authentication algorithm for verifying IoT devices' identities before running them in an operational network, by adopting the Constrained Application Protocol (CoAP).
      - using a single key for authentication purposes reduces connection overheads and computational load.
      - does not defend the IoT network if the malicious node actively spoofs multiple identities.
    - ✓ Kothmayr et al. [62] introduced a twoway authentication scheme for the IoT paradigm based on the Datagram Transport Layer Security (DTLS) protocol.
    - ✓ Sciancalepore et al. [113] presented a Key Management Service (KMS) protocol that employs certificates, by applying the Elliptic Curve Qu-Vanstone (ECQV) algorithm.
    - ✓ Porambage et al. [64] introduced a lightweight authentication mechanism, namely PAuthKey, for WSNs in distributed IoT applications, which aimed at ensuring end-to-end security and reliable data transmission.
    - ✓ Park [114] adopted ECQV certificates and employed the concept of Cryptographically Generated Address (CGA).
      - proposed scheme required less energy and execution time
    - ✓ Garcia-Morchon et al. [115] proposed two security architectures by adapting the DTLS [175] and the HIP [179] protocols for IoT devices with Pre-Shared Keys (PSK).
      - DTLS induces a larger memory footprint while HIP added significant overhead in the context of key management.

- Countermeasure
  - Access and Authentication Control
    - ✓ Rostami et al. [116] introduced an access-control policy, namely Heart-to-heart, for IMD.
      - lightweight authentication protocol which exploits Electrocardiography (ECG) randomness to defend against active attacks
    - ✓ Hossain et al. [117] presented an infrastructure for an end-to-end secure solution based on biometric characteristics.
      - The sensors collect biometric features and transmit them through encrypted communication channels to a cloud, where they are processed by the application layer.
    - ✓ Guo et al. [118] proposed an access control approach which includes biometric-based key generation.
      - employ an additional chip that acts as a permutation block, in order to permit secure communications between programmable and nonprogrammable components
    - ✓ Dhillon and Kalra [75] proposed a lightweight multi-factor authentication protocol to elevate the security of the IoT.
      - Security is enforced by utilizing one-way hash, perceptual hash functions, and XOR operations that are computationally less expensive and, thus, suitable in IoT environments.

- Countermeasure
  - Access and Authentication Control
    - ✓ Jia et al. [76] aimed to design a context-based permission system that captures environmental IoT contexts, analyze previous security-relevant details, and take further mitigative action.
    - ✓ Fernandes et al. [119] introduced a method of restricting access to sensitive IoT data.
      - system dubbed as FlowFence, which allows controlling the way data is used by the application.
      - empowers developers with the ability to split their application into two modules
        - the first module operates sensitive IoT information in a sandbox
        - second component coordinates the transmission of such sensitive data by employing integrity constraints.

- Countermeasure
  - Software Assurance
    - ✓ Aims at reducing the vulnerabilities of both source and binary code to provide resiliency to the IoT paradigm.
    - ✓ Costin et al. [120] proposed a scalable, automated framework for dynamic analysis aiming to discover vulnerabilities within embedded IoT firmware images.
    - ✓ Li et al. [121] proposed to extend traditional code verification techniques by fusing safety-related properties of specific medical device to code model checker such as CBMC.
    - ✓ Zaddach et al. [122] presented a framework dubbed as Avatar for dynamic analysis of embedded IoT systems by utilizing an emulator and a real IoT device.
    - ✓ Feng et al. [84] demonstrated how learning of high-level features of a control flow graph could improve the performance of firmware vulnerability search methods.
    - ✓ Elmiligi et al. [85] introduced a multidimensional method to analyze embedded systems security at different levels of abstraction.
      - mapping the attacks to three dimensions, namely, programming level, integration level, and a life cycle phase

- Countermeasure
  - Security Protocols
    - ✓ Balasubramanian et al. [125] designed an Energy-Aware-Edge-Aware (2EA) architecture in which an IoT sensor can rely on energy harvesting.
    - ✓ Kamalinejad et al. [126] pinpointed that IoT self-sustainability is an open research question and requires the design of improved techniques at both the circuit and system levels.
    - ✓ Zhang et al. [123] proposed the Coverage Interface Protocol (CIP) with the aim to design an energy efficient and compromisetolerant scheme.
      - Boundary Node Detection scheme (BOND) equips IoT nodes with the ability to recognize their boundary nodes.
      - Location-Based Symmetric Key management protocol (LBSK) establishes related keys to secure core network operations.
    - ✓ Rao and M [124] proposed the predictive node expiration-based, energy-aware source routing protocol, which attempts to optimize the overall energy efficiency of the IoT sensor network.
    - ✓ Glissa and Meddeb [127] considered various potential attacks on 6LoWPAN and proposed a multi-layered security protocol, namely, the Combined 6LoWPSec.

- Countermeasure
  - Security Protocols
    - ✓ Shafagh et al. [68] approached IoT security by designing a data protection framework, dubbed as Talos, where the cloud curates encrypted data while permitting the execution of specific queries.
      - Partial Homomorphic Encryption (PHE) solution for IoT
    - ✓ Wei et al. [69] recently offered a scalable, one-time file encryption protocol, which combined robust cryptographic techniques to protect files from arbitrary users.
      - adopting techniques and technologies rooted in identitybased encryption
    - ✓ Yang et al. [129] proposed a lightweight access protocol for IoT in healthcare.
      - In this context, access to IoT data should be granted in two different situations under usual and emergency modes/situations.

IV. TAXONOMY OF IOT VULNERABILITIES

❖ Situational Awareness Capabilities

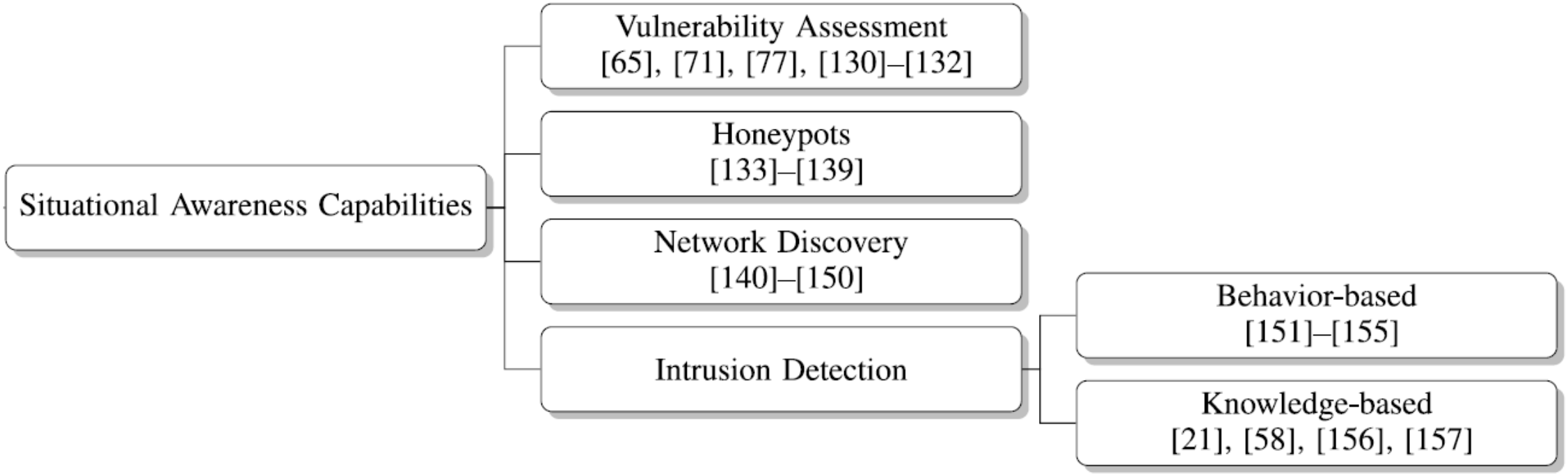
TABLE IX
IOT SECURITY SITUATIONAL AWARENESS CAPABILITIES

Vulnerability	Situational Awareness Capabilities				References
	Vulnerability Assessment	Honeypots	Network Discovery	Intrusion Detection	
Deficient physical security	●	○	○	●	[130], [155]
Insufficient energy harvesting	○	○	○	●	[58], [151], [152], [156]
Inadequate authentication	●	○	●	●	[65], [71], [145], [149], [151], [153], [155], [157]
Improper encryption	●	○	○	○	[71], [131], [132]
Unnecessary open ports	●	●	○	○	[71], [77], [133]–[137]
Insufficient access control	●	●	●	○	[71], [77], [133]–[144]
Improper patch management capabilities	●	○	○	○	[77]
Weak programming practices (e.g. root user, lack of SSL, plain text password, backdoor, etc.)	●	○	○	●	[65], [71], [77], [151], [153], [157]
Insufficient audit mechanism	○	○	○	●	[151], [153], [157]
IoT device identification	○	○	●	●	[21], [58], [142], [146]–[148], [151]–[157]

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

IV. TAXONOMY OF IOT VULNERABILITIES

❖ Situational Awareness Capabilities



- Situational Awareness Capabilities
  - Vulnerability Assessment
    - ✓ One of such testbeds was proposed by Tekeoglu and Tosun [77].
      - enables the capturing of network traffic for analyzing its features to identify IoT security vulnerabilities
        - most of the investigated IoT devices do not lock-out users after failed login attempts
        - several unnecessary open ports facilitate targeted attacks
        - a large number of devices are operated with outdated versions of their software and firmware
    - ✓ Siboni et al. [71] designed a unique testbed for wearable devices.
    - ✓ Reaves and Morris [130] designed two testbeds for IoT within Industrial Control Systems (ICS) to compare different implementation types and to infer the most efficient way to identify vulnerabilities.
    - ✓ Furfaroa et al. [65] offered a scalable platform, known as SmallWorld, which enables security professionals to design various scenarios to assess vulnerabilities related to IoT devices.
      - physical, abstraction, core service, API, and management layers
    - ✓ Fuzzy-based approaches
      - Lahmadi et al. [131] designed a testing framework that enables developers to assess the security of the 6LoWPAN protocol.
      - Cui et al. [132] applied a fuzzy technique to ZigBee networks to locate and analyze vulnerabilities within IoT networks.

IV. TAXONOMY OF IOT VULNERABILITIES

- Situational Awareness Capabilities
  - Honeypots
    - ✓ For capturing malicious activities for further investigation of attack vectors or to generate attack patters, which could be used for future mitigation
    - ✓ Pa et al. [133] offered a trap-based monitoring system dubbed as IoTPOT.
      - Telnet services of various IoT devices to analyze ongoing attacks in depth
    - ✓ Guarnizo et al. [134] presented the Scalable high-Interaction Honeypot platform (SIPHON) for IoT devices.
      - provided insights regarding such traffic, including the popularity of target locations, scanned ports, and user agents
    - ✓ Vasilomanolakis et al. [135] proposed HosTaGe, a honeypot that aims to detect malicious activities targeting ICS networks.
      - identification of attacks in various protocols as HTTP, SMB, Telnet, FTP, MySQL, SIP, and SSH.

- Situational Awareness Capabilities
  - Honeypots
    - ✓ Buza et al. [136] designed the Crysys honeypot.
      - To detect targeted attacks against ICS which rely on Programmable Logic Controllers (PLC)
    - ✓ Litchfield et al. [137] proposed a CPS framework supporting a hybrid-interaction honeypot architecture.
      - Aims to provide the ability to simulate the behavior of both CPS processes and IoT devices.
    - ✓ Dowling et al. [138] designed a honeypot which simulates a ZigBee gateway to explore attacks against ZigBee-based IoT devices.
    - ✓ Gandhi et al. [139] proposed another IoT honeypot, namely HIoTPOT, to analyze the threats against the IoT paradigm.
      - To find vulnerable IoT devices.

IV. TAXONOMY OF IOT VULNERABILITIES

- Situational Awareness Capabilities
  - Network Discovery
    - ✓ for the large-scale deployment of vulnerable IoT devices
    - ✓ Approach to CPS Network
      - Bou-Harb et al. [140] proposed an approach for resilient CPS.
      - Fachkha et al. [141] recently analyzed attackers' intentions when targeting protocols of Internet-facing CPS.
      - Galluscio et al. [142] illustrated the widespread insecurity of IoT devices by proposing a unique approach to identify unsolicited IoT nodes.
    - ✓ Nguyen et al. [148] proposed a system for the detection of compromised IoT devices without labeling training data.
    - ✓ Search engine
      - Shodan [143] crawles the Internet 24/7 and updates its repository in real-time to provide a recent list of IoT devices.
      - Censys [144] collects data (including IoT information) through executing horizontal scans of the public IPv4 address space and provides public access to raw data through a Web service.

IV. TAXONOMY OF IOT VULNERABILITIES

- Situational Awareness Capabilities
  - Network Discovery
    - ✓ Meidan et al. [145] leveraged network traffic analysis to classify IoT devices connected to an organization's network.
      - promise to enable reliable identification of IoT connections in an enterprise setting
    - ✓ Formby et al. [149] designed two approaches for device fingerprinting.
      - leverages the crosslayer response time
      - utilizes the unique physical properties of IoT devices
    - ✓ Shahid et al. [146], aiming at predicting the IoT device type by observing network traffic, trained six different machine learning classifiers.
    - ✓ Thangavelu et al. [147] presented a distributed fingerprinting mechanism which explores the presence of IoT devices with high accuracy and low level of false positive misclassification rate.

- Situational Awareness Capabilities
  - Intrusion Detection
    - ✓ Given the limited resources of IoT devices, most deployed intrusion detection techniques are network-based with an active response system, which operates by halting communications of the compromised nodes.

    - ✓ Behavior-based IDS
      - Raza et al. [151] pioneered an IDS, known as SVELTE, for IoT contexts.
      - Shreenivas et al. [152] extended SVELTE with two additional modules.
        - module that uses Expected Transmissions (ETX) metrics
        - attempts to locate malicious nodes inside the 6LoWPAN network
      - Yang et al. [153] proposed a scheme that enables the detection of FDI attacks in IoT-based environmental surveliance at an early stage.
      - Thanigaivelan et al. [154] leveraged collaboration between 1-hop neighbor nodes to design a distributed anomaly detection system for the IoT paradigm.
      - Parno et al. [155] proposed two distributed schemes, namely, randomized and line-selected multicast, for detecting nodes' replications.

    - ✓ knowledge-based IDS
      - Bostani and Sheikhan [156] proposed a novel real-time intrusion detection framework for detecting sinkhole and selective-forwarding attacks.
      - Midi et al. [157] proposed a selfadaptive knowledge-driven IDS, namely Kalis, that is capable of detecting attacks against IoT environments across a wide range of protocols.

IV. TAXONOMY OF IOT VULNERABILITIES

- Situational Awareness Capabilities
  - Intrusion Detection

TABLE X
INTRUSION DETECTION TECHNIQUES DEPLOYED IN IOT ENVIRONMENTS

Attack	Behavior-based					Knowledge-based		
	[151]	[152]	[153]	[154]	[155]	[156]	[58]	[157]
Dictionary attack	○	○	○	○	○	○	○	○
Side-Channel attack	○	○	○	○	○	○	○	○
Sybil attack	●	○	○	○	○	○	○	○
False Data Injection	●	○	●	○	○	○	○	●
Firmaware modification attack	○	○	○	○	○	○	○	○
Device capture	○	○	○	○	●	○	○	○
Sinkhole Attack	●	○	○	○	○	●	○	○
Battery draining attack	○	●	○	○	○	○	●	○
Selective-forwarding	●	●	○	○	○	●	○	●
Anomaly detection	○	○	○	●	○	○	○	○

Legend: ● a technique detects an attack, ○ a technique does not detect an attack

V. EMPIRICAL EVALUATION OF IOT MALICIOUSNESS

❖ Analysis darknet data & Using Shodan

Fig. 7. Global distribution of exploited IoT devices.

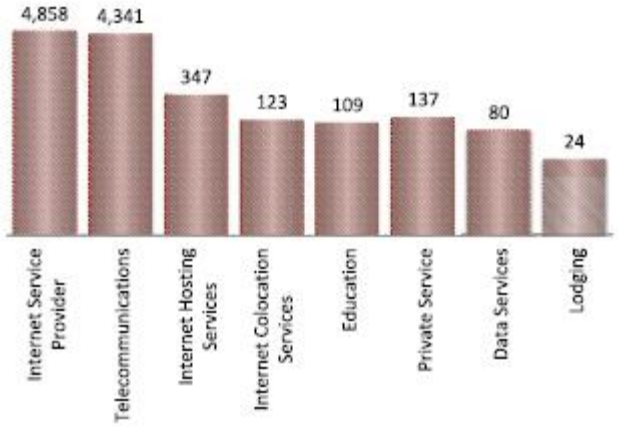


Fig. 8. Top sectors hosting exploited IoT devices.

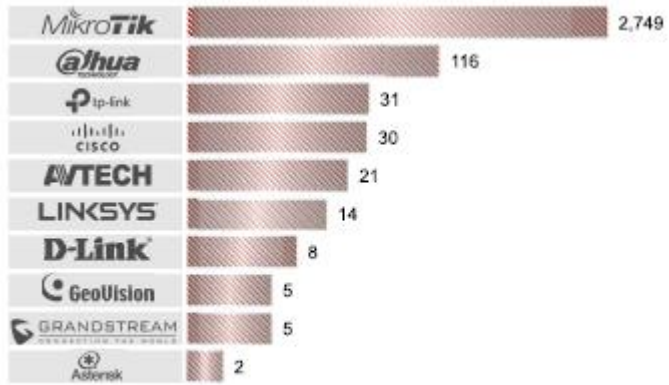


Fig. 9. Top ten manufacturers of exploited IoT devices.

VI. IOT VULNERABILITIES

- Challenge 1. Lack of Large-Scale Identification Techniques of Exploited IoT Devices
  - There is a paramount need for collaborative knowledge and information exchange regarding the notion of maliciousness from various sources (including ISPs, IoT operations, researchers, etc.)

- Challenge 2. Inadequacy of Scalable Vulnerability Assessment Solutions
  - Applying transfer learning algorithms [215] to the currently available knowledge related to IoT vulnerabilities could ameliorate and automate the tasks of vulnerability assessment and simulation in order to extrapolate this knowledge to various IoT devices, platforms and realms.

- Challenge 3. Limited Security-Related Awareness Capabilities for IoT Users
  - need to explore techniques and methods to increase users' awareness about the consequences of potential IoT threats and possible technical and nontechnical strategies to reduce the risk of exposure
  - Need much attention from the research community.

VI. IOT VULNERABILITIES

- Challenge 4. Immaturity of Security Protocol Standardization and Reactive Frameworks
  - The combination of technological advances with robust regulatory frameworks

- Challenge 5. Lack of Secure Software Development Processes
  - need to execute exploratory studies to inspect the time required from the discovery of IoT vulnerabilities to their disclosure to producing patches and subsequently deploying them at the affected IoT devices.
  - need to enforce stringent IoT programming standards and develop automated code tools to vet IoT applications

VII. CONCLUDING REMARKS

- Need Internet-scale solutions addressing the IoT security
- Research efforts are also required in the context of studying IoT-specific attacks and their malicious signatures.
- suitable schemes, which take into account IoT-specific threats coupled with their unique characteristics, undoubtedly require to be designed

VIII. OPINION

- This paper is recommended for anyone who wants to write a paper on IoT Security.

- The attacks available in the IoT environment and their countermeasures are well organized.

- Although the countermeasure using the latest technology is described,
  there is no description of what each technology is.

- In addition, it is difficult to trust the data in EMPIRICAL EVALUATION OF IOT ALICIOUSNESS.
  - because there is no explanation on how to collect and analyze the data

Thank you for your attention