Computers and Electrical Engineering 100 (2022) 107997

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges[☆]

Renya Nath N [*], Hiran V Nath

Department of Computer Science and Engineering, National Institute of Technology Calicut, Kozhikode, Kerala 673 601, India

ARTICLE INFO

Keywords:
IoT security
Challenges
IoT ecosystem security
Threats and attacks
IoT malware
Security requirements

ABSTRACT

As an emerging technology, the Internet of Things (IoT) is revolutionizing the global economy and society. The wide adoption of IoT opens up new security and privacy challenges as well. Building efficient, secure IoT systems need a thorough understanding of the potential threats and vulnerabilities of the system. The non-uniformity in the presentation of IoT architecture poses a significant challenge in understanding security issues. Motivated by this, we present a systematic study of substantial threats and attacks based on four primary elements of the IoT ecosystem: devices, internal network services, external network services, and users. Besides, we include a detailed study of IoT malware. We examine the major security requirements and challenges to confront the devised attack categories. We believe that an IoT ecosystem can be designed efficiently and securely by adhering to the proposed requirements, including identity management, access control, end to end communication security and trust management systems.

1. Introduction

Internet of Things (IoT) is an emerging communication paradigm that envisions the connectivity of the physical world to the digital world. The decrease in the IoT component cost, improved wireless services, battery life, and improved business models have made IoT vision a reality. Furthermore, empowering technologies such as cloud computing, data analytics, Internet Protocol (IP)-based networking, nanotechnology, ubiquitous computing and other enabling technologies have fueled the rapid advancement in various IoT applications. As a result, Smart city, Smart grid, Smart home, Smart health care, and so on are no longer a futuristic reality.

Cisco's Annual Internet Report (2018–2023) reveals that Internet-connected devices will exceed 30 billion by 2023. Despite the benefits that IoT technology brings to individuals, society and industry, its wide adoption opens up new security and privacy challenges. A vital challenge is protecting devices and resources (data, applications and services) produced within IoT ecosystems. Furthermore, the rapid change from physically isolated systems to Internet-connected, remotely controlled and monitored machines has increased the attack surface. Moreover, the resource-constrained nature of devices in IoT applications makes complex security designs more challenging.

The security requirements of each element in the IoT ecosystem vary according to different applications. As a result, the security solutions also vary accordingly. The survey [1] outlines the various security requirements and challenges of IoT systems such as smart city, smart healthcare, smart transportation and smart grids. As the IoT ecosystem is not merely a single system of computing devices, an in-depth analysis of security threats considering their risk level on each IoT element is needed.

[☆] This paper is for regular issues of CAEE. Reviews were processed by Area Editor Dr. G. Martinez Perez and recommended for publication.

[*] Corresponding author.
E-mail addresses: renya_p190141cs@nitc.ac.in (R. Nath N), hiranvnath@nitc.ac.in (H. V Nath).

https://doi.org/10.1016/j.compeleceng.2022.107997
Received 30 June 2021; Received in revised form 6 April 2022; Accepted 8 April 2022
Available online 6 May 2022

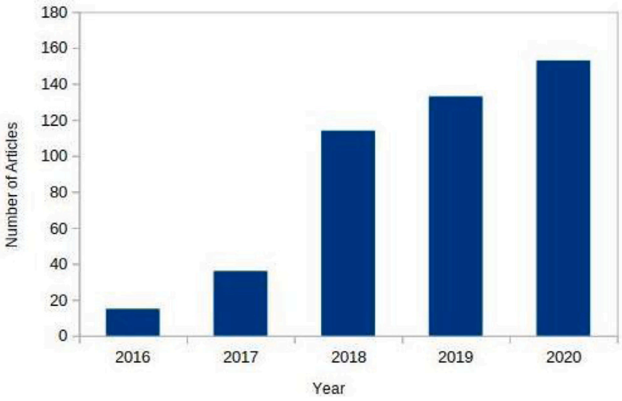

Fig. 1. Summary of articles published in past 5 years.

The non-uniformity in the presentation of IoT architecture and layered protocol stack poses a significant challenge in understanding the underlying security issues. Hence, research biased toward layered IoT architecture alone is insufficient to address the security threats holistically. Therefore in our survey, we explore major IoT security threats and vulnerabilities by systematically analyzing essential elements of an IoT ecosystem. We also examine the proper security requirements to address the devised attack categories.

The contribution of this paper can be summarized as follows: Firstly, we study prominent threats and attacks by systematically analyzing each component in a generalized IoT ecosystem: devices, internal network services, external network services, and users. Secondly, we conduct a comprehensive study on recent IoT malware attacks. Finally, we discuss the general security requirements and challenges to address the devised attack categories.

The rest of the paper is structured as follows: Section 2 reviews the existing surveys on IoT security. Section 3 describes IoT security threats and attacks in detail. Section 4 explains different recent IoT malware families. In Section 5, we discuss essential security requirements and challenges based on the studies we have conducted. Finally, we conclude the paper with Section 6.

2. Motivation and related work

This paper conducts a comprehensive literature survey by exploring relevant articles from four major academic databases(IEEE Xplore, Web of Science, ACM digital library, and ScienceDirect) to understand the cyber-security threats and vulnerabilities on the IoT ecosystem. This study identifies cyber-security countermeasures and highlights the challenges that will help readers get a clear idea of state-of-the-art IoT security. According to these four databases, there are many journal articles and conference papers related to IoT cybersecurity. For this research, we selected 451 articles from IEEE Xplore since 2016 for review purposes. The trend shown in Fig. 1 illustrates that IoT cyber-security is getting significant attention from the research world.

Many papers have been published in the area of IoT security until now. Most of them have focused on different layers of IoT architecture as a base to classify prominent security threats and attacks. Table 1 lists popular IoT architectures' different perspectives, including basic three-layer architecture, derived four-layer architecture, and detailed five-layer architecture.

For instance, most studies in the three-layered architecture have the same architecture as Atzori's [2,3]. This architecture defines the concept of IoT but is not adequate for emerging IoT applications. From a service-oriented view, the four-layered architecture [4–6] includes a middleware layer between the network and application layers. However, [7,8] consider the semantic layer and data-cloud service layer, respectively, as the fourth layer for addressing security issues of data in the cloud. Similarly, none of the studies [9,10] has used common layers to analyze security threats in the five-layered architecture.

The non-uniformity in the layers of IoT architecture makes it challenging to analyze security issues. Very few papers have adopted other systematic approaches to analyze IoT security holistically. In [10] authors cover the security issues from the perspective of users, devices, mobility, communication and integration of resources. Whereas the paper [11] covers the security issues based on three levels: object, network and communication and application. However, the paper focuses on very few threats, namely side-channel attacks and firmware update attacks.

A collaborative analysis combining layered architecture and systematic generalization of the IoT ecosystem can give better insight. Recent IoT malware attacks have raised the attention of the research community. However, none of the IoT security survey papers has given more details. Our paper studies IoT threats and vulnerability, including IoT malware based on a generalized IoT ecosystem, and discusses the existing countermeasures on a derived four-layered IoT architecture.

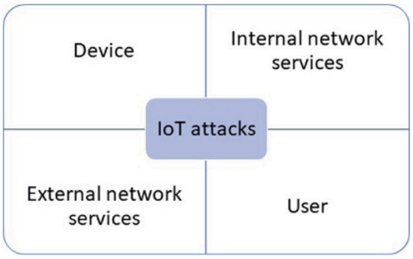

Fig. 2. Devised threats and attacks categories.

Table 1
Summary of different IoT Architecture.

Architecture	Layers
Three Layer	Perception, Network, Application [2,3]
Four Layer	Perception, Network, Application, Semantic [4] Sensing, Network, Middle-ware, Application [5–7] Sensing, Network management, Service, Data center/Virtualization [8]
Five Layer	Sensing, Network, Transport, Application, Data and Cloud Service [9] Sensing, Network, Service composition, Application, User interface [10]

Table 2
Devised IoT attacks and related attack surfaces.

Category	Attack surface	Threats and attacks
Device	Wireless signal strength, Node identity, Unencrypted confidential data in memory	Replay attack, Cyber–physical attack, Side channel attack, Jamming attack, Booting attack, Firmware update attack, Node cloning, Node capture attack, Reverse engineering attack.
Internal network services	Vulnerabilities of routing protocols, Trustworthiness of network/devices, Unencrypted channels	Black hole attack, Gray hole attack, Sinkhole attack, Wormhole attack, Sybil attack, Hello flood attack, Other routing attack, Eavesdropping
External network services	Vulnerability of application protocols, Vulnerabilities of access control systems	DDoS: UDP flood attack, ICMP flood attack, Smurf attack, Fraggle attack, DNS flood attack, HTTP flood attack, TCP SYN attack, TCP PUSH and ACK attack. Phishing, SQL injection, Cross site scripting
User	Privacy	Identification, Tracking, Profiling
IoT Malware	Service disruption, Data espionage.	Linux.Hydra, Psyb0t, Tsunami/Kaiten, Aidra, BashLite, Mirai, Hajime, IoTReaper, VPNFilter

3. IoT security threats and attacks

To understand the threat scenario in-depth, we analyze the IoT ecosystem from four perspectives: devices, internal network services, external network services and users. The primary security threats vary from each perspective. In Fig. 2, we illustrate these categories. The device category covers all the threats that use interfaces, memory and computing power to disrupt device functioning. The category of internal network services mainly includes the exploitation inside an IoT network. Since many IoT devices operate in open environments, insider threats are most obvious and treated with utmost care.

The connectivity to the Internet infrastructure provides remote access to the devices. The increased number of IoT devices and poor security configurations make these devices an attractive target for massive distributed denial of service(DDoS) attacks. In external network services, we cover such attacks that exploit the vulnerability of web services. Finally, the fourth category deals with the privacy threats against users in an IoT ecosystem. Next, we provide a detailed discussion on significant threats to these categories. In Table 2 we illustrate various attacks and related attack surfaces.

3.1. Device

Devices comprising sensors and actuators are the fundamental elements in the IoT ecosystem. Every IoT device will have a perception layer to provide functionalities such as modulation/demodulation, encryption/decryption, frequency selection, data transmission, and reception to perceive their environment. The significant challenges associated with these objects are energy utilization, security and interoperability [7]. The rigorous analysis of the significant perils that inversely affect these devices will give more insights into the necessary security measures at the perception and upper layers. This section details some of the significant threats and attacks on devices.

3.1.1. Replay attack

A replay attack is performed by spoofing, altering, or replaying the identity information of intelligent devices in the IoT network [7].

3.1.2. Node capture attack

A node capture attack occurs when an intruder gains control over nodes and captures valuable data. This way, the attacker can send malicious data to other nodes in the network [12].

3.1.3. Side Channel Attacks (SCA)

SCA exploits the target devices' physical information leaking from different side channels such as power consumption (power analysis attack), electromagnetic radiation (EM attack), and time taken for computation (timing attack). An adversary can effortlessly extract the secret key by analyzing side-channel parameters using relatively low-cost tools within a short period [12]. Hence SCA poses a severe menace to IoT devices.

3.1.4. Jamming attack

This attack is performed through intentional radio signal emissions to decrease the signal to noise ratio, thereby disrupting the functioning of nodes, causing a denial of service [7]. Constant jamming, deceptive jamming, random jamming and reactive jamming are different types of Jamming attacks. In continuous jamming, the target channel gets interrupted continuously, whereas, in random jamming, the transmission of radio signals over the target channel occurs on a random basis. In deceptive jamming, the adversary employs regular data frames rather than radio signals over the target communication channel. In reactive jamming, the adversary operates based on the targeted channel's network activity.

3.1.5. Booting attacks

Smart things are prone to various attacks during the device initialization (booting). As inbuilt security processes will not be there at booting time, adversaries can quickly attack nodes and capture them. Also, sleep–wake cycles in low powered devices hinder the secure boot process [4].

3.1.6. Firmware update attacks

It is imperative to verify the integrity of the IoT devices taking part in communication. Therefore, the firmware regulating the behavior of the embedded system should be secure and periodically updated to address vulnerabilities on the device. Reverse engineering, firmware modification, and unauthorized firmware installation are some examples of firmware attacks. [11] discusses hardware, software and hybrid attestation techniques as a solution against firmware attacks.

3.2. Internal network services

The tiny smart devices often create Low power and Lossy Networks (LLN). They employ multi-hop communication protocols to interact with each other. If not IP enabled, most objects communicate with the external world via IoT enabled gateways or hubs. The gateways or hubs function as an intermediary aggregator before passing the collected data to the servers for further processing and analytics for intelligent service provision. The network layer in IoT devices is responsible for maintaining consistent internal IoT networks. In other words, this layer governs network availability, scalability, power utilization, and security. The multi-hop protocols bring about the possibility of internal threats. As more and more heterogeneous IoT devices become part of the IoT network, the internal threats will adversely affect the trust associated with each object. An in-depth study of insider threats that exploit internal network services will help design suitable trust management systems within the IoT network. Next, we discuss major insider threats in detail.

3.2.1. Black hole attack/Selective forwarding Attack (Gray hole attack)

Sensor nodes collaborate to forward packets from one node to another in a local network. In a black hole attack, [13], the malicious node(s) does not take part in the packet forwarding process in such a way that it may drop all the data packets resembling a black hole in the network and causing Denial of Service(DoS). The Fig. 3 illustrates a black hole attack, where the malicious node "c" drops all packets after joining the network. Unlike black hole attacks, the hostile nodes drop only selected packets in gray hole attacks.

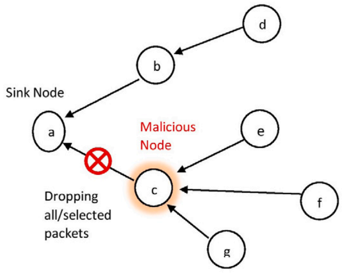

Fig. 3. Black hole Attack/Gray hole attack: An illustration.

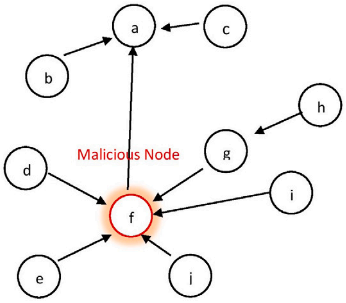

Fig. 4. Sinkhole Attack: An illustration.

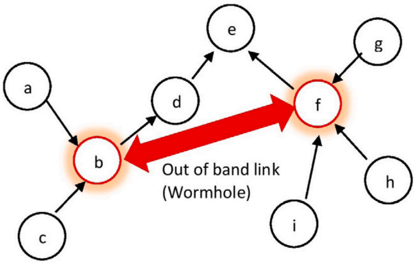

Fig. 5. Wormhole Attack: An illustration.

3.2.2. Sinkhole attack

In sinkhole attack [14], the malicious node(s) advertise fabricated route with prevaricated matrices and try to be in sink with as many nodes as possible. As shown in Fig. 4, the malicious node “f” advertises the better route matrices with their neighbors, resulting in it becoming the parent for many nodes. Although sinkhole attacks are not disruptive, they can damage the whole network traffic combined with other attacks such as gray hole attacks and black hole attacks.

3.2.3. Wormhole attack

In Wormhole, two malicious nodes collaboratively create a tunnel. Instead of transmitting packets either entirely or selectively through the regular dedicated path in the network, the adversary uses this tunnel.

An adversary commonly uses three ways to create Wormholes: Packet Encapsulation, Packet Relay, and Out-of-Band Link [13]. Malicious nodes use the out-of-band link (wired or wireless) to interact with each other. Thus an adversary can communicate with the network and bypass the border router. For example, in Fig. 5, the malicious nodes “b” and “f” creates out of band link to communicate with each other. In this way, node b can send all packets to node “f” instead of root “e”.

3.2.4. Sybil attacks

In a Sybil attack, malicious node(s) takes the identity of another legitimate node(s). In this way, Sybil node(s) can advertise multiple identities of legitimate devices. Adversary targets nodes in a fixed region or a randomly distributed network and compromises the identities of nearby nodes to launch the attack in the network.

3.2.5. HELLO flood attack [13]

New nodes join a network by broadcasting "HELLO" messages. In this attack, the adversary uses powerful computational devices to broadcast HELLO messages with better routing metrics and then disappears or reduces transmission power. Thus, the perpetrated advertisements make the malicious node the preferred parent route for other neighborhood nodes while transmitting data packets. Consequently, the packets from legitimate nodes would fail to deliver, leading to the exhaustion of honest nodes.

3.2.6. Eavesdropping

As IoT devices are often deployed in open environments and also use wireless communication technologies, eavesdroppers can capture sensitive data from the communication medium. Radio Frequency Identification (RFID) and Near Field Communication (NFC) systems are more prone to this attack since it lacks any encryption technique during the transmission process.

3.3. External network services

The connectivity to the external world or the Internet makes IoT devices vulnerable to external attacks. Different DDoS Attacks and Web-based attacks can threaten the functioning of standalone application servers or servers in the cloud. Therefore, a thorough study of the most prominent external threats will help devise peripheral security defensive and preventive measures toward the extensive exploitation of IoT devices. Many resource-constrained IoT devices with poor security make an attractive space for attackers to launch DDoS attacks against well-established services. The below section gives a brief overview of some of the most common DDoS attacks carried out in the past decade.

3.3.1. UDP flood attack

In UDP Flood Attack, a large amount of UDP packets are sent to either random ports or a selected port of the victim server by the compromised nodes using spoofed IP addresses [15]. On receiving the packet, the host attempts to identify the application running on that port, finds none, and sends back the "Destination unreachable ICMP" (Internet Control Message Protocol) message as the respective response. However, the response packet does not often reach its senders since compromised nodes often use spoofed IP addresses to hide their identity. Consequently, the victim's network bandwidth gets exhausted, causing a denial of service to even legitimate users.

3.3.2. ICMP flood attack

In ICMP Flood Attack [15], a lot of ICMP ECHO REQUEST packets (also called "ping") are sent to the victim machine by the compromised nodes using spoofed IP addresses. These packets request a reply from the victim machine. The combination of requests and responses leads to the victim's network bandwidth depletion denying service to legitimate nodes. Since malicious node often uses spoofed IP addresses, the response messages never reach nodes from where the request originated. This attack can effectively disable the network connectivity.

3.3.3. Smurf attack

Smurf attack [15] is a specific type of ICMP flood attack in which the attacker with a spoofed IP address sends ICMP ECHO REQUEST packets to a routing system (target machine) that supports broadcast addressing. The router will broadcast the ping packets to all the machines within its broadcast address range. On receiving, each device sends back ICMP ECHO REPLY to the target machine. The original attack packet gets amplified significantly depending on the number of systems located in the target machine's broadcast address range. Thus, the attack affects both the target machine and the intermediate broadcast systems.

3.3.4. Fraggle attack

Fraggle attack [15] is a type of UDP Flood Attack in which the attacker with a spoofed IP address sends UDP ECHO packets to the router or server that supports broadcast addressing. Either sending UDP ECHO packets can perform this attack to the port that supports character generation protocol (port 19) or spoofing the source port with victim echo service protocol (port 7), creating an infinite loop. The same will happens at each intermediary broadcast system as well. As a result, the Fraggle attack is more disruptive than the Smurf attack due to its ability to produce more packets.

3.3.5. DNS flood attack

In DNS Flood attack [15], the compromised nodes send a large number of spoofed DNS queries to the targeted name server. As malicious DNS requests are identical to benign ones, it is challenging to detect such attacks.

3.3.6. HTTP flood attack

In HTTP Flood Attack [16] a significant number of HTTP requests from the infected machines or bots overwhelm the target server. An adversary can launch an HTTP flood attack in two ways: HTTP GET attack occurs when the attacker employs a botnet to concurrently initiate HTTP GET requests for arbitrary files and images from the target server. The server, exhausted with malicious requests, cannot even serve legitimate requests. In an HTTP POST attack, the attacker uses a botnet to submit forms on a Website. The website will be kept busy in this computationally and bandwidth-intensive task. The server eventually gets exhausted. The HTTP POST attacks are more dangerous than HTTP GET attacks since the former often includes some parameters that trigger complex processing on the server.

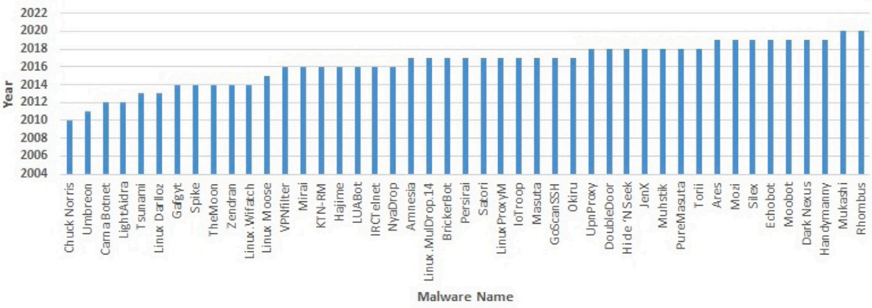

Fig. 6. Growth of IoT malware family between year 2010 and 2020.

3.3.7. TCP SYN attack

The handshake protocol in TCP operates based on a series of acknowledgments from both server and client [16]. As part of connection establishments, the server sends an SYN-ACK packet to each SYN packet received from the client awaiting further acknowledgment to complete the handshake process. The server will allocate space in the memory stack until a specific period or till connection establishment. Exploiting this weakness adversary sends spoofed SYN packets to the server in large volumes. The server will process the requests and provide SYN-ACK as the response. However, the responses never reach the actual destination as malicious nodes have hidden their identity. The half-open connections consume the server's resources. Eventually, the server will reach a limit that it cannot accept SYN requests anymore.

3.3.8. TCP PUSH and ACK attack

In this attack [16], the attacker instructs their bots to send many TCP packets to the target server with the PUSH and ACK flag set to "1". These flags direct the server to unpack all the data in the TCP buffer and send it back ACK message [15]. The large volume of PUSH and ACK packets from different bots will eventually exhaust the server resources.

3.3.9. Other attacks

According to the Open Web Application Security Project (OWASP), IoT systems' access via web interfaces is more vulnerable to SQL injection and cross-site scripting (XSS). The SQL injection attack [15] allows an attacker to read the database containing the login credentials of other users. Once the adversary obtains the credentials, they can control other devices and perform several other attacks using the compromised machines. Cloud management consoles are also susceptible to this kind of attack.

3.4. Users

Privacy is a primary concern from the users' point of view. The inherent nature of intelligent things in terms of ubiquitous data collection and tracking often raises privacy threats, limiting the success of the Internet of Things vision if not correctly handled. With increased scale and heterogeneity in IoT devices, users will likely maintain multiple identities resulting in various interactions supporting these identities. Privacy threats can happen from the perception phase to the data dissemination phase.

Authors in [17] define privacy as individual control over the level of personal data collection of the subject and awareness of subsequent use of the collected data by entities outside the subject's control sphere. Humans can be subject to data collection by the surrounding smart things or recipients of data or services [18]. This definition clearly describes the information self-determination property of the subjects involved.

IoT devices and services generate data that often describe the constituting entity uniquely. For example, an intelligent thermostat collects data such as temperature, humidity, and motion to make inferences and adjust the temperature automatically. However, this also gives insight into occupants' current state and activities. Hence intrusion into this data causes privacy threats. In other words, by inferential profiling, information and communication technologies could derive a new user identity, called externally constructed informational identity, apart from self-constructed identity. Inferential profiling can take place in three ways: (i) data collection from a single IoT device (e.g., Internet browsing behavior) (ii) Linking of multiple IoT data sets for more extensive profiling, also called sensor fusion (iii)profiling through data sharing with third parties such as insurance [19].

4. IoT malware

Recent years have seen a rapid increase in IoT malware. Fig. 6 shows the evolution of IoT malware in the past ten years. Statistics show that the number of IoT malware families is increasing rapidly. Hence IoT security threat analysis will not be complete without discussing IoT malware. Adversaries use IoT malware to perform massive Distributed Denial of Service(DDoS) attacks and other endpoint exploits. The following sections provide a detailed description of different IoT malware in detail.

4.1. Tsunami/Kaiten

This malware empowers botnets to carry out traditional SYN flood attacks, UDP flood attacks, PUSH and ACK attacks, sophisticated HTTP flood attacks and TCP XMAS attacks. Moreover, in 2016, this malware-infected Linux Mint Official ISO, threatening a huge number of freshly installed Operating Systems.

4.2. Aidra

Aidra [15]is a DDoS capable IoT malware. LightAidra and Zendran are some of the variants of Aidra. This IoT malware can infect devices with different architectures such as MIPS, ARM, and PowerPC due to cross-compiled binaries. The IRC-based botnet architecture relies on brute force attacks to gain access and carry out attacks like TCP SYN flooding and PUSH and ACK flooding.

4.3. BashLite

BashLite [20], a DDoS capable IoT malware family derived from Aidra, appeared in the wild of 2014, targeting Linux based devices. Gafgyt, Lizkebab, Qbot, Torlus and LizardStresser are the known variants of BashLite. The malware exploited Telnet ports using brute force attacks by generating random IP addresses. Furthermore, the lightweight version of the Internet Relay Chat (IRC) protocol gave malware the potential to execute independently of the IRC server. Hence it is considered as an Agent-Handler based botnet. Although the deliverable attacks include only SYN, UDP and ACK Flood attacks like its predecessors, BashLite can even infect SPARC devices.

4.4. Mirai

Mirai is one of the most predominant IoT malware in the past decade, which nearly changed the world's perception of IoT security due to the massive disruption it caused. The sophisticated features of Mirai [15] enable it to conduct massive attacks on several CPU architectures based on UDP, TCP, DNS and HTTP. The malware created an enormous botnet through a dictionary attack by compromising around 500,000 IoT devices with poor security, such as home routers, CCTV cameras, and Digital Video Recorders (DVRs). The attacks include service disruption of a French Internet and hosting provider, OVH, in September 2016 and Dyn DNS server in October 2016. The public release of its code has given birth to a wide variety of new malware with improved capabilities.

4.5. Hajime

Although the propagation strategy looks similar to Mirai, Hajime [20] differs in its design and operation uniquely. Unlike other malware, Hajime used a peer to peer system as its command-and-control infrastructure with the continuous inclusion of new exploits. This feature makes Hajime like malware more robust and fault-tolerant. Furthermore, the compromised peer nodes are grouped based on their architecture and other features. Apart from that, Hajime botnet has anti-detection features such as masquerading itself as a Telnet process.

4.6. IoTReaper

IoTReaper is an IoT malware with inherited properties of Hajime and Mirai that emerged in late 2017. However, unlike Mirai, IoTReaper employs known security flaws in the code of insecure devices to gain access and installs back-doors. This malware exploits numerous vulnerabilities in different IoT devices such as routers from D-Link, Netgear, and internet surveillance cameras.

4.7. VPNFilter

VPNFilter targets industrial plants and companies. It can spy on any local network from a compromised machine [15]. This malware targets the most prevalent Industrial Control System (ICS) communication protocol Modbus.

5. Discussion

This section summarizes the lessons learned from our analysis, including the critical security requirements that need to be addressed for designing a secure IoT system.

- **Identity Management:** Identity management in IoT means consistently identifying users and objects, enabling efficient resource and service discovery. The scalability and interoperability issues in IoT technology demand distributed identity and access management systems over centralized systems. IoT security must provide reliable techniques for administering devices' and users' identities to handle their relationships flexibly. However, it poses privacy risks due to multiple interactions and sensitive personal data exchange between devices and service providers. Currently, there are no globally accepted identity management protocols such as certification authorities and commonly accepted trust negotiation language [21].

- **Authentication and Access Control mechanisms:** Access control mechanisms can protect IoT devices from unauthorized access. However, the IoT ecosystem demands more fine-grained and context-aware access control mechanisms [22]. Researches show that Attribute-based access control models can bring context-awareness and granularity to some extent. However, current IoT application protocols such as MQTT and CoAP do not include such solutions [23]. Hence, mapping existing systems to different access control models can reveal more insight into its benefits and risks and thus design better context-aware solutions.
- **Trust Management Systems:** Since IoT devices are prone to attacks within the network, defaming the trust of the network/device, we need trust management systems that can ensure the authenticity of objects that take part in communication. Studies based on policy-based and trust score-based techniques address this issue. However, the potential applicability of recent technologies such as blockchain and software-defined networking (SDN) needs to be explored thoroughly.
- **End to End Communication Security:** End-to-end communication security is a critical requirement for these IoT application scenarios, which can protect sensitive data even if the underlying network infrastructure is not under the user's control [24]. Current IoT security solutions include standards-based proposals. The Transport Layer Security (TLS) protocol and its datagram-oriented variant Datagram TLS (DTLS) protocol are the de-facto protocols for communication security in the IoT, which can provide encryption, authentication, and data integrity for information exchange. However, deployment of the above protocols raises a significant challenge to operate with highly constrained devices [25]. It requires a lightweight end to end security solution suitable for IoT applications.
- **Lightweight Security Solutions:** The resource constraint nature of IoT devices makes it challenging to apply traditional security techniques directly to IoT networks. Lightweight security solutions with a balance between cryptographic techniques and improved computing resource(memory, power) consumption can better serve IoT security requirements. However, much of the research in IoT security makes computationally overloaded designs challenging for resource-constrained devices.
- **Intrusion Detection System (IDS):**Protecting the IoT network from malicious activities from the Internet infrastructure is of greater importance, as attackers often perpetrate massive service disruption attacks such as DDoS attacks and IoT malware by exploiting these devices. Most research focuses on network-based intrusion detection systems rather than host-based IDS due to the resource constraints associated with IoT devices. But the insufficiency of real-time data sets often makes it challenging to measure and compare the efficiency of the studies.

6. Conclusions

The Internet of Things is an emerging paradigm that can make several opportunities with a range of cost-effective, efficient applications and services to the end-users. However, security is one of the leading concerns towards a broader deployment of IoT systems. An IoT system will be vulnerable to attacks if a proper assessment of potential threats and attacks does not meet appropriate security requirements. In this paper, we have analyzed the concerns regarding the non-standardization of IoT architecture. Systematic approaches considering IoT systems as a whole ecosystem have added flexibility while security and design implementations. Hence we analyzed significant threats and attacks on essential elements in an IoT ecosystem, systematically combining the derived four-layered IoT architecture. We have also included a detailed study of different IoT malware families by considering the recent increase in malware attacks against IoT devices. Finally, we discuss the critical security requirements that need to be explicitly advanced for IoT systems, which will help researchers in IoT security to innovate new and improved security solutions.

CRediT authorship contribution statement

Renya Nath N: Methodology, Writing, Formal analysis, Resources, Visualization . **Hiran V Nath:** Conceptualization, Writing, Supervision, Project administration.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Kouicem DE, Bouabdallah A, Lakhlef H. Internet of things security: A top-down survey. Comput Netw 2018;141:199–221.
[2] Hassan WH, et al. Current research on internet of things (IoT) security: A survey. Comput Netw 2019;148:283–94.
[3] Ogonji MM, Okeyo G, Wafula JM. A survey on privacy and security of internet of things. Comp Sci Rev 2020;38:100312.
[4] Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access 2019;7:82721–43.
[5] Mahbub M. Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. J Netw Comput Appl 2020;102761.
[6] Lu Y, Da Xu L. Internet of things (IoT) cybersecurity research: A review of current research topics. IEEE Internet Things J 2018;6(2):2103–15.
[7] Iqbal W, Abbas H, Daneshmand M, Rauf B, Bangash YA. An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. IEEE Internet Things J 2020;7(10):10250–76.
[8] Aly M, Khomh F, Haoues M, Quintero A, Yacout S. Enforcing security in internet of things frameworks: A systematic literature review. Internet Things 2019;6:100050.
[9] Mrabet H, Belguith S, Alhomoud A, Jemai A. A survey of IoT security based on a layered architecture of sensing and data analysis. Sensors 2020;20(13):3625.
[10] Pal S, Hitchens M, Rabehaja T, Mukhopadhyay S. Security requirements for the internet of things: A systematic approach. Sensors 2020;20(20):5897.

[11] Hou J, Qu L, Shi W. A survey on internet of things security from data perspectives. Comput Netw 2019;148:295–306.
[12] Tsague HD, Twala B. Practical techniques for securing the internet of things (IoT) against side channel attacks. In: Internet of things and big data analytics toward next-generation intelligence. Springer; 2018, p. 439–81.
[13] Raoof A, Matrawy A, Lung C-H. Routing attacks and mitigation methods for RPL-based internet of things. IEEE Commun Surv Tutor 2018;21(2):1582–606.
[14] Liu Y, Ma M, Liu X, Xiong NN, Liu A, Zhu Y. Design and analysis of probing route to defense sink-hole attacks for internet of things security. IEEE Trans Netw Sci Eng 2018;7(1):356–72.
[15] De Donno M, Dragoni N, Giaretta A, Spognardi A. Ddos-capable IoT malwares: Comparative analysis and mirai investigation. Secur Commun Netw 2018;2018.
[16] Salim MM, Rathore S, Park JH. Distributed denial of service attacks and its defenses in IoT: a survey. J Supercomput 2019;1–44.
[17] Ziegeldorf JH, Morchon OG, Wehrle K. Privacy in the internet of things: Threats and challenges. Secur Commun Netw 2014;7(12):2728–42.
[18] Hernandez G, Arias O, Buentello D, Jin Y. Smart nest thermostat: A smart spy in your home. 2014, Black Hat USA, no. 2015.
[19] Wachter S. Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the GDPR. Comput Law Secur Rev 2018;34(3):436–49.
[20] Ceron JM, Steding-Jessen K, Hoepers C, Granville LZ, Margi CB. Improving iot botnet investigation using an adaptive network layer. Sensors 2019;19(3):727.
[21] Sicari S, Rizzardi A, Coen-Porisini A. 5G in the internet of things era: An overview on security and privacy challenges. Comput Netw 2020;179:107345.
[22] Ravidas S, Lekidis A, Paci F, Zannone N. Access control in internet-of-things: A survey. J Netw Comput Appl 2019;144:79–101.
[23] Malik AK, Emmanuel N, Zafar S, Khattak HA, Raza B, Khan S, et al. From conventional to state-of-the-art IoT access control models. Electronics 2020;9(10):1693.
[24] Prantl T, Iffländer L, Herrnleben S, Engel S, Kounev S, Krupitzer C. Performance impact analysis of securing MQTT using TLS. In: Proceedings of the ACM/SPEC international conference on performance engineering. 2021, p. 241–8.
[25] Park C-S, Nam H-M. Security architecture and protocols for secure MQTT-SN. IEEE Access 2020;8:226422–36.

Renya Nath N is currently pursuing Ph.D. in Computer Science and Engineering at National Institute of Technology Calicut, Kerala. She received a bachelor's degree in Information Technology from the University of Calicut and a master's degree in Computer Science and Engineering from Anna University. Her research interest includes Cyber Security, IoT security, Access Control Mechanisms, Communication Security, and IoT malware.

Hiran V Nath is currently working as an Assistant Professor in the Department of Computer Science and Engineering at National Institute of Technology Calicut, Kerala. He received Ph.D. from Institute for Development and Research in Banking Technology(IDRBT), University of Hyderabad, in 2016. His research interest includes Cyber Security, Banking Security, Malware Analysis, Network Vulnerability & Analysis, Attack Graphs, and Digital Forensics.