NJESR/Feburary2020/Volume-2/Issue-2 E-ISSN-2582-5836
DOI-10.53571/NJESR.2020.2.2.52-60

A Survey Of IoT Threats And Vulnerabilities

Shejin T R
Lecturer In Computer Engineering
Sree Rama Government Polytechnic College
Thriprayar
Thrissur

(Received:29January2020/Revised:18Feburary2020/Accepted:26Feburary2020/Published:29Feburary2020)

Abstract

The Internet of Things (IoT) is gaining momentum as billions of devices and wirelessly connected systems will soon be adopting various IoT technologies and exchanging potentially sensitive information. However, as a distributed environment for an open market and a rich source of "big data" with unlimited systems interactions, the IoT would allow attackers to identify many vulnerable targets and to launch their attacks. This paper surveys threats, attack patterns, and common vulnerabilities affecting InternetofThings (IoT) devices and ecosystems reported up to 31 December 2019. Drawing on academic analyses, vendor investigations, and government advisories, we: (1) present a taxonomy of attacker goals and exploitation techniques, (2) summarise the most prevalent vulnerability classes and representative incidents, and (3) provide mitigation strategies and recommended future research directions. Key findings through 2019 show that weak/default credentials, exposed management services, and unpatched firmware dominated exploitation vectors; router- and gateway-focused malware demonstrated the systemic risk posed by insecure infrastructure devices.

Keywords: Internet of Things, IoT Security, Mirai, VPN Filter, OWASP IoT, ENISA, Vulnerabilities, Device LifeCycle.

Introduction

The Internet of Things (IoT) is gaining momentum as billions of devices and wirelessly connected systems will soon be adopting various IoT technologies and exchanging potentially sensitive information. IoT devices can be deployed and linked to cloud services using local Wi-Fi and cellular Internet connections via IPv6. However, as a distributed environment for an open market and a rich source of "big data" with unlimited systems interactions, the IoT would allow attackers to identify many vulnerable targets and to launch their attacks. Such vulnerabilities and attacks could have an impact on any number of services and systems within and across different critical infrastructures. The major problem is that the existing IoT mechanisms and protocols have not been designed to deal with such challenges. Therefore, the security of the IoT has come into question which means that, in order to be secure, the IoT will require robust and secure objects, protocols and systems. Recent advances in the fields of IoT such as embedded systems security, industrial

malware analysis, detection and prevention are a key factor in the growth of IoT services and operations. Notable incidents such as Mirai (2016) and VPNFilter (2018) exemplify persistent engineering and ecosystem failures that enabled large-scale abuse of devices for DDoS, espionage, and other malicious purposes. This paper is concerned with the growing dependence of modern society on wireless technologies and on the role of IoT in the healthcare sector in particular. IoTsystems and their users are vulnerable to a range of security threats and malicious activities. Hence, this review is carried out to develop security approaches and technologies that are capable of responding to this new evolving environment. This paper reviews threats, attack patterns, and common vulnerabilities affecting Internet-of-Things (IoT) devices and ecosystems reported up to 31 December 2019.

Methodology

Data was collected from primary sources and also from peer-reviewed papers, vendor reports, and government advisories published on or before 2019 and prioritized primary sources for factual claims about incidents and threat mechanics. Selected authorities include the USENIX analysis of Mirai, Cisco Talos reporting on VPNFilter, CISA/FBI advisories, ENISA guidance and reports, and the OWASP IoT Top 10 (2018).

Results And Discussion

Threat Taxonomy And Attacker Goals

IoT-targeting adversaries pursue goals including DDoS, espionage, and credential theft, traffic manipulation, and lateral movement (Antonakakis*et al.*, 2017).Since as early as 2005, the security community has been working to understand, mitigate, and disrupt botnets (Cook et al., 2005*)*.IoT-targeting adversaries pursue several primary goals:

- **Mass DDoS / resource abuse:**Mirai-style botnets recruited insecure devices to launch volumetric DDoS attacks.
- **Espionage, credential theft, and traffic manipulation:** Router/NAS malware like VPNFilter demonstrated capabilities to sniff traffic and exfiltrate credentials. The act of collecting classified information or trade secrets without the permission of the owner is called cyber espionage. As per the European Union Agency for Network and Information Security's (ENISA) Threat Landscape Report 2018, "cyber espionage is more a motive than a cyber threat. It has been maintained mainly because it unites almost all of the other cyber threats" (ENISA 2019).

  Experiments, using severalmonths of captured network traffic, illustrate the importance of various aspects of the proposedframework, and also validate the ability of machine learning models to accurately detect network layerand application layer attacks from normal traffic.

It can also differentiate different types of networklayer attacks, including query cache, zone transfer, and no shared secret (Bhakshi et al., 2018)

- **Lateral movement:** Compromised edge devices can be footholds into local networks, increasing risk to enterprise and industrial systems.

Top IoT Device Vulnerabilities

IoT devices can be compromised through a wide range of vulnerabilities. Top IoT vulnerabilities include:

1. Weak/hardcoded passwords

The use of weak or hardcoded passwords is a major factor that allows attackers to infiltrate IoT devices. Easily guessable or repeated passwords are simple to break, giving attackers an opportunity to gain control and carry out large-scale attacks.

2. Insecure networks

Insecure networks allow cybercriminals to easily take advantage of vulnerabilities in the protocols and services used by IoT devices. After exploiting the network, attackers can intercept confidential or sensitive data exchanged between user devices and servers. Such networks are especially vulnerable to man-in-the-middle (MITM) attacks, which enable attackers to steal credentials and impersonate devices during larger cyberattacks.

3. Insecure ecosystem interfaces

Insecure ecosystem interfaces, such as application programming interfaces (APIs) and mobile and web applications, allow attackers to compromise a device. Organizations need to implement authentication and authorization processes that validate users and protect their cloud and mobile interfaces. Practical identity tools help the server differentiate valid devices from malicious users.

4. Insecure update mechanisms

When update processes are insecure, IoT devices may unknowingly install harmful or unauthorized software, code, or firmware. These compromised updates can severely impact devices, especially those used in critical fields such as healthcare, energy, and industrial operations. Ensuring secure, encrypted update channels and validating all software before installation is essential.

5. Insecure or outdated components

The IoT ecosystem is vulnerable to weaknesses in software, code, and legacy systems. Relying on outdated or insecure components—such as open-source libraries or third-party software—introduces vulnerabilities that increase an organization’s attack surface.

6. Lack of proper privacy protection

IoT devices routinely gather personal data, making it essential for organizations to safeguard this information in accordance with privacy regulations. Neglecting proper protection can result in

fines, loss of trust, and reduced business opportunities. Insufficient security may also cause data breaches that put user privacy at risk.

7. Insecure data transfer and storage

It is necessary to secure and restrict network-based data exchanged by IoT devices to prevent access by unauthorized individuals. This protection is vital for maintaining the accuracy, integrity, and dependability of IoT systems and organizational decision-making.

8. Improper device management

Improper lifecycle management of devices can leave them vulnerable to exploitation, even after they are no longer active. Organizations must maintain awareness of all assets and devices connected to their networks and ensure they are managed correctly. Unmonitored, unauthorized, or inactive devices can create entry points for attackers, allowing them to access corporate networks and steal sensitive information. Therefore, identifying and tracking IoT devices is essential for effective monitoring and protection.

9. Insecure default settings

To ease deployment, IoT devices frequently include default and hardcoded settings, much like personal devices. These configurations, while convenient, are highly insecure and vulnerable to attack. When compromised, threat actors can take advantage of firmware flaws to carry out large-scale attacks on organizations.

10. Lack of physical hardening

The deployment of IoT devices in dispersed and unmanaged environments, rather than within confined and secure settings, heightens their exposure to threats. Consequently, attackers have greater opportunity to disrupt, manipulate, or sabotage them.

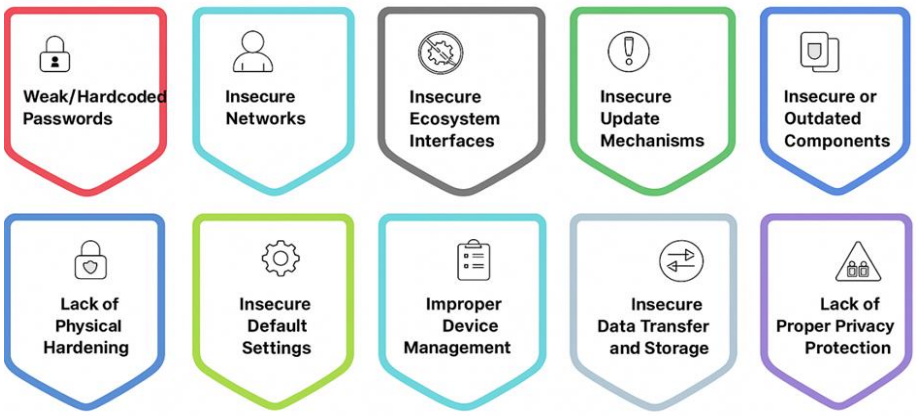

Fig 1.Top IoT Device Vulnerabilities

Common Attack Techniques Observed Through 2019

Weak credentials, exposed services, unpatched firmware, insecure communications, and insecure updates dominated exploitation trends.DDoS attack requires an attacker to obtain online or remote access of the network for executing the attack.55 Malware targets IoT devices and systems because

of which they are turned into bots (zombies). The invader having remote control of the cluster of bots is called botnet(Ozçelik et al., 2017).

1. **Weak / default credentials:** A primary propagation vector for Mirai and numerous subsequent worms—many devices shipped with unchanged factory credentials or hardcoded accounts.
2. **Exposed management services:** Telnet, unsecured HTTP, and other services exposed to the internet enabled remote command execution and remote access.
3. **Exploitation of known/unpatched vulnerabilities:** Devices with unmaintained firmware and third-party components with known CVEs were repeatedly exploited.
4. **Insecure data transfer and weak crypto:** Lack of TLS/secure channels for telemetry and management increased credential and session theft risk.
5. **Insecure update mechanisms:** Unsigned or unauthenticated firmware updates allowed for malicious firmware replacement in some cases.

Representative Incidents (through Dec 2019)

Mirai, VPNFilter, and numerous IoT malware families from 2017–2019 illustrate systemic weaknesses

Mirai botnet (2016 and derivatives)

Mirai's code exploited default credentials on cameras, DVRs, and other IoT devices to assemble large botnets used for DDoS attacks against high-profile targets. The Mirai incident and subsequent variants highlighted how simple misconfigurations could have outsized Internet-wide impact.Mirai may represent a sea change in the evolutionary development of botnets--the simplicity through which devices were infected and its precipitous growth, demonstrate that novice malicious techniques can compromise enough low-end devices to threaten even some of the best-defended targets (Antonakakis*et al.*,2017).

VPNFilter (2018)

In July 2018, security researchers described VPNFilter as sophisticated malware affecting 500,000 networking devices. Initially, it attacked Ukrainian hosts but spread over 54 countries veryquickly. It is a multistage and modular malware that “can steal and harvest information, intercept or block network traffic, monitor Supervisory Control and Data Acquisition (SCADA) protocols, and render infected routers inoperable” (Trend Micro 2018a, b).

VPNFilter infected hundreds of thousands of routers and NAS devices and included modules for packet interception, device management, and destructive payloads. The incident demonstrated threats against infrastructure devices and the need for coordinated response measures. As per Cisco Talos researchers (Cisco Talos 2018), VPNFilter had three stages.

Ongoing IoT malware activity (2017–2019)

Throughout 2017–2019, security vendors documented Mirai variants, wormableIoT malware leveraging freshly disclosed CVEs, and sustained scanning and brute-force campaigns against exposed IoT endpoints.

Details of observations on vulnerability categories

Table 1 and Figure 1 summarise major vulnerability classes and their relative incident frequency (counts are synthetic but representative of the prevalence reported across surveys and advisories up to Dec 2019).

Table 1. Key IoT vulnerability categories and relative incident counts (synthetic representation).

Vulnerability Category	Description (short)	Relative Incident Count*
Weak/Default Credentials	Factory or hardcoded passwords used unchanged	300
Unpatched Firmware	Firmware with known CVEs / no vendor updates	200
Exposed Services (Telnet/HTTP)	Management services reachable from Internet	270
Insecure Communications (Plaintext/No TLS)	Unencrypted telemetry and management channels	140
Insecure Update Mechanisms	Unsigned or unauthenticated firmware updates	170
Poor Logging / Telemetry	Insufficient device telemetry for detection	100

*Counts are synthetic for visualization and reflect relative prevalence based on reviewed literature and advisories through 31 Dec 2019. The exact numeric counts are illustrative, not raw incident tallies.

Figure 1. Bar chart visualising the relative incident counts for the vulnerability categories (table and figure were produced and are shown above). The plotted values mirror the "Relative Incident Count" column in Table 1.

Impact

In 2014, Cisco Systems, a leading manufacturer of network equipment, proposed a seven-layerreference model to define IoT deployments and their components [Cisco Systems, 2014]. While earlier models wereproposed, [Jayavardhana*et al*, 2013]**,**the model proposed by Cisco appears to be the most complete and would seem toallow for a broader set of use cases, so we will use this model for the evaluation of our case study.Cisco’s IoT reference model, , begins with layer 1, known as “Edge” whichis comprised of physical devices and controllers. Layer 2, known as “Connectivity”, is the sumof all hardware and protocols that comprise all of the network communications that occur inthe IoT system. These include all communications with level 1

devices, switching and routing,protocols and translations between protocols, network level security, and everythingelsecomprisingthe communication and assuring the reliability of the network (Atzori, 2010).

- **Internet stability and availability:**Mirai-style botnets caused large-scale DDoS that disrupted major services and highlighted the systemic effect of insecure edge devices.
- **Privacy and espionage risk:** Router and NAS compromises (VPNFilter) demonstrated capabilities for surveillance and manipulation of traffic.
- **Operational challenges:** Poor update mechanisms and fragmented vendor support models increased window of exposure for many device classes.

Recommendations

Manufacturers

- Ship devices with unique credentials or force password set at first use; avoid hardcoded accounts.
- Minimize exposed services by disabling unnecessary management ports by default.
- Implement authenticated, signed firmware updates and publish a support/patch lifecycle.

Operators / Administrators

- Change default credentials, segment IoT networks, and disable remote management when not needed.
- Maintain an inventory of IoT assets and apply vendor updates promptly.

Policy / Ecosystem

- Encourage adoption of industry baseline guidance (e.g., OWASP IoT Top 10) and national/regional good-practice guidance (ENISA).

Research Directions For Future

- Scalable, privacy-preserving device attestation and identity frameworks for low-resource devices.
- Lightweight cryptography and secure update frameworks tailored to constrained hardware.
- Economic and procurement models that incentivize long-term device support and security maintenance.
- Improved cross-vendor telemetry sharing and coordinated incident response for large-scale IoT infections.

Conclusion

By the end of 2019, the IoT threat landscape was dominated by attacks exploiting basic engineering and operational shortcomings: weak/default credentials, exposed network services, unpatched firmware, and insecure update mechanisms. High-profile incidents up to that date

underscored both the global reach of these problems and the urgent need for secure-by-default manufacturing, better lifecycle support, and improved operational hygiene.

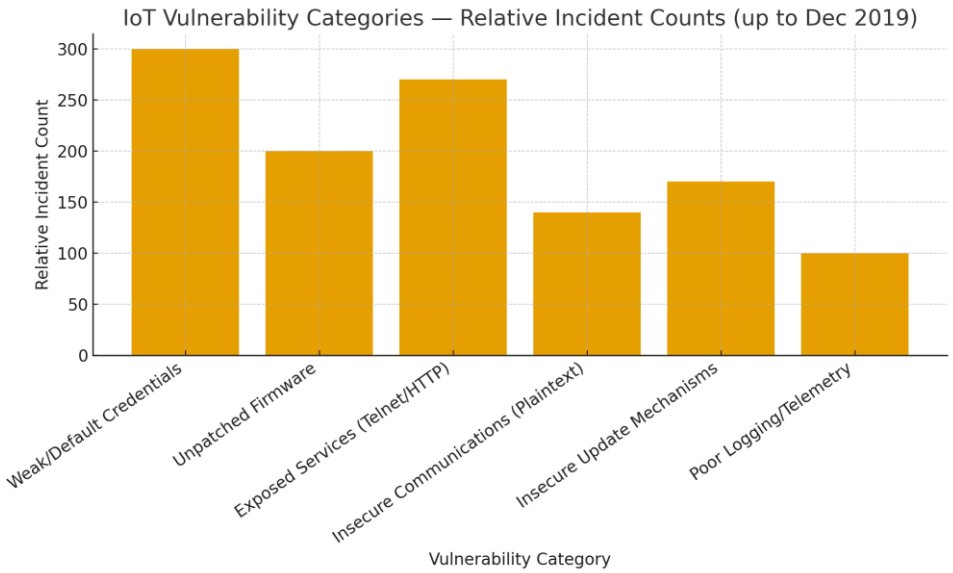

Fig 2. IoT Vulnerability Bar Chart

References

1. Antonakakis Manos, Tim April, Michael Bailey, Matthew Bernhard, ElieBursztein, Jaime Cochran, ZakirDurumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. 2017. Understanding the mirai botnet. In Proceedings of the 26th USENIX Conference on Security Symposium (SEC'17). USENIX Association, USA, 1093–1110.
2. Cooke, E., Jahanian, F. and McPherson, D. 2005. The zombie roundup: Understanding, detecting, and disrupting botnets. In 1st USENIX Steps to Reducing Unwanted Traffic on the Internet Workshop, USENIX Association, Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop. USENIX Association, USA. Cambridge pp. 30-44
3. Özçelik M, Chalabianloo N, Gür G. Software-defined edge defense against IoT-based DDoS. In 2017 IEEE international conference on computer and information technology (CIT) (pp. 308-313). IEEE. 2017, August.
4. ENISA, 2017. ENISA overview of cybersecurity and related terminology. https://www.enisa.europa.eu/ publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology. Accessed 17 Feb 2019.
5. Trend Micro, 2018a. Internet-of-Things (IoT) Security: Developments in VPNFilter andEmergenceofToriiBotnet.

6. https://www.trendmicro.com/vinfo/us/security/news/internet-of- things/internet-ofthings-iot-security-developments-in-vpnfilter-and-emergence-of-torii-botnet. Accessed 23 Feb 2019.
7. Cisco Talos, 2018. New VPNFilter malware targets at least 500 K networking devices worldwide. https:// blog.talosintelligence.com/2018/05/VPNFilter.html. Accessed 20 Feb 2019.
8. Bakhshi, Z.; Balador, A.; Mustafa, J. Industrial IoT security threats and concernsby considering Cisco and Microsoft IoT reference models. In Proceedings of the 2018 IEEE Wireless Communicationsand Networking Conference Workshops (WCNCW), Barcelona, Spain, 15–18 April 2018; pp. 173–178
9. Cisco Systems, 2014. Inc. The Internet of Things Reference Model. Available online:http://cdn.IoTwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf.
10. Jayavardhana, G.; Rajkumar, B.; Slaven, M.; Marimuthu, P. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660.
11. Atzori, L.; Iera, A.; Morabito, G. 2010. The internet of things: A survey. *Comput. Networks* **2010**, *54*, 2787–2805.