Internet of Things (IoT) Security: A Comprehensive Review of Threats, Challenges, and Countermeasures

Shubham Zende
1132220266
School Of Computer Science

Table of Content

Keywords- IoT security , vulnerabilities , risk management , cybersecurity , privacy , regulations , best practices , threat modeling , access controls , identity management , cryptography , secure code analysis , intrusion detection , software updates , federated learning , homomorphic encryption , blockchain technology

1. Introduction

The Internet of Things (IoT) refers to the network of physical objects embedded with sensors, software, and connectivity that enable data collection and exchange. IoT devices include common household items like smart thermostats, security cameras, appliances, and vehicles. There has been rapid growth in IoT devices and applications across industries like healthcare, transportation, manufacturing, and agriculture. It is estimated that there will be over 30 billion IoT devices by 2025 (Nordrum, 2016). While IoT innovation has led to greater efficiency, automation, and insights, it has also introduced new cybersecurity risks and challenges. This literature review provides a comprehensive overview of the key IoT security threats, challenges, and countermeasures.

2. IoT Security Threats

IoT systems have become a major target for cyberattacks due to the wealth of sensitive data they collect and ability to cause disruptions through access to physical systems. Common IoT security threats include:

- **Reconnaissance and Network Attacks**

One of the first steps in attacking an IoT system is through reconnaissance to map the network topology and discover vulnerable devices. Sicari et al. (2015) explain that attackers can fingerprint IoT devices through network reconnaissance including port scanning, traffic analysis, and probing default credentials. This allows them to identify device types, firmware versions, open ports, and IP addresses to target.

Network-level attacks are then used to gain leverage against IoT devices and networks. Denial of service (DoS) attacks overwhelm devices and networks with traffic to disrupt connectivity and service availability (Sicari et al., 2015). Distributed denial of service (DDoS) attacks leverage multiple compromised devices to amplify the scale and impact of disruption. IoT networks are especially vulnerable to DDoS attacks due to the sheer scale of potentially compromised devices with Internet connectivity (Bertino & Islam, 2017). The Mirai botnet in 2016 infected over 600,000 IoT devices through default password exploits and coordinated them for massive DDoS attacks exceeding 1 Tbps traffic against domain registration systems (Antonakakis et al., 2017).

Man-in-the-middle (MITM) attacks insert attackers between endpoints to eavesdrop on communications and manipulate traffic by compromising the integrity and authenticity of data exchanged (Roman et al., 2018). IoT networks rely heavily on wireless communications over mediums like WiFi, Bluetooth, Zigbee, and RFID which are susceptible to MITM attacks (Sicari et

al., 2015). IoT protocols such as Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) are also vulnerable to MQTT due to lack of built-in security (Roman et al., 2018). Without transport encryption, MITM attackers can gain access to sensitive data like health metrics and PII transmitted from IoT devices and falsify commands controlling physical systems.

Network spoofing attacks falsify the identity of devices and users on IoT networks. IP spoofing allows attackers to masquerade as trusted devices and bypass access controls (Roman et al., 2018). Sybil attacks create multiple fake identities to manipulate reputation systems and distributed computing algorithms reliant on valid identities (Sicari et al., 2015). IoT networks are prone to spoofing due to limited device authentication. Attackers can exploit spoofing to circumvent access restrictions and launch insider attacks while evading detection and accountability.

- **Malware Infections**

The constrained nature of many IoT devices limits their ability to run anti-virus and intrusion detection software. This makes IoT networks prime targets for malware infections including viruses, worms, spyware, and ransomware (Bertino & Islam, 2017). Mirai in 2016 and the VPNFilter malware in 2018 demonstrated how IoT malware can infect hundreds of thousands of vulnerable IoT devices for large-scale DDoS and data theft attacks (Bertino & Islam, 2017).

Worms are malicious programs that self-replicate across devices within a network by exploiting software vulnerabilities. The distributed nature of IoT networks allows worms to rapidly infect devices and critical systems (Sicari et al., 2015). Remote execution attacks take control of IoT devices through exploits and malicious code injection to launch attacks on other devices and networks (Roman et al., 2018). The killerbee toolkit and Shodan search engine lower the barriers to identifying and compromising vulnerable IoT devices.

Viruses inject malicious code into existing programs and devices to infect a network. IoT viruses can evade detection and disable security software due to limited device processing power (Bertino & Islam, 2017). The CodeBlue worm demonstrated how medical devices like CT scanners and MRI machines with weak authentication could be compromised to spread infections while remaining stealthy (Sicari et al., 2015).

Spyware gathers data and system information from compromised IoT devices silently without user consent. Data like network credentials, personal identities, and behavioral patterns is stolen and transmitted to external servers (Roman et al., 2018). The Moon worm targeted enterprise storage devices and spread by brute-forcing weak credentials to extract sensitive documents.

Ransomware encrypts data on infected IoT devices and demands ransom payments in cryptocurrency to decrypt the data and restore access for victims. BrickerBot was ransomware that caused permanent denial-of-service on victim IoT devices in 2017 (Bertino & Islam, 2017). The

lack of reliability in many IoT firmware updates poses risks of corruption that can brick devices, disrupt continuity of business operations, and ruin consumer experiences.

- **Data Leakage**

The increasing use of IoT devices in daily life results in vast amounts of personal data generated from homes, vehicles, wearables, and smart city infrastructure. The lack of security makes it easy for attackers to steal private data like health metrics, home activities, location patterns, and business secrets from IoT devices (Roman et al., 2018). Surveillance devices like security cameras can leak sensitive video footage if not properly secured. Attackers often exfiltrate stolen IoT data to botnets and compromised servers under their control. Side-channel attacks infer sensitive data from indirect device emission such as timing, power consumption, and radiation (Sicari et al., 2015).

- **Identity Spoofing**

The identities of IoT devices, networks, and users need to be authenticated to prevent unauthorized access and abuse. However, many IoT devices lack robust authentication mechanisms making spoofing easy (Roman et al., 2018). Identity spoofing attacks pretend to be legitimate IoT endpoints – this allows attackers to bypass access controls, distribute malware, and circumvent trust relationships among entities (Sicari et al., 2015). IoT data provenance can also be spoofed to disguise the origin of untrusted data and conceal attacks. Without hardware roots of trust and platform attestation, attackers can create counterfeit devices with backdoors to infiltrate IoT networks.

- **Permanent Denial of Service**

The constrained nature of IoT devices makes them dependent on automatic firmware updates to patch vulnerabilities and add features. Failed firmware updates can cause devices to crash and become unusable, resulting in permanent denial of service (Bertino & Islam, 2017). The bricking of IoT devices through corrupted firmware has been experienced in smart TVs, cameras, routers, and other appliances when unvalidated updates go wrong. Attackers can also trigger malicious or corrupt firmware updates to brick devices as a denial of service attack.

- **Ransomware Attacks**

Entire IoT networks can be hijacked and held for ransom by exploiting vulnerabilities in common protocols like Zigbee and Bluetooth LE. The ransomworm attack demonstrated in 2017 took control of IoT networks using Philips Hue smart lights to propagate across air-gapped networks (Richardson & Director, 2017). The ransomworm encrypts network traffic and device storage to restrict access until a ransom is paid in cryptocurrency to retrieve decryption keys. Similar wormable ransomware threats remain a critical risk as IoT adoption grows. Attackers may also threaten to brick compromised devices permanently unless extortion demands are met.

3. IoT Security Challenges

There are several unique security challenges in protecting IoT systems and data:

- **Heterogeneity**

The incredible diversity of IoT devices, platforms, networks, and interfaces makes end-to-end security extremely challenging (Sicari et al., 2015). IoT ecosystems comprise a myriad of vendors, devices, protocols, and cloud services with little uniformity. Different verticals like healthcare, energy, and agriculture have adopted IoT idiosyncratically based on distinct requirements and technologies. This heterogeneity greatly complicates threat monitoring, access controls, patching, data protection, and other security processes across fragmented environments, vendors, and data flows.

- **Resource Constraints**

Most IoT devices such as sensors, wearables, and embedded systems have tight resource constraints in terms of computing power, storage, battery life, and connectivity bandwidth (Roman et al., 2018). This restricts the ability to implement strong security controls on IoT endpoints themselves. Encryption taxes device processors and drains batteries faster while running anti-malware also requires significant computing resources. The limited storage makes it hard to log security events and risks devices running out of space for critical data. Weak wireless protocols are used to conserve power at the cost of security protections.

- **Difficult Updates**

The set-and-forget nature of IoT device deployments across remote geographical locations makes performing security updates extremely challenging (Bertino & Islam, 2017). IoT networks comprise dispersed sensors, cameras, and gateway nodes that cannot be easily patched on-site. Vendors struggle to promptly test and deliver security fixes and firmware updates to far-flung devices. This delays remediation and keeps vulnerabilities exposed for longer durations. Lack of updates multiplies exposure to known threats and exploits.

- **Lack of Standards**

The fragmented IoT landscape has led to a lack of widely accepted security standards (Sicari et al., 2015). IoT products and platforms each adopt custom security implementations and protocols tailored to their use case. Different vendors take divergent approaches to authentication, encryption, and access management based on factors like hardware limitations and time-to-market pressures. This lack of standardization poses interoperability issues and gaps in end-to-end security across diverse IoT ecosystems. Vendors often fail to incorporate secure development best practices.

- **User Privacy**

The highly distributed and data-driven nature of consumer IoT networks raises significant privacy risks for users through potential surveillance or unauthorized data access (Roman et al., 2018). IoT

home devices like smart TVs, speakers, and appliances capture extensive personal activities within private spaces and transmit this data over the Internet. IoT wearables reveal sensitive information about health and behaviors. Cars, phones, and transit cards provide extensive location tracking of individuals. Lax data protection poses risks of user profiling, behavioral analysis, and targeted advertising without consent. Side-channels like traffic analysis can infer activities from metadata.

- **Unregulated Devices and Entities**

While traditional information technology systems operate on networks governed by security policies, IoT deployments often expand into uncontrolled environments (Sicari et al., 2015). Enterprise IoT devices get installed and connected to corporate networks without oversight from IT and security teams. This exposes internal systems to rogue devices vulnerable to threats. Moreover, consumers adopt IoT devices from a long tail of vendors with lax security practices or fly-by-night entities difficult to hold accountable. Unvetted devices increase attack surfaces.

- **Human Element**

Despite advanced automation promised by IoT systems, human intervention is still required for oversight and exception handling. Insider threats arise when compromised users abuse legitimate credentials and access to IoT networks, devices, and data (Roman et al., 2018). Employees may install backdoored IoT devices or flout security policies. Social engineering attacks manipulate authorized users into disabling protections and granting system access. Lack of security training and awareness increase such insider risks among employees and consumers.

4. IoT Security Countermeasures

A multi-layered cybersecurity approach is necessary for comprehensive protection of IoT devices, networks, data, and users. The following sections describe technical, legal, and administrative IoT security best practices.

- **Device Hardening**

IoT endpoints are attractive targets for attackers and need to be hardened against threats. Unused services should be disabled to minimize the attack surface – for example, telnet and SSH may not be required on some sensors (Bertino & Islam, 2017). Accounts with default passwords should be changed to prevent access with easily guessable credentials. Firmware should be kept up to date to patch known vulnerabilities.

Enabling built-in encryption capabilities provides confidentiality of data stored on devices and in transit. Code signing verifiable firmware updates ensures integrity against tampering. Jailbreaking policies prevent compromise of safety-critical functions. Enabling Trusted Platform Module (TPM) hardware secures cryptographic operations and storage of keys and credentials. IoT devices should undergo rigorous security testing and validation to identify flaws prior to deployment in production environments (Bertino & Islam, 2017).

- **Network Security**

IoT networks must be designed with strong network security controls. Network segmentation and firewalling limit lateral threat movement from compromising entire ecosystems (Sicari et al., 2015). Gateways and proxies prevent direct Internet access for devices. Intrusion detection systems (IDS) analyze traffic patterns to identify network-based attacks against IoT infrastructure and data flows. Security Information and Event Management (SIEM) solutions can correlate threats across diverse IoT environments.

Network encryption via VPN tunnels or TLS secures communications channels between IoT endpoints and protects data in transit against eavesdropping. Legacy IoT protocols lacking built-in encryption like CoAP and MQTT need additional encryption layers like Datagram Transport Layer Security (DTLS). Mutual authentication using signed digital certificates prevents unauthorized devices and users from accessing IoT networks and data.

- **Access Control & Identity Management**

Role-based access control (RBAC) mechanisms restrict access to IoT devices, networks, and data based on user and device identities and permissions (Roman et al., 2018). User accounts should be limited to least privilege access strictly as per their roles. Multi-factor authentication (MFA) augments basic passwords with additional factors like biometrics, security keys, or one-time codes. The principle of least privilege contains breaches and lateral movement following any account compromise.

Trusted authentication and authorization of machine identities is equally important in IoT ecosystems. Device identity and certificate management solutions provision unique keys and certificates to validate IoT endpoints (Sicari et al., 2015). Federated identity management integrates with existing directory services to provision single sign-on (SSO) access to diverse IoT applications and data across organizational domains.

- **Data Protection**

The sensitive nature of much of the machine and user data generated across consumer and enterprise IoT verticals necessitates strong protection controls for confidentiality and integrity (Roman et al., 2018):

- ❖ - Encryption of IoT data end-to-end using algorithms like AES or ECC protects against data theft and tampering.
- ❖ - Tokenization substitutes sensitive data like device identifiers and user account numbers with randomized values to reduce data exposure.

- ❖ - Data masking hides segments of data like health metrics visible only to certain system roles and users.

- ❖ - Data loss prevention controls prevent unauthorized users from extracting IoT data from networks and databases.

- ❖ - Digital rights management controls data usage policies and access rights for protected IoT data assets.

- **Anomaly Detection**

Machine learning techniques can analyze device behavior and network activity to detect anomalies indicative of threats and exploits (Sicari et al., 2015). Supervised learning classifies events as normal or malicious based on training data. Unsupervised learning spots outliers and anomalies from expected patterns. This provides dynamic detection capabilities adjusting to new attacks IoT devices may face. Big data analytics scales security monitoring across massive, heterogeneous IoT environments.

- **User Awareness & Education**

Lack of cybersecurity awareness among consumers and employees is a weak link across IoT deployments. Users play a critical role in ensuring strong authentication practices, prompt patching, and identifying phishing attacks (Roman et al., 2018). Security education helps improve adherence to corporate IoT and BYOD policies on device usage and data protections. Users need to be made aware of IoT privacy risks and best practices to follow like disabling unnecessary device features, limiting collected data, and keeping systems updated.

- **IoT Security Program & Incident Response Planning**

A comprehensive IoT security program spanning people, processes, and technology is fundamental to managing risks across heterogeneous ecosystems (Sicari et al., 2015). A strong vision and charter to align cross-functional teams enables strategic IoT security planning and preparedness. The program defines unified policies, standards, responsibilities, and compliance metrics governing IoT deployments and data usage. Third-party vendors and service providers need to be evaluated on their security posture and risk exposure.

As IoT footprints grow, ensuring effective incident response capabilities in the event of attacks or data breaches becomes critical (Richardson & Director, 2017). Incident response plans trained through simulations prepare IoT operators to quickly identify and respond to compromises through coordination among internal teams and external agencies. The plans identify processes to isolate compromised nodes, patch vulnerabilities, reset credentials, collect forensic data, and notify impacted customers per breach disclosure laws and contractual obligations.

- **Regulations and Compliance**

Government regulations are beginning to prescribe IoT device security and privacy requirements different industries must comply with:

- ❖ - The Food and Drug Administration (FDA) issued post-market guidance for managing cybersecurity vulnerabilities in medical devices through ongoing patches and risk management (Mueller & Chernich, 2020).

- ❖ - The state of California enacted Senate Bill 327 prohibiting default passwords in IoT devices and mandating reasonable security features to protect user data (State of California, 2016).

- ❖ - The European Union's Radio Equipment Directive and General Data Protection Regulation (GDPR) regulate wireless communications security and personal data privacy across IoT ecosystems (Europa, 2016).

- ❖ - The United Kingdom enacted regulations under the Consumer Protection Act requiring conformance to IoT security design principles protecting user data (GOV.UK, 2018).
- ❖ - The U.S. National Telecommunications and Information Administration (NTIA) released IoT security guidance centered around device transparency, patching, and encryption (NTIA, 2018).

Organizations need to monitor regulations applicable to their IoT solutions and implement necessary controls to avoid penalties or customer lawsuits over non-compliance. Third-party risk management assesses vendors to ensure they adhere to a minimum regulatory baseline.

- **Blockchain for IoT Security**

Blockchain's decentralized ledger and built-in tamper resistance lends itself well to addressing certain IoT security risks like compromised devices, identity spoofing, and data integrity:

- ❖ - Storing hashes of firmware code in the blockchain allows IoT devices to attest their software provenance and boot integrity (Bertino & Islam, 2017).

- ❖ - Device identities and associated metadata can be immutably logged in blockchain transactions to prevent spoofing and trace provenance (Sicari et al., 2015).

- ❖ - Sharing encryption keys over the blockchain enhances secure communication between devices needing to discover and coordinate with peers (Roman et al., 2018).

- ❖ - A blockchain ledger consistently tracks all transactions and changes in IoT data flows to detect tampering or leaks (Sicari et al., 2015).

However, blockchain IoT implementations need to consider challenges like storage limitations, latency, computational overhead, and energy constraints on devices (

5. **Operational Challenges**

Beyond addressing technical security considerations, organizations need to assess challenges in operationalizing and maintaining security across the IoT product lifecycle (Roman et al., 2018):

- - Defining ownership and responsibilities for IoT cyber risks across IT, OT, product teams, and executive leadership.
- - Performing asset management and inventory of all connected devices, data flows, and integrations.
- - Ensuring IoT platforms provide security instrumentation for monitoring, logging, and alerts.
- - Implementing vulnerability management to scan for flaws and patch software dependencies.
- - Providing user access controls, identity management, and gateway protections.
- - Building security into IoT solutions through secure architecture, design principles, and procurement.
- - Training administrators and users on risks and best practices to avoid misconfigurations or unsafe behavior.
- - Conducting red team exercises to probe real-world effectiveness of deployed security measures.

6. **Research Directions**
    - Ongoing research efforts seek to advance IoT security across various problem areas:
    - - Lightweight cryptography optimizes algorithms like ECC and AES for lower power and compute requirements on IoT devices (Bertino & Islam, 2017).
    - - Secure code analysis techniques can help developers identify vulnerabilities in IoT firmware and apps (Roman et al., 2018).

- - Power-efficient intrusion detection explores performing network anomaly detection directly on IoT devices vs. the cloud (Sicari et al., 2015).

- - Secure software updates aim to deliver urgent patches while guaranteeing integrity and preventing bricking (Bertino & Islam, 2017).

- - Privacy-enhancing techniques like federated learning and homomorphic encryption distribute intelligence and computing on-device without exposing sensitive user data (Roman et al., 2018).

- - Embedded hardware security through TPM, secure elements, and trusted execution environments make tampering and extraction of secrets difficult (Sicari et al., 2015).

- - Standardization initiatives define uniform device security and interoperability requirements vendors need to adopt (Bertino & Islam, 2017).

- - Predictive security models based on data science uncover new attack vectors and vulnerabilities in evolving IoT deployments (Sicari et al., 2015).

- - Policy engines tailored to IoT help dynamically configure network enforcement and monitoring as new devices get added (Roman et al., 2018).

7. Conclusion

In summary, this literature review highlighted the diverse range of threats targeting various layers of IoT infrastructure including reconnaissance, network attacks, malware, data theft, identity spoofing, firmware attacks, and ransomware. Key IoT security challenges arise from vast heterogeneity, resource-constrained devices, remote deployments, lack of standards, and privacy risks. A robust IoT cybersecurity program requires adopting device hardening, network security monitoring, access control, data encryption, user awareness programs, and regulations. With massive growth projected in IoT adoption across critical infrastructure and personal spaces, ongoing research and industry collaboration are imperative to promote security, privacy, and public safety.

8. References

1. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... Christodorescu, M. (2017). Understanding the Mirai Botnet. 26th USENIX Security Symposium (USENIX Security 17). https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

2. Bertino, E., & Islam, N. (2017). Botnets and Internet of Things Security. Computer, 50(2), 76–79. https://doi.org/10.1109/MC.2017.62

3. Europa. (2016). Commission implementing regulation laying down standards for the security of radio equipment. Regulation 10(1), 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R0824

4. GOV.UK. (2018). Government to strengthen security of internet-connected products. https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products

5. Mueller, M., & Chernich, G. (2020). FDA's Role in Medical Device Cybersecurity. JAMA, 323(23), 2338. https://doi.org/10.1001/jama.2020.7952

6. Nordrum, A. (2016). Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. IEEE Spectrum: Technology, Engineering, and Science News. https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

7. NTIA. (2018). Communicating IoT Device Security Update Capability to Improve Transparency for Consumers. https://www.ntia.gov/files/ntia/publications/ntia_iotpatch_july2018.pdf

8. Richardson, R., & Director, C. S. (2017). CSIAC IoT ransomware whitepaper. Journal of Cyber Security and Information Systems, 5(2).

9. Roman, R., Zhou, J., & Lopez, J. (2018). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57, 2266–2279.

10. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164.

11. State of California. (2016). SB-327 Information privacy: connected devices. California Legislative Information. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB327