Security Issues in IoT

Challenges and Countermeasures

Internet of Things (IoT)-connected devices have become an integral part of daily life. The IoT is quickly growing as more and more devices are attached to a global network. Many IoT devices' data and applications are highly sensitive and should be accessible only to authorized individuals. These applications are the computer programs that use real-time/near real-time conditions to ensure they do not fail, and they use consumption data to analyze and predict the future with artificial intelligence algorithms.

IoT security should include more than just the IoT device itself. IoT devices have minimal security and many flaws. Many feel that IoT manufacturers are not prioritizing security and privacy. But, despite the security challenges, the spread of IoT is not stopping. Thus, it is a must for security practitioners and users to learn about it to provide more security.

Characteristics

IoT is a collection of devices attached to the Internet that gathers and exchanges data using nodes and controllers. IoT can be defined as a network of uniquely identifiable physical objects or "things" that have the capability to sense and interact with themselves, with their external environment or both. Through controllers and cloud processing, these devices may have the ability to think and act autonomously and gather information for various reasons. The characteristics of many "things" are:

- Fully embedded with or without an operating system (OS) to run
- Collect mostly real-time data
- Use all kinds of networks (local area network [LAN], low-power wide-area network [LPWAN], cellular LPWAN [narrowband IoT and LTE-M], and cellular)
- Have permanent or intermittent connections to the cloud so there is a need to store data with a time stamp
- Measure physical parameters
- Capable of making decisions based on the data collected by these devices, which is necessary to achieve automated decision-making centrally

Opportunities

The goal of IoT is to improve the quality of life and provide benefits to consumers and enterprises. IoT helps to achieve the following:

Gokhan Polat, CISA, CRISC, CCSA, CGAP, CIA CISSP, CRMA
Has experience in risk management, internal auditing and information systems auditing, and now is a senior manager at EY Risk Advisory Services, Turkey. Polat can be reached at gokhan.polat@tr.ey.com or *linkedin.com/in/gokhan-polat/*.

Fadi Sodah, CISA, CISSP, CFR, eJPT, ICATE
Has been involved in networks, open source, infrastructure, software engineering, disaster recovery, security, system administration, audit and systems integration. Sodah can be reached at madunix@gmail.com or *experts-exchange.com/members/madunix*.

- Reduction in energy consumption
- Enhancements in safety and security
- Improvements in automation of everyday tasks
- Enhancements in quality of life

In this context, IoT deployment can be categorized into five types:

1. **Industrial IoT**—Facilitates an improvement in customer service through better customization of products and services to customers in shorter time frames. The establishment of better connectivity and communication between the assembly line and manufacturing, made possible by IoT, enables manufacturers to be closer to market demand and customize what they are building to the needs of their customers (e.g., smart factory)
2. **Commercial IoT**—Includes smart commercial buildings
3. **Healthcare IoT**—Improves patient care. For example, IoT devices connect patients to healthcare systems for continuous medical data monitoring. Patients can share their data with doctors, nurses and family members, and also with machines and algorithms that provide automated feedback from the processed data.
4. **Transportation IoT**—Monitors the status of transporting goods and takes preventive action as needed during transit. For example, IoT devices can track packages end-to-end for temperature, location and potential tampering (location tracking).
5. **Consumer IoT**—Consumer-connected devices including smart TVs, smart speakers, toys, wearables and smart appliances

Building Blocks

IoT systems include hardware and software that communicate with each other using a wide variety of protocols. There are five core building blocks that are fundamental to IoT devices:

1. The hardware components in an IoT device vary depending on the application and usage. Sensors, actuators, accelerometers, gyroscopes and radio-frequency identification (RFID) chips are examples of such components that make devices smart.
2. The software includes platforms and applications that determine what data to collect, what data sources to connect to, which decision-making algorithms to use and the application programming interface (API) to connect with other software components. This also includes firmware that enables applications and APIs to communicate with the hardware components.
3. Data refers to all the components that analyze, process, store and visualize data such as data gathering, analysis and response.
4. Connectivity is taken across the hardware, software and information elements. While the term "Internet of Things" might indicate that everything is connected to the Internet, different types of connectivity and communication protocols are required depending on factors such as device type and proximity.
5. Security is mandatory across all the other elements, including connectivity. It is vital to ensure device-level, network-level, API-level and data-level security because a security vulnerability in any of these elements has the potential to compromise the protection of the entire system.

> "THERE IS A NEED FOR A TRUST FRAMEWORK TO ENABLE USERS OF THE SYSTEM TO HAVE CONFIDENCE THAT THE INFORMATION AND SERVICES ARE BEING EXCHANGED IN A SECURE ENVIRONMENT."

Challenges

There are many challenges facing the implementation of IoT. IoT security is not just device security, as all elements need to be considered, including the device, cloud, mobile application, network interfaces, software, use of encryption, use of the authentication and physical security. The scale of IoT application services is large, covers different domains and involves multiple ownership entities. There is a need for a trust framework to enable users of the system to have confidence that the information and services are being exchanged in a secure environment. The most frequent weaknesses in the data security of IoT applications, as stated in the Open Web Application Security Project (OWASP), are due to:

- Insecure web interface[1]
- Insufficient authentication/authorization[2]
- Insecure network services[3]
- Lack of transport encryption[4]
- Privacy concerns[5]
- Insecure cloud interface[6]
- Insecure mobile interface[7]
- Insufficient security configurability[8]
- Insecure software/firmware[9]
- Poor physical security[10]

> “SECURITY IS NOT JUST AN ADD-ON TO EXISTING SYSTEMS, BUT AN INTEGRAL PART OF THEM.”

IoT application security and end point security are the biggest concerns. Poorly secured IoT devices and applications make IoT a potential target of cyberattacks. Application developers or manufacturers that create IoT products are not mature from a security standpoint. However, security is a critical dimension of every IoT design. Integrating security in IoT impacts both hardware and software design from the beginning. The technologies to secure devices and connectivity are changing very quickly. It is challenging; security is not just an add-on to existing systems, but an integral part of them. The scope of security should be end-to-end to support the device from the very beginning.

Because many IoT devices are small with limited processing, memory, and power capabilities and resources, most current security methods, such as authentication, encryption, access control and auditing, are too complex to run on IoT devices.

IoT devices are being used in urban areas where physical security is difficult to establish or achieve due to the density of structures and complex infrastructure, and this makes it easy for attackers to have direct physical access to the IoT devices. Additionally, denial-of-service (DoS) attacks can weaponize IoT devices and recruit them as part of a massive zombie army. Insecure IoT databases or data stores are also a serious matter to consider.

IoT devices have a long shelf life and may possibly outlive support for the device, and outdated devices might be used in circumstances that make it difficult or impossible to reconfigure or upgrade, thus leaving them vulnerable to cybersecurity threats. Additionally, improper data disposal practices without adequate wiping is a serious concern.

IoT devices have built-in functions such as microphones, cameras and night vision, and are the eyes and the ears of the device. These devices passively collect petabytes of data, sometimes without user knowledge, that can fall into the wrong hands, affecting user privacy. Undisclosed collection, distribution and use of data, and failure to provide clear, comprehensive disclosures regarding data collection, use and sharing, especially when such practices may be unexpected, places the collector in potential violation of various governance and data privacy laws.

IoT products often ship with insecure default credentials. This could include hard-coded passwords that cannot be changed and shared passwords across a family of devices, making it simple for attackers to compromise these devices. Many IoT devices have built-in default usernames and passwords. Malware seeks out IoT devices and generally tries to attack devices by using the default username and password. Once accepted, the malware is able to take over the device to participate in coordinated botnet attacks.

Countermeasures

Generally, multiple layers of administrative, technical and physical controls are used to protect organizational assets against risk. This creates an organized defense that is intense and strong. Commitment and support from senior management are important for successful establishment and continuance of an information security structure. IoT's significant potential requires management's attention.

Manufacturers and vendors must include security in the design process. The most effective strategy for securing IoT is to focus on the fundamentals. IoT device manufacturers, IoT connectivity architects, IoT platform developers, IoT application developers, IoT service developers and IoT experience designers should work together to get this done. It is critical for all those who take part in developing IoT to add security features during the design phase of their IoT solution development. The best efforts to prevent attacks include designing for security, embedding firewall features to add an additional layer of defense, providing encryption capabilities and including tamper detection capabilities. If manufacturers do not thoroughly test their devices, consumer trust and safety may be at risk. It is important to ensure that security is purpose-built into every aspect of the ecosystem that is running a particular IoT product, service or device.[11] When building products for IoT, vendors should always employ good practice and aim for confidentiality, integrity and availability (the CIA triad). The main difference in IoT security compared to traditional IT security is the number of devices, the purpose of usage and the physical condition of the devices. And, perhaps, the main issue is that IoT device manufacturers still do not think of their devices as computers.

Testing can provide assurance that the device and its protocols can cope with the ecosystem of the IoT by developing market-accepted test specifications. This helps introduce the time that it takes to get the product or protocol tested, and this helps to accept devices that can work with other IoT objects. Improving security configurability requires testing IoT web interface management, reviewing the IoT network traffic, analyzing the need of physical ports, and assessing authentication and interaction of devices with the cloud and mobile applications.

Segmenting IoT devices increases network security. So does developing IoT protocols that not only work together, but also ensure security and privacy. Unused services/ports must be shut down and closed, as these networking ports/services can expose the device to additional attack vectors. It is important to deactivate unnecessary services; these may go undetected, allowing an attacker to stealthily use them as a vector or target of an attack. It is also necessary to build in authentication between devices so that only trusted devices can exchange data. A solid password management tool to manage multiple IoT passwords must also be in place.

User awareness training encourages users and consumers to be aware of the vulnerabilities that the device may experience. When selecting an appropriate IoT device, consumers should require that the vendors have defended the device against common attacks.

> “IT IS ESSENTIAL TO CREATE AN ADEQUATE LEGAL FRAMEWORK AND DEVELOP THE UNDERLYING TECHNOLOGY WITH SECURITY AND PRIVACY IN MIND.”

User data need to be processed and encrypted to remain safe. The entire communication channel from the sensors to the service providers must be secure. Some ways to address the huge gap in security include ensuring confidentiality by providing encrypted communication streams, ensuring integrity by providing encrypted data storage and using hash integrity checkers, providing authentication methods so that the devices are communicating with known and trusted entities, and providing security updates in the form of patches and bug fixes.[12]

> “A CAREFUL ASSESSMENT OF SECURITY RISK MUST PRECEDE ANY IOT IMPLEMENTATION TO ENSURE THAT ALL THE RELEVANT, UNDERLYING PROBLEMS ARE DISCOVERED.”

Regulations will force manufacturers and vendors to make security a priority and provide guidelines on the expectation from IoT developers and manufacturers. IoT regulations will give a level of transparency to consumers, or packaging can reflect the level of security of the IoT device. It is essential to create an adequate legal framework and develop the underlying technology with security and privacy in mind. Regulation will force manufacturers to upgrade and secure their products. IoT applications need to have some consideration for the EU General Data Protection Regulation (GDPR).[13] The GDPR introduced a general mandatory notification regime in the event of personal data breaches. Data controllers are required to report personal data breaches to their supervisory authorities no later than 72 hours after becoming aware of such a breach and, in some cases, are also required to report such breaches to affected individuals. Data controllers using the IoT need to ensure that they are in a position to identify and react to security breaches in a manner that complies with the requirements of the GDPR.[14]

Regular firmware updates and maintenance help protect the ecosystem and the ability of the IoT to handle virtually all functional operations. It should be possible to get updates of the firmware, the OS, or the specialized logic on stationary and mobile IoT devices. This requires maintenance interfaces to access the application runtime environment and the security settings for the apps themselves.

It is important to have monitoring systems in place when an event occurs. Once the event has been detected, a responsive action must be triggered to prevent any malicious use of the device. A back-end application should have functionality in place that can log abnormalities in the data it is receiving. Monitoring and software maintenance are essential to minimizing the impact of any device downtime due to software bugs or any other potential problems.

Guidelines

Practitioners should conduct a risk assessment in the IoT stack for all types of attacks in device security (endpoint security), network or connectivity layer security, cloud infrastructure security, and application security. An effective IoT framework should provide guidelines on managing IoT risk faced by organizations. Those guidelines include:[15]

- Enable security and control by design from the start.
- Build security into the IoT software development life cycle.
- Enable IoT hardening, access management, log management and patch management.
- Enable audit controls related to data collection, privacy, storage, sharing, handling and disposal.
- Enable controls on network protocols related to remote access, session management and access management.
- Test controls and look for vulnerabilities by creating and testing use cases and misuse cases.
- Exercise program effectiveness of monitoring controls on IoT.
- Build a watchdog protocol to continuously monitor connectivity and to detect connection loss and optimize resources. The activities of IoT products will be tracked by the watchdog, and this makes it easy to handle the events immediately.

- Emphasize the criticality of security along with functionality.
- Build and enhance the skills of IT security and assurance personnel to span cybersecurity and IoT risk and benefits.
- Align the IT function and business IoT usage.
- Plan system acquisition, development and maintenance of IoT services.
- Regulate trust between IoT devices.
- Maintain asset inventory, management and disposal of IoT devices.
- Exercise governance over IoT initiatives.
- Design devices with security in mind.
- Build in malware protection in IoT applications.
- Audit the IoT environment, e.g., security audit and code reviews.
- Define data flows in the IoT environment.
- Build a vulnerability management program. Include vulnerability assessments and penetration testing.
- Develop IoT threat modeling.
- Establish governance and accountability.

Conclusion

Applying IoT technology yields both opportunities and security risk, so the challenges with IoT devices in relation to security are huge. A careful assessment of security risk must precede any IoT implementation to ensure that all the relevant, underlying problems are discovered. Without sufficient data security and data protection, IoT will not be successful in the long run. Therefore, every IoT manufacturer is challenged to complement all phases of development processes through to the operation of the equipment with appropriate security measures. In future work, it is important to develop a framework for realizing and evaluating security risk within IoT to ensure confidentiality, integrity and availability.

Endnotes

[1] Open Web Application Security Project, "Top 10 2014-I1 Insecure Web Interface," *https://www.owasp.org/index.php/Top_10_2014-I1_Insecure_Web_Interface*

[2] Open Web Application Security Project, "Top 10 2014-I2 Insufficient Authentication/Authorization," *https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization*

[3] Open Web Application Security Project, "Top 10 2014-I3 Insecure Network Services," *https://www.owasp.org/index.php/Top_10_2014-I3_Insecure_Network_Services*

[4] Open Web Application Security Project, "Top 10 2014-I4 Lack of Transport Encryption," *https://www.owasp.org/index.php/Top_10_2014-I4_Lack_of_Transport_Encryption*

[5] Open Web Application Security Project, "Top 10 2014-I5 Privacy Concerns," *https://www.owasp.org/index.php/Top_10_2014-I5_Privacy_Concerns*

[6] Open Web Application Security Project, "Top 10 2014-I6 Insecure Cloud Interface," *https://www.owasp.org/index.php/Top_10_2014-I6_Insecure_Cloud_Interface*

[7] Open Web Application Security Project, "Top 10 2014-I7 Insecure Mobile Interface," *https://www.owasp.org/index.php/Top_10_2014-I7_Insecure_Mobile_Interface*

[8] Open Web Application Security Project, "Top 10 2014-I8 Insufficient Security Configurability," *https://www.owasp.org/index.php/Top_10_2014-I8_Insufficient_Security_Configurability*

[9] Open Web Application Security Project, "Top 10 2014-I9 Insecure Software/Firmware," *https://www.owasp.org/index.php/Top_10_2014-I9_Insecure_Software/Firmware*

[10] Open Web Application Security Project, "Top 10 2014-I10 Poor Physical Security," *https://www.owasp.org/index.php/Top_10_2014-I10_Poor_Physical_Security*

[11] White Hat Security, "IoT Security—Combining Innovation With Protection," *https://www.whitehatsec.com/trending/content/iot-security-combining-innovation-protection*

12 Bock, L.; "The Internet of Things Operate on a Cowboy Code—There Are No Rules," LinkedIn, 18 June 2017, *https://www.linkedin.com/pulse/security-privacy-iot-lisa-bock/*

13 Chapin, M., *et al*; *Implication of the General Data Protection Regulation*, March 2018, *https://www.aacrao.org/docs/default-source/signature-initiative-docs/gdpr/gdpr_discussiondraft_03272018_v2.pdf?sfvrsn=4556dd66_0*

14 Bird & Bird, "Personal Data Breaches and Notification," *https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/42--guide-to-the-gdpr--personal-data-breaches-and-notification.pdf?la=en*

15 *Internet of Things (IoT) Security Guidelines*, *https://static1.squarespace.com/static/5516199be4b05ede7c57f94f/t/56b153eb86db439f9f8d181f/1454461935011/Internet_of_Things_Security_Guidelines.pdf*