Security and Privacy Challenges of IoT-enabled Solutions

Sivarama Subramanian, CISM, is lead security tester for Center of Excellence (CoE) at Cognizant Technology Solutions, where he is leading security testing research, enabling new service rollouts and aligning new security trends to customer needs. He can be reached at *sivaramasubramanian.kailasam@cognizant.com.*

Varadarajan Vellore Gopal, CEH, is a security researcher and security testing manager at Cognizant Technology Solutions, where he manages a security testing program for a banking and financial company. He can be reached at *varadarajan.velloregopal@cognizant.com.*

Marimuthu Muthusamy is chief architect at Cognizant Technology Solutions. He can be reached at *marimuthu.muthusamy@cognizant.com.*

The Internet of Things (IoT) is captivating organizations because of its potential to rapidly transform businesses and people's lives. It is widely believed that IoT will precipitate a major shift in people's lives similar to how the Internet transformed the way people communicate and share information.

IoT comprises devices and sensors interacting and communicating with other machines, objects and environments. Gartner has predicted that there will be 26 billion devices connected to each other by 2020.[1, 2] There are still other predictions that put this number at 50 billion devices by 2020.[3] As a result of this exploding growth in interaction between devices and systems, huge volumes of data are expected to be generated and moved across information processing systems. These raw data will be processed and analyzed to generate meaningful information and to perform actionable decision making.

IOT APPLICATION DOMAINS

In its current form, IoT is expected to transform every business domain, including manufacturing and logistics (ManLog), health care, banking and financial services, life sciences, retail and industrial, and home automation. Usage cases for IoT in some of the domains[4] include the following:

- **ManLog:**
  - Machine-to-machine communication
  - Machine-to-infrastructure communication
  - Asset tracking of goods on the move
- **Health care and life sciences:**
  - Remote monitoring of patient health
  - Diagnosis and drug delivery
- **Industrial and home automation:**
  - Smart city, smart homes and automation
  - Industrial building automation
  - Appliance monitoring, such as washing machines, air conditioners and refrigerators
  - Livestock farming—tagging and devices to monitor activities
- **Retail:**
  - Replacement of bar coding and radio frequency identification (RFID) with devices that feed more data to monitoring systems, thereby improving supply chain efficiency
  - Easier product learnability and discoverability through product and smart phone communication

The diversity of services being planned using IoT means no one company can develop a full end-to-end solution and support IoT-based innovations. Of all the business domains, retail would be the first sector to see numerous IoT adoptions. This is evident as Walmart has already implemented IoT in its supply chain management.[5]

GENERIC TOPOLOGY OF IOT

IoT architecture can be typically represented by four interconnected systems, or entities, as shown in **figure 1.**

Certain organizations might do away with a cloud infrastructure for their local server.

Things or Devices

"Things" are anything that is currently interconnected in an industrial, home or business setting and has the capability to gather current state/information and act on it or send it to other systems for further analysis. All these things, or devices, are attached with sensors that help gather current state/information. There are effectively three classes of devices based on the capability and processing power:

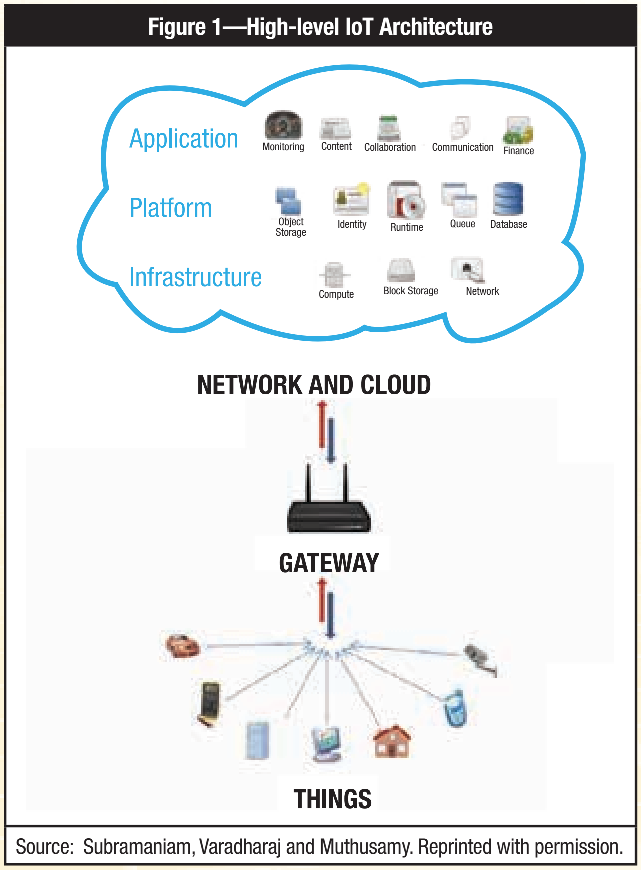
- The smallest devices have 8-bit system-on-a-chip (SoC) controllers (e.g., Arduino boards).
- The next level of devices is based on Atheros or ARM chips with 32-bit architecture. These run a cut-down or embedded Linux platform such as OpenWRT.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and choose the Comments tab to share your thoughts.

Go directly to the article:

Figure 1—High-level IoT Architecture



Source: Subramaniam, Varadharaj and Muthusamy. Reprinted with permission.

- The most capable are 32-bit or 64-bit platforms, such as Raspberry Pi or BeagleBone. These devices may run a full Linux OS or other OS such as Android. In many cases, these are either mobile phones or based on mobile phone technology.

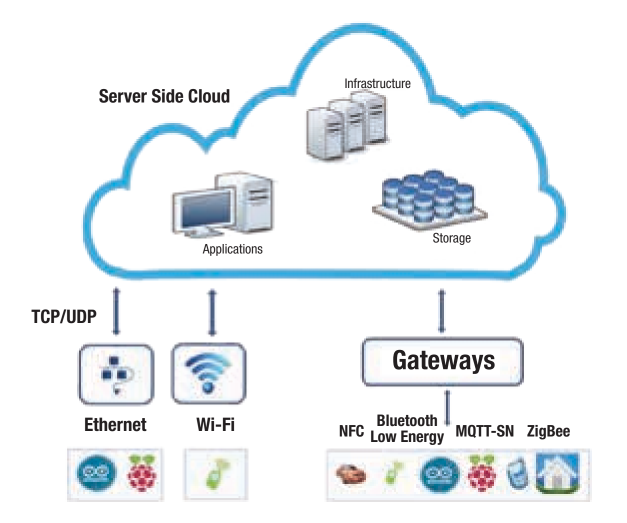
There are multiple technologies/protocols that the devices are connected to in the external world. Some of the most widely used include:

- Direct Ethernet or Wi-Fi connectivity
- Bluetooth low energy
- Near field communication
- Zigbee

Gateways

Gateways are intermediate systems that connect IoT devices through the Internet and provide much-needed support functions such as manageability and security. Gateways are needed in situations in which devices cannot directly connect to existing systems on the Internet. From an IoT standpoint, 85 percent of existing devices/things that are in use were not designed to connect to the Internet and gateways are the key to connecting these existing things to the IoT domain.[6] **Figure 2** shows various network protocols that would be used in the IoT environment.

Figure 2—IoT Network Interfaces



Source: Subramaniam, Varadharaj and Muthusamy. Reprinted with permission.

Network and Cloud Infrastructure

A network is nothing but the current Internet with connected Internet Protocol (IP) systems, such as routers, repeaters and gateways, which control data flow and connect to telecom and cable networks such as 3G, 4G and LTE.

Cloud infrastructure provides the necessary means in terms of hardware capacity and processing power required for processing the enormous amounts of data expected to be generated from IoT.

Service Creation Layer

This layer is comprised of middleware components (e.g., Service Bus; extract, transform, load [ETL]; applications; web servers) that perform the act of data massaging and presenting it for consumption through various channels such as desktop, browser and mobile applications (apps).

SECURITY AND PRIVACY CONCERNS/CHALLENGES

IoT promises to provide unprecedented and ubiquitous access to the devices that make up everything from assembly lines, health and wellness devices, and transportation systems to weather sensors. Unfettered access to that much data poses major security and privacy challenges, including:

- **Insufficient authentication/authorization—**A huge number of users and devices rely on weak and simple passwords and authorizations. Many devices accept passwords such as "1234."
- **Lack of transport encryption**—Most devices fail to encrypt data that are being transferred, even when the devices are using the Internet.
- **Insecure web/mobile interface**—Most IoT-based solutions have a web/mobile interface for device management or for consumption of aggregated data. This web interface is found to be prone to the Open Web Application Security Project (OWASP) Top 10 vulnerabilities, such as poor session management, weak default credentials and cross-site scripting vulnerabilities.
- **Default credentials**—Most devices and sensors are configured to use the default username/passwords.
- **Lack of secure code practices**—Services and business logic would be developed without adhering to secure coding practices.
- **Privacy concerns**—Devices used in the health care domain collect at least one piece of personal information; the vast majority of devices collect details such as username and date of birth. However, the fact that many devices transmit information across networks without encryption poses even more privacy risk. Privacy risk arises as the objects within the IoT collect and aggregate fragments of data that relate to their service. For example, the regular purchase of different food types may divulge the religion or health information of the buyer. This is one aspect of the privacy challenges with respect to IoT.

MITIGATING SECURITY AND PRIVACY CHALLENGES

IoT products are made secure only when security is embedded in the production life cycle. Each building block of IoT solutions should also undergo a security review to detect vulnerabilities.

Countermeasures, such as the following, can be taken to address the security challenges:

- **Base device platform analysis**—Weak platform configuration might lead to compromises such as privilege escalation.[7] A base device platform operating system and its security properties, configurations and features should be verified against the base-lined information security requirements. Verification needs to be done to ensure that any test interfaces are removed from the hardware.
- **Network traffic verification**—Network traffic (wired or wireless) should be analyzed for any interceptable, unencrypted or modifiable data.[8] There is a compromise between performance and security when encryption is recommended. Lightweight encryption algorithms can be used to cater to performance requirements.
- **Verification of functional security requirements**—High-level functional security requirements should be validated. They should also be subjected to negative testing (subversion or fuzzing).[9] IoT solutions can use Software as a Service (SaaS)-based identity management solutions for authorization and authentication requirements.
- **Trust boundary review and fault injection**—All trust boundaries across the signal path should be reviewed and subject to fault injection using negative test cases.[10] The trust boundaries can be verified using manual penetration techniques. Periodic penetration testing is recommended.
- **Side channel attack defense verification**—If side channel defenses are implemented, either in software or hardware, they should be verified using continuous penetration testing activities. Continuous penetration testing helps to minimize advanced persistent threats (APTs) for IoT solutions.
- **Secure code reviews**—Early secure code reviews lead to early mitigation techniques. Sensitive and security impact areas such as boot process, security enforcement and encryption modules should go through secure code reviews. The cost of fixing a security defect is greatly reduced when the security vulnerability is discovered during the development cycle.
- **End-to-end penetration test**—End-to-end penetration tests should be conducted across the signal path to identify any vulnerabilities in the web interface, mobile interface and cloud interface of the IoT solutions. The penetration testing would give the security posture of the IoT solution for each of its components.

Figure 3—STRIDE Approach to Identifying and Mitigating Attacks

Components	Attack Scenarios	Mitigation
Gateway	Interception of and tampering with communication	• Implement Secure Sockets Layer (SSL) transport layer security.
Services	DoS, sending large amounts of data based on spoofed identifier	• Implement SSL transport layer security. • Implement server monitoring for high traffic from a particular user.
Web interface	Structured Query Language (SQL) injection attack on MySql databases leading to data theft and database downtime	• Use parameterized SQL statement. • Sanitize user inputs for SQL injection.
Web app to third-party apps communication	Interception of and tampering with communication	• Implement SSL transport layer security.
Data stores	Weak database credentials that can pose privacy challenges	• Collect only the required data. • Implement strong database access controls per information security standards.

Source: Subramaniam, Varadharaj and Muthusamy. Reprinted with permission.

SECURITY ASSESSMENT OF AN IOT SOLUTION

A US-based software company developed a SecureTravel product using IoT technology. The product provides real-time data about the speed of vehicles, location of the vehicles and people traveling on the vehicles.

The technology components involved included:

- Sensors in the vehicles
- Gateways
- Services
- Web interface
- Mobile interface

Threat modeling using the Spoofing, Tampering, Repudiation, Information disclosure, Denial of service (DoS), Elevation of privilege (STRIDE) software approach was conducted to identify the attack scenarios and formulate mitigation plans for each of the components (**figure 3**).

CONCLUSION

Introducing security in the early life cycle of the IoT solution can make mitigation design much easier. Security and privacy challenges for any IoT solution can be addressed by following secure systems development life cycle (SDLC) practices, secure coding practices and periodic penetration testing activities.

ENDNOTES

[1] Gartner, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units by 2020," Newsroom, 12 December 2013, *www.gartner.com/newsroom/id/2636073*

[2] Gartner, "Gartner Says the Internet of Things Will Transform the Data Center," Newsroom, 19 March 2014, *www.gartner.com/newsroom/id/2684616*

[3] Cisco, "The Internet of Things," Cisco Visualizations, 2014, *http://share.cisco.com/internet-of-things.html*

[4] Freescale, *What the Internet of Things (IoT) Needs to Become a Reality*, white paper, May 2014, *www.freescale.com/files/32bit/doc/white_paper/INTOTHNGSWP.pdf*

[5] Hardgrave, Bill; "RFID Adoption Is on Target," *RFID Journal*, 5 January 2015, *www.rfidjournal.com/articales/view?12575*

[6] Intel, *Developing Solutions for Internet of Things*, white paper, 2014, *www.intel.in/content/dam/www/public/us/en/documents/white-papers/developing-solutions-for-iot.pdf*

[7] NCC Group, *Security of Things: An Implementer's Guide to Cyber-Security for Internet of Things Devices and Beyond*, 2014, *https://www.nccgroup.com/en/learning-and-research-centre/white-papers/security-of-things-an-implementers-guide-to-cyber-security-for-internet-of-things-devices-and-beyond/*

[8] *Ibid.*

[9] *Ibid.*

[10] *Ibid.*