2020 15th International Conference on Computer Engineering and Systems (ICCES) | 978-0-7381-0559-8/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICCES51560.2020.9334589

Security Framework for Internet of Things (IoT)

Sherif El-Gendy
School of Information Technology and Computer Science
Nile University
Cairo, Egypt
s.elgendy@nu.edu.eg

Marianne. A. Azer
National Telecommunication Institute
Nile University
Cairo, Egypt
mazer@nu.edu.eg

***Abstract*—The Internet of things technology provides people with new experiences through the interaction between devices, people and networks. Examples include smart grid, smart health, smart home, smart workplace, e-commerce, smart industrial management, and e-governance. More and more devices are connected every day, resulting in greater security threats and problems. An extensive IoT security model is needed in order to aid resource-based IoT devices and end security. In this paper, we focus on the IoT devices applications and networks, in addition to the attack vectors and security requirements for IoT systems, as well as the organizational approach towards IoT security. We also propose a security architecture to provide security enabled IoT services, and provide a baseline for security deployment.**

Keywords—Applications, Attacks, IoT; Security; Smart services

I. Introduction

The Internet of Things (IoT) allows objects in our world to be linked over the Internet with the ability to interconnect without human interference. The IoT comprises a variety of artifacts that can be linked through wireless or wired networks. These objects have a special addressing scheme that allows them to communicate and collaborate with each other to create new applications and services, such as smart houses, smart transportation, connected vehicles, smart grids, smart cities, smart traffic control and others [1]. IoT safety is considered as one of the major considerations for avoiding physical damage or undesirable threats to the IoT and its elements and for protecting the surrounding environment from damage. In order to develop new design architectures that provide a secure and reliable system environment, the building of the IoT framework with integrated protection and reliability features should be considered [2].

Terrorists can damage furnaces and facilities of power generation. Individual identities and related data may be stolen. Therefore, IoT security should be an essential concern. IoT infrastructure differs from one another, because IoT systems contain resource-restricted equipment. Such systems may not be compliant with conventional protection techniques. For resource-constrained devices, specialized resource-efficient security techniques and architectures are needed. The lack of backup security is another major problem in the IoT network.

IoT devices Security issues should be discussed from the manufacturing to IoT technology implementation Three components need to be addressed as IoT security concerns; Networks, applications and IoT devices. For instance, because of incorrect configuration or vulnerabilities, IoT devices may be compromised. Security challenges need to be addressed strategically to find effective solutions. Security in the IoT system should be built in. IoT devices are made unfortunately without focus on security concerns [3].

Further deficiencies in security could be due to inadequate IoT system configuration and management. Thus, until the device has been replaced, IoT requires articulated configuration and management. In addition, IoT vendors should focus on security before their product becomes available. Potential IoT system risks may also be related to physical attacks. Attackers may attack IoT devices if connected to the Local or home network; an attacker may be able to access encrypted IoT data; or change the IoT security credentials. The intruder may be able to attack the IoT framework with malicious software mounted on a IoT device connected to a local or home networks.

In this paper, we provide an overview of major IoT security issues, discuss IoT system attack vectors; IoT system security requirements; IoT system literature security techniques; the organizational cyber-security approach. We propose an IoT security architecture.

The remainder of this paper is organized as follows. Sections II and III presents the related works, and IoT security respectively. Section IV focuses on the IOT Security Organizational Approach, while section V presents the proposed IOT security architecture. Finally, conclusions and future work are presented in section VI.

II. Related Work

There were various suggestions for IoT security in the literature.

The authors in [4] proposed the hardware-based security technique. To achieve protection at hardware level, a cryptographic processor was suggested. For their approach, the methodology of elliptical curve cryptography was adopted. The authors in [3] suggested a software-based approach. Their work serves as a defense strategy against cryptographic device security attacks that encrypt or generate cipher text. A new data integrity verification scheme was proposed in [5]. The third-party auditor used Merkel hash tree. The solution aimed to check the validity of the data stored.

The IoT network does not prevent attackers that can target from inside or outside the network. The introduction of a signature based and anomaly intrusion detection solutions can use a security mechanism to prevent any intrusion in the network. Signatures of attacks are essential to determine any network misconduct. This is in addition to tests

978-0-7381-0559-8/20/$31.00 ©2020 IEEE

for regular network activity conduct and alerts when the network deviates from its normal behavior. Both methods have advantages and disadvantages. The authors in [6] later suggested a mixed approach, in which both anomaly and signature-based approaches are extended to the proposed system.

The fingerprints suggested in [7] can be used to identify devices such as base stations or access points. To get uniquely identifiable signatures from the wireless signals can do this. The authors in [8] suggested IoT RFID authentication protocols. Such protocols may be Hash Chain, Hash Lock and Interactive Authentication Protocols. However, these protocols consume resources and jeopardize IoT system performance.

The authors in [9] recommended a framework to protect against IoT attacks. They introduced a model to make an IoT system robust taking into consideration resource constraints to implement security for low restriction devices such as gateways or other IoT devices. Fingerprinting for low constraint devices can be beneficial. It utilizes unique features of IoT devices for identification purposes, for example signal strength, frequency and capacity.

III. IoT Security

In this section, we discuss the security requirements, security concerns, as well as the different attacks against IoT. They are presented in sections A, B, and C respectively.

A. *Security Requirements*

The security requirements for the IoT system have some challenges as follows:

- IoT consists of heterogeneous technologies that make security requirements more difficult to determine and understand.
- IoT can have mobile devices that require versatility, which raises security risks.
- IoT also produces a large number of information called Big data. Big data has its own security issues and management.

An IoT system requires users and devices to be authenticated, authorized, and access controlled. The identity of users or devices is verified in an IoT system through authentication. Authorization gives the designated body the required rights, and access control limits access to IoT system data or resources in order to protect against unintended use, and keep data confidentiality, data is encrypted either in store or in transit form. Data integrity ensures data consistency and accuracy, is and that non-repudiation ensures data origin and integrity. Exploiting any vulnerability indirectly leads to violate one or more of the given attributes while security provides the immunity against the violation of above attributes. Security attributes and requirement description are summarized in Table 1.

TABLE I. IoT Security Attributes, Techniques and Requirements

Attribute	Techniques	Requirement Description
Confidentiality	Encryption	Data protection is required, no one should be able to read it except authorized entity.
Integrity	Hash generation	It should be verified that no one has altered the data.
Authentication, Authorization, Access control (AAA)	Implement policies, Security credentials, firewall, and Authentication servers. Digital signature etc.	• Identification of users and devices. • Special permissions or privileges for authenticated user. • Access should be limited to the resources and data.
Non Rrepudiation	Digital signature	Originator of data should not be able to deny its origin.

B. *Security Concerns*

Open Web Application Security Project (OWASP) has listed some of the security concerns in IoT as follows [11].

- Weak authentication or authorization.
- Weak security on network services.
- Weak security configuration.
- Lack of encryption in transportation.
- Weak security on cloud interface.
- Weak security on mobile interface.
- Weak Firmware security.
- Weak physical security.

Some IoT device providers do not securely update the firmware to encrypt and digitally sign the update. Sometimes the mutual authentication between client device and server is not carried out. Authentication can therefore be compromised. Web applications also have significant vulnerabilities with connections to the database network to exploit for gaining access to the backend system. Most cloud interfaces allow weak credentials such as the "12345" password to be set. This is easily guessable by use brute force attack. Most of the cloud interfaces do not endorse a multi-factor or two factor authentication that highly verifies a stated person. Some IoT devices do not apply strong passwords and can easily be hacked. Some IoT services do not implement security measures against account harvesting and some do not take into account delayed authentication processes support brute force attacks.

Most smart applications that control IoT devices such as smart mobile application does not use secure cloud connections. To communicate securely with the cloud, the control application should use the Secure Socket Layer (SSL) protocol. Physical safety is another attack vector, that spans from physical devices and wired to the wireless connection. Physical devices can be physically secured by not allow unauthorized connection, but full security to the wireless medium is quite impossible as radio waves travel in open air.

Only by limiting their range in open air can wireless media be secured. Some techniques secure the radio waves, but they require greater computer power. Therefore, these vectors become the vulnerabilities for the attacker to exploit and gain control over system, data, even in network and cloud. Such vectors can be extremely discussed and controlled by the respective entities.

C. *Types of Attacks*

In this section, we present different and common types of attacks against IoT systems. They are presented in Table 2.

TABLE II. DIFFERENT TYPES OF ATTACKS AGAINST IOT

Type of Attack	**Attack Description**	**Examples**	**Advantages from an attackers' perspective**
Physical Attacks [12]	Aim to tamper with the hardware components. They are fairly difficult to carry out because they require expensive resources.	• De-Packaging of Chip • Layout Reconstruction • Micro-Probing • Particle beam	Can help attackers to have full and effective control of devices.
Side Channel Attacks [13]	Are focused on random deviations which allow the correlation between the challenges and their responses, and can be retrieved from the encryption devices (that is neither the plaintext to be encrypted nor the cipher text results from the encryption process). Encryption devices can generate easily measurable timing information and energy consumption statistics etc.	• Timing Attacks • Power Analysis • Fault Analysis • Electromagnetic • Environmental	Help hackers to retrieve the key used by a device. They are based on the fact that the physical characteristics of logical operations depend on the input data.
Cryptanalysis Attacks [14]	Are focused on the cipher text and they try to break the encryption	• Cipher Text-Only • Known Plaintext • Chosen Plaintext • Man-In-The-Middle	Help hackers to find the encryption key to be able to obtain the plaintext
Software Attacks [15]	Exploit different implementation vulnerabilities in the system through its own communication interface.	• Exploit Buffer Overflows • Trojan Horses • Worms And/ or Viruses to Deliberately Inject Malicious Code into the System	Help hackers to exploit different software vulnerabilities to gain unauthorized access or steal sensitive information
Wireless Network Attacks [16]	Wireless communication systems are vulnerable to network security attacks due to the broadcast nature of the transmission medium. These attacks are classified as active and passive attacks.	• Denial of Service • Node Subversion • Node Malfunction • Node Capture • Node Outage • Message Corruption • False Node • Routing Attacks	Help attackers to intercept data transmission and sniff sensitive data

IV. IoT SECURITY ORGANIZATIONAL APPROACH

Organizations involved in adoption of IoT technologies must consider IoT privacy and security risks. In order to meet their customers and company security requirements, organizations must consider security measures to their solutions. To address the security of IoT, we suggest the following measures:

A. *Measure Security Impact:*

The security impacts on consumers and business must be measured by the organization. What is the loss for both customers and businesses? Who is going to be responsible for security? How will the IoT system be secured? And what is the security solution's impact?

B. *Multi-layerl security approach:*

Security approaches should cover all possible aspects or security attributes such as authentication, access control, encryption mechanisms, analysis techniques, network security.

C. *Control life cycle:*

Defines the security control from its deployment to become operational and incident occurrence to neutralization and expiration and replacement of IoT objects. Control cycle consists on the following phases as shown in Figure 1.

- Implementation phase: Deploys the security in IoT systems such as identification of any object.
- Operational phase: Security becomes operational by continuously monitoring and maintaining updates and fixes in the process of "monitoring of known objects.".
- Incident and reverse phase: If any unwanted security breach occurs despite of countermeasure, upshot is neutralized and restoration to normal state should be done.
- Expiration phase: Exits the system and replaces devices and then gets back to the first phase.

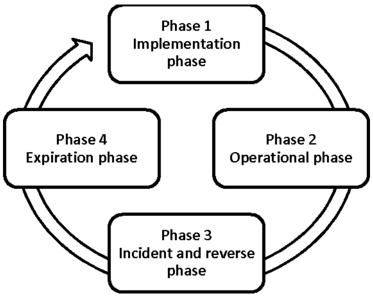

Fig. 1. Control Life Cycle

D. Preservative approach:

Manufacturers should consider securing IoT devices. For instance; IoT gateways should be available with built in security. This function reduces the organization's security overhead. Increased understanding of IoT security in different markets can be achieved through partnership with security vendors and researchers.

V. PROPOSED IOT SECURITY ARCHITECTURE

In this section, we propose an IoT security architecture that takes into account security requirements and the IoT attack sources mentioned earlier. To deploy security, the IoT system can be divided into three parts: Physical, network, and application.

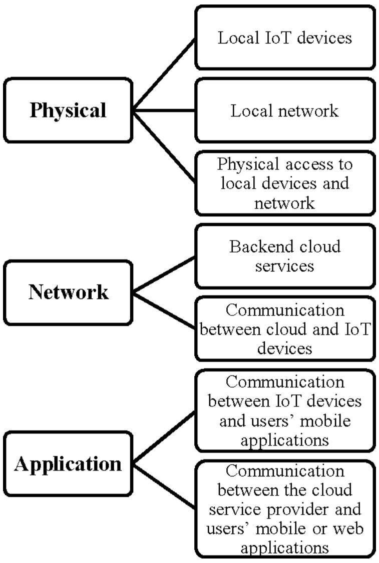
Physical
Local IoT devices
Local network
Physical access to local devices and network
Network
Backend cloud services
Communication between cloud and IoT devices
Application
Communication between IoT devices and users' mobile applications
Communication between the cloud service provider and users' mobile or web applications

Fig. 2. IOT system components

A. Physical Security

IoT systems consist of IoT devices connected through a network. Many local devices are available in markets depending on the usage such as security alarms, smart thermostats, smart locks, smart IP cameras, smart energy management devices, smart electricity meters, smart home appliances, smart health sensors, voice detectors and many more. These devices are connected to the backend servers or cloud service providers; data from these smart devices is collected and stored over the cloud. Therefore, users can access these devices directly or through the cloud.

Devices can be categorized into two types one that uses existing networking technologies like TV boxes using Wi- Fi or Ethernet connections. Second category includes sensor devices that use wireless technologies for local communication like ZigBee, Bluetooth, Z-Wave, Powerline and many other radio frequency protocols.

The highest level of attacks is when the attacker has physical access in the local network. The attacker will be then able to cut off the cables, system setup can be misconfigured and security parameters can also be modified, and then it will be remotely accessible. A physical attacker can also read the memory and access the firmware in order to understand the device's operations and vulnerabilities. The cryptographic information will also be accessible for the attacker. Physical attackers may be able to either install or update new firmware because most devices do not have signed firmware or devices digitally and can update them offline.

An intruder may also target Wi-Fi or the Ethernet interface, while the system updates the cloud service status or gets firmware upgrade from the remote server. The attackers may intercept the communication with ARP-poisoning or changing DNS settings in order to redirecting the traffic. Self-signed certificates also help attackers with HTTPS communication interception, since most devices do not have a verification mechanism. Local network devices can be scanned if the attacker has physical access via universal Plug-and-Play (P&P) or discovery protocol.

Mitigation may be done, by securing the devices from being physically accessed via locked racks. This is in addition to using wired connections instead of wireless connection, disabling unnecessary device functionalities, changing default passwords, using strong device passwords, limiting remote access when needed, installing updates whenever available. Also exploring security measures on device by vendor before buying it. If possible, purchasing devices with self-healing mechanism. Such precautions can help to protect an IoT system's physical part. There may be many more problems and possible solutions, but there must be a preparation for unknown attack vectors.

B. Network Security

The second part of proposed architecture is the network security. It consists of different cloud service and Cloud-IoT Communication. Because IoT devices communicate directly with the cloud, the cloud itself should be properly protected. Communication between IoT devices and cloud should therefore be secured and authentic. When communicating with cloud service, proper device authentication is required. When devices and cloud use a weak form of authentication, the device identity could be used by a third party. Without a strong encryption process in place, the intruder will be able to obtain access to sensitive data during communication with the cloud. There should be a protection against man in the middle attack that can also intercept the IoT traffic. There should also be a protection against playback attack, which can cause an unauthorized action against cloud services or device. These problems can be mitigated by using strong authentication mechanism with cloud to protect against misidentification of device. Strong encryption can protect data from unauthorized access during the communication. TLS with certificate validation mechanism for authentication and secure key distribution is also recommended.

C. Application Security

The third part is the application that includes communication between users' applications and IoT devices as well as mobile or web application with cloud.

Wi-Fi and Bluetooth connectivity are used for communication between mobile apps and devices. Data should therefore be encrypted; otherwise local traffic will be revealed during communication. Mobile applications should be carried out the use of TLS / SSL and validate TLS certificates which in turn will secure the communications against the Man in The Middle attack (MITM). TLS / SSL should be used to ensure secure connectivity between smartphones and web applications with the cloud services, otherwise attackers will passively capture the data. Numerous cloud service providers do not restrict users against creating weak, unsafe passwords, while the usage of strong passwords increases the efforts of hackers using different types of attacks such as brute force or dictionary attacks. Server's TLS certificate validation should be properly carried out by the applications. Therefore, these best practices can contribute to secure the communications. Figure 3 represents the proposed IoT security architecture.

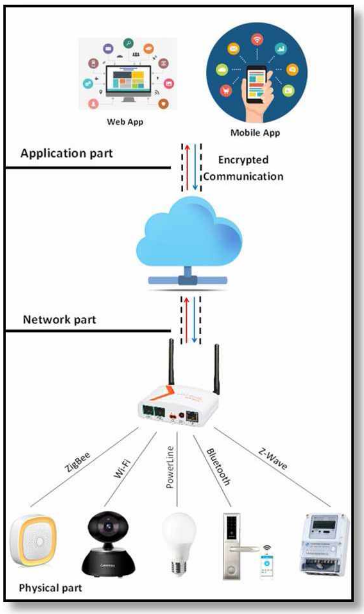

Fig. 3. Security architecture for IoT system.

It does not matter how much the IoT system has been secured, some threats can absolutely defeat these security measurements. The analysis of IoT security can provide good understanding for network operations. Another aspect in IoT security is that most IoT devices come in such conditions that no one can add security features. Therefore, security should come with IoT device as a built-in feature. IoT devices should be secured by design with traditional security techniques like encryption, authentication, integrity check and secure updating. IoT devices should also execute secured signed code authorized to run on devices, while being secured during run time. It is important to ensure that malicious attacks do not overwrites the code that should not be tampered with after being signed.

Some open source libraries perform strong encryption and these encryption methods are being used widely. These techniques work well with the resource constrained IoT devices. Certificate authorities are serving millions of users and companies in their e-commerce transactions every day. Certificate authorities carry simple and strong trust model for authentication purpose. Certificate authorities ensure authentication mechanism for secure communication between different companies and systems. These certificates are being embedded in millions of devices for trusted communication.

Certificate authorities manage certificates, keys and security credentials which are important for authentication purposes. Different standards are available for certificates, keys and security credentials management and distribution. Standardized formats for certificates are also available. Certificate Authorities "CAs" may use standard formats or custom format support. Certificates are managed through standard protocols like Online Certificate Status Protocol (OCSP), Simple Certificate Enrollment Protocol (SCEP) and Enrollment Over Secure Transport (EST). These protocols help in the management of certificates. Some other protocols use certificates, keys and access tokens to perform authentication. Both protocols are Transportation Layer Security (TLS) and Datagram Transport Layer Security (DTLS).

For the authentication of endpoints, IoT system can use "TLS" or "DTLS". Upon mutual authentication, the keys can be exchanged to establish an encrypted communication to save data from the eavesdropper.

VI. CONCLUSIONS AND FUTURE WORK

IoT systems face more security issues than normal IT system. IoT system contains new communication technologies and resource constrained devices. There are different attack vectors that can threaten IoT systems. Security on IoT systems can be deployed by presenting a security framework according to the security need of IoT system. Security framework helps in understanding and minimizing security threats of IoT system. Certificate authorities can provide trust system for mutual authentication between end points. By using digital certificates, keys and security credentials, authenticated and encrypted communication is possible. Our future work will address a special issue of back up connectivity in IoT system along with implementation details.

REFERENCES

[1] Atlam, H.F., Walters, R.J., Wills, G.B.: (2018) *"Internet of things: state-of-the-art, challenges, applications, and open issues*", Int. J. Intell. Comput. Res. 9(3), 928–938

[2] Cerf, V., Ryan, P., Senges, M., Whitt, R.: (2016) *"IoT safety and security as shared responsibility*". Bus. Inform. 1, 7–19

[3] Gebotys, C, H., Tiu, C, C., Chen, X., (2006) *"A countermeasure for EM attack of a wireless PDA."* Information technology: coding and computing 2005. ITCC 2005, International conference on, vol. 1, pp 544-549. vol. 1, pp. 4-6. April 2006.

[4] Kernis, T., Mamane, W, P., Popovici, E, M., (2005) *"An FPGA implementation of a flexible secure elliptic curve cryptography*

processor". Distinguished paper. International workshop on applied reconfigurable computing ARC 2005. Proceedings, pp 22-30, IADIS press.

[5] Wang, Q., Wang, C., Ren, K., *et al.* (2011) *"Enabling public auditability and data dynamics for storage security in cloud computing"*. Parallel and distributed systems. IEEE transaction on,22(5).847-859, May 2011.

[6] Raza, S., Wallgren, L., Voigt, S, T., (2013) *"Real time intrusion detection in internet of things, Ad-Hoc networks"*, 11(8), 2661- 2674.

[7] Danev B, Zanetti, D., and Capcun, S., (2012) *"On physical layer identification of wireless devices"*. ACM computing surveys. 11/2012. 45(1).

[8] Yan, L., *et al.* (2013) *"Construction and strategies in IoT security system. Green computing and communication (GreenCom)"*, IEEE and Internet of things, IEEE international conference on and IEEE cyber physical and social computing, pp. 1129-1132, 20-23 August 2013.

[9] Chen, P., Cheng, S., Chen, K., (2014) *"Information fusion to defend international attack in Internet of things"*. IEEE IoT journal, vol. 1, No. 4.

[10] Xu, Q., Zheng, R., Saad, W., and Han, Z., (2016) *"Device fingerprinting in wireless networks, Challenges and opportunities*". IEEE communication surveys & tutorials, vol. 18, no 1, pp. 94-104.

[11] Open web application security project, https://owasp.org/www-project-internet-of-things/

[12] Pan, Yao, et al. (2017) *"Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems",* International Journal of Interactive Multimedia & Artificial Intelligence 4.3.

[13] Backenstrass, T., et al. (2016) *"Protection of ECC computations against side-channel attacks for lightweight implementations",* Verification and Security Workshop (IVSW), IEEE International. IEEE.

[14] Bahnasawi, Mohamed A., et al. (2016) *"ASIC-oriented comparative review of hardware security algorithms for internet of things applications",* Microelectronics (ICM), 28th International Conference on. IEEE.

[15] Gonzalez, Jesus David Terrazas, and Witold Kinsner. (2016) *"Zero-Crossing Analysis of Lévy Walks and a DDoS Dataset for Real-Time Feature Extraction: Composite and Applied Signal Analysis for Strengthening the Internetof-Things Against DDoS Attacks."* International Journal of Software Science and Computational Intelligence (IJSSCI) 8.4, 1-28.

[16] Han, Guangjie, et al. (2016) *"Security and privacy in Internet of things: methods, architectures, and solutions",* Security and Communication Networks 9.15: 2641-2642.