Internet of Things (IoT): A Study on Security attacks and Countermeasures

Ahmed A. Mohsin, M.Sc. (Asst. lect.)*

Abstract: Internet of Things (IoT) applications represents a new revolution in information technology field. Researchers have predicted that by 2020, the number of digitally connected devices will exceed 50 billion. However, due to the fact that IoT applications aim to provide the ability for billions of smart devices to connect and interact to each other via the Internet, IoT security challenges are huge. IoT security has always been a major concern of discussion not only for researchers, but also for users when assessing the risks of using IoT applications. IoT applications are vulnerable to various types of attacks related to security issues. Therefore, the need to protect such applications from those attacks has been increased. Many works of researchers have been conducted to reduce or minimize the effect of security attacks on IoT environment. This research aims to explore the security requirements and limitations of IoT, then classifies security attacks based on IoT architecture layers. Finally, up-to-date IoT security solutions are proposed briefly and conclusions are made. This research gives a better understanding to future trends for researchers in IoT security.

Keywords: Internet of Things, IoT Security, Architecture layers, Attacks Countermeasure

* Ministry of Higher Education and Scientific Research

1. Introduction

IoT refers to the connection of physical objects to the Internet based on standard communication protocols; those objects able to collect the data from different resources, exchange them using intelligent interfaces to connect and take a decision and reply with action after analyzing the captured data [1, 2]. IoT applications link physical and virtual things through communication capabilities and securely integrated into the Internet. IoT applications use wireless sensors since these devices responsible for gathering the data and forwarding them to the internet. Different types of applications is shown in figure 1 such as smart homes, wearables, industry, smart cities, building management, monitoring, Smart Transportation, health, smart grids, retail and many others [3, 4].

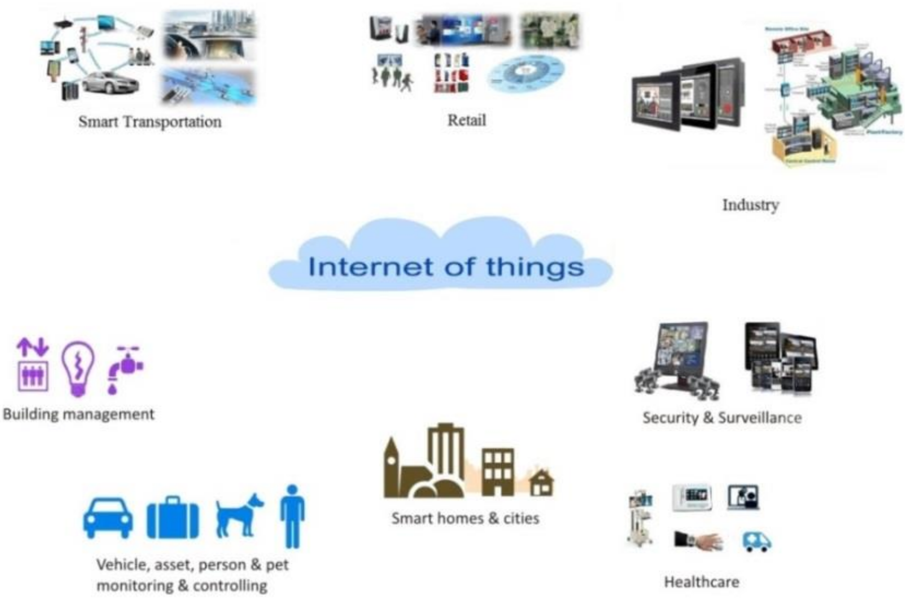

Figure (1): Internet of Things Applications

IoT applications can face challenges and issues regarding all the exchanged data by IoT devices, the security requirements. In 2008, the number of IoT devices connected to the internet was more than the humans on the earth. Looking to the future, the International Data Corporation (IDC) predicts that 41 billion connected devices will be utilize in 2020, [5, 6]. This estimation do not take into account rapid advances in Internet or device technology.

1.1 Security Requirements

Security requirements of IoT system extend past the traditional security requirements. They also need to address authentication, authorization, data freshness, availability and nonrepudiation. In 2016, Distributed Denial of Service (DDoS) attacks against Domain Name System (DNS) causing disruption access or slowness at Twitter, SoundCloud, Spotify, Reddit and many other sites [7]. It is important to highlight the need for extensive researches addressing security concerns for the IoT field. IoT are susceptible to various types of security attacks due to the resources limits computation and transmission operations. From [8, 9, 10, 11], IoT devices should ensure some security goals to consider IoT as secure, which include:

- Confidentiality
- Integrity
- Data authentication
- Authorization
- Integrity
- Non-repudiation
- Availability
- Client privacy
- Attack resiliency
- Access control
- Key management
- Physical security design

Part of or all the above goals should be satisfied and this is a challenging.

1.2 IoT Limitations

Authors of [12, 13] summarized challenges or limitations of IoT:

- **IPv4 address drought:** the world ran out of public IPv4 addresses in February 2010. However, the number of billions of new sensor nodes will require unique IP addresses. IPv6 Features such as auto configuration capabilities and improved security features make the network management easier.

- **Sensor energy:** wireless sensor are low cost, resource-constrained devices that can be used for remote sensing uses. The limited energy is drained due to the execution of the designed functionality that required (e.g., encryption, decryption, key exchange). Different methods can be used to reduce sensor energy.

- **Agreement on Standards:** the lack of standards of authentication and authorization of IoT devices, the demanding for standards are increasing, especially in security of IoT technologies and solutions.

As well as there are some other challenges and parameters, that make the design and implementation of IoT complicated process [14].

- Deployment and mobility of objects
- Heterogeneity
- Network infrastructure
- Connectivity
- Coverage area
- Network size
- Device lifetime
- QoS requirements
- Cost minimization
- Network topology
- Scalability
- Flexibility
- Legal, regulatory and rights.

The design space of IoT requirements is achieved when the characteristics of design step are exploited. However, new advances in smart things will help in design and developing some technologies and tools, which can face these issues and challenges. The study lies in five sections. Section 2 presents IoT architectures. The security threats of a particular layer in section 3 are classified. Section 4 will studies IoT attacks countermeasures. In order to meet the security requirements, some possible solutions are discussed in 5 section. Finally, section 6 summarizes the conclusion of the research.

1.3 Related Works

This subsection tried to study the related works of IoT security based on security solutions and security goals. As the table 1 shows, a range of studies on IoT security solutions with the corresponding protection methods have been tested. The proposed solutions provide confidentiality, integrity, authentication or availability to IoT security proposals.

Table 1: The IoT Security Solutions

Proposed solution for the IoT security	**Approches for realizing Security**	**Security goals**
R. Tahir, H. Tahir, K. McDonald-Maier and A. Fernando[15].	ICMetric (cryptographic keys) coupled with SRRP	Confidentially, Integrity, Authentication, Availability
W. Wang; P. Xu; L. T. Yang [16].	A proxy re-encryption scheme	confidentiality
M. Rebbah, D. El Hak Rebbah, O. Smail [17].	An intrusion detection system based on Signature-based approach	Authentication
L. Zhou and H. C. Chao. [18].	Key management	Authentication
G. Lessa dos Santos, V. T. Guimarães, G. da Cunha Rodrigues, L. Z. Granville and L. M. R. Tarouco [19].	ECC cryptography	Confidentially, Integrity, Authentication, Availability
M. Xin [20].	AES and ECC hybrid encryption algorithm	Confidentially, Integrity, Authentication
M. Leo, F. Battisti, M. Carli and A. Neri [21].	Secure mediation gateway (SMGW)	Authentication, Availability
D. Zegzhda and T. Stepanova [22].	Adaptive random d-regular graph topology	Integrity
S. Raza, L. Seitz, D. Sitenkov and G. Selander [23].	Symmetric Keys	Confidentially, Integrity, Authentication, Availability
T. Fischer, C. Lesjak, A. Hoeller and C. Steger [24].	Off-the-shelf security trust anchors	Authentication
L. Bisne; M. Parmar [25].	Attribute-based	Confidentially,

	Encryption (ABE) and Dynamic S-Box Advanced Encryption Standard (AES)	Authentication
B. Ovilla-Martinez, L. Bossuet [26].	Physically Unclonable Functions (PUF)	Authentication

2. The Architecture of IoT Environnent

This section introduce the most basic architecture that is commonly accepted. Then, we explore IoT architecture which take into account IoT security requirements. There is no single view of IoT structure, which is agreed universally. The IoT needs architectural solutions to manage heterogeneous states and to works efficiently [27]. Different researchers have proposed different architectures. IoT implemented in architecture of several layers.

2.1 Architecture of IoT (Three Layers)

The most basic architecture of IoT network contains at least the following three layers [28, 29] as shown in table 2. It has three layers, namely, application layers, network, and a sensor layer.

Table 2: The three-layer IoT architecture

Layers	Description	Applications
Application layer	defines the required data and the mechanisms used to process and analysis the data in IoT. In this layer, actions such as management, control and Security and of the IoT application are made.	Smartphones, E-Heath, Smart transport, Power Management, Environnent monitor
Network layer	Is responsible for linking to other smart things. Its features are also used for transmitting and processing sensor data.	Wireless/wire Networks
Sensor layer	is sensing and collecting information about IoT devices.	Smart device, RFID, Camera, Sensors, GPS

2.2 IoT Security Architecture

It is recommended that a typical IoT architecture be implemented into four -tiered architecture. Each level will be responsible for performing different tasks. The architecture implementation should take into account the IoT applications security requirements and their domains. The architecture layers of IoT security are secure Device, secure Communications, secure Cloud, and Lifecycle Management by George Cora, which is shown in figure 2, [30].

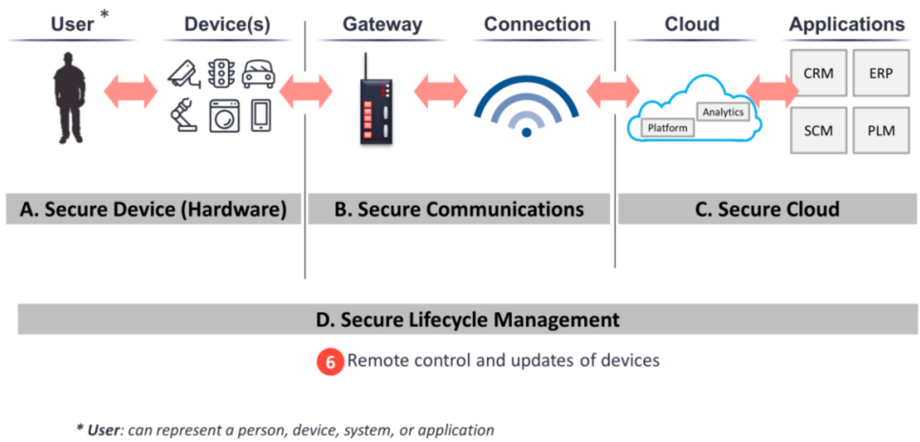

Figure (2): Layered architecture of IoT

1. Secure Device Layer

The device layer represents hardware level of IoT, which may consist of devices or things that are responsible of collecting data or control objects.

2. Secure Communications Layer

This layer transmits and receives data. Regardless the layer that transmits the sensitive data, unsecure communication channel can be susceptible to various attacks.

3. Secure Cloud Layer

The cloud layer can be considered as data handler, it performs many tasks such as ingestion, analyzing and interpretation

4. Secure Lifecycle Management Layer

It is a central layer to keep IoT security up-to-date.

3. Classification of IoT Attacks

The IoT applications are known to be susceptible to security attacks such as unauthorized router access, man-in the-middle attacks, DOS attacks, interference, etc. [31]. Previous works have conducted extensive studies on IoT security. We classify IoT attacks based on the physical layer, the network layer or the application layer (table 3). Attacks are classified depending on which layer the attack happens, some attacks affect more than one layer such as Side channel attacks, Crypto Attacks, Traffic Analysis and Relay attacks.

Table (3). Layered classification of IoT attacks

Attacks	Application layer	Network layers	Sensor layers
Buffer overflows	✓		
Sinkhole		✓	
Relay Attacks			✓
Man-in-the-middle		✓	
Synchronization Attack		✓	✓
Injection	✓		
Unfairness		✓	
Jammers			✓
Malicious Code injection		✓	✓
Sybil		✓	✓
False Routing		✓	
Sleep Deprivation Attack		✓	
Hello and Session Flooding		✓	
Selective Forwarding			✓
Unauthorized access to the tags			✓
Unauthorized tag Reading	✓		
Tag Cloning		✓	

Spoofing		✓	✓
Tag modification	✓		
Impersonation		✓	
Eavesdropping		✓	✓

4. Attacks Countermeasures

This section studies countermeasure for attacks to enhance security of IoT, as shown in Table 4, some of the developed approaches applicable to the protection of IoT are presented.

Table (4). Attacks and countermeasures methods for the three Layered architecture

Attacks	Protection method
Buffer overflows	Address Space Layout Randomization (ASLR) [32].
Sinkhole	Message digest Algorithm
Relay Attacks	Timestamps and challenge response cryptography[45].
Man-in-the-middle	Mutual Authentication and Tamper Detection
Synchronization Attack	VLFSR lightweight encryption function [33].
Injection	Static Analysis (Data-flow analysis [34], Symbolic execution [35, 36]), Dynamic detection (Runtime tainting [37, 38, 39], Instruction set randomization [28], Policy enforcement [41,42], Whitelisting [43])
Unfairness	Small Frames Transmission
Jammers	Direct-Sequence Spread Spectrum, and Hybrid FHSS/DSSS [45].
Malicious Code injection	Signature and anomaly based approach
Sybil	Trusted Certification, Resource Testing, Recurring Fees, Privilege Attenuation, Economic Incentives, Location/Position Verification, Received Signal Strength Indicator (RSSI)–based scheme and Random Key Predistribution [45].
False Routing	Append a Message Authentication Code (MAC) with message

Sleep Deprivation Attack	Random vote, Round Robin scheme
Hello and Session Flooding	Authentication, Packet Leashes
Selective Forwarding	Multiple Disjoint Paths, Egress Filtering, Authentication, Monitoring, Hartbeat protocol
Unauthorized access to the tags	Secure Data Exchange Protocol
Unauthorized tag Reading	Authentication, install field detectors, shift data to backend
Tag Cloning	OTP Synchronization between tag and backend, unique 'RFID Fingerprint' for RFID tag
Spoofing	Message authentication, RC4, TinySec, RC5, Filtering, SSL authentication, IDEA
Tag modification	Authentication, install field detectors, use-read only tags
Impersonation	Cryptographic techniques
Eavesdropping	Session Keys protect NPDU from Eavesdropper, RFID private, Random key agreement method [44], Authentication protocol, RWP, AFMAP

5. IoT Security Solutions

For consumer IoT devices, with all-powerful technology has developed, the potential damage has increased also. Companies such as Dell and Cisco have all spent Billion dollar to develop a reliable and secure platform for the IoT. Any suggested solution should provide security objectives at design levels, at production levels and at all levels of the IoT device and data lifecycle. In addition, A security solution must ensure that the data exchanged by the device and communication are secured. Implementing security procedures into IoT is impossible to implement perfectly. However, to realize secure IoT, more hardware security implementations and standards are needed. As a result, there is no one single security solution, which fits for all security requirements. Here are suggested recommendations that should be considered to build and develop secure IoT solutions:

1. Realization of secure booting of IoT device by cryptography technology Scheme.
2. The consideration of implementation cost and security solution failure.
3. Implementing a multi-layered approach to secure a device in an IoT environment.
4. Avoiding the risk of unauthorized access to resources, devices, data or communication.
5. building all IoT devices and systems with the ability to be updated when a malicious code introduced into IoT system.
6. Authentication all communicating IoT devices.
7. Implementation of secure communication to IoT devices by using encrypting communication such as HTTPS, SSH, SSL, TLS, etc.
8. Providing a Firewall which is a layer of security against common attacks.
9. Detection and monitoring invalid login activities and any malicious attempts.
10. Controlling data traffic.
11. Testing the IoT device configurations.
12. Classification the IoT devices and their management requirements for various protocols and data formats.
13. Defining a unifying architecture that can supporting heterogeneity of network technologies.
14. Defining the related security activities that must be triggered.
15. Securing the Big Data strategy for IoT.
16. Developing privacy strategies for IoT data.

Design and implementation of IoT security should support an open, ubiquitous and interoperable secure infrastructure throughout device lifecycles. We do hope that this suggestions will be useful for researchers in the field of IoT security, devising a better technical solutions able to make IoT security applicable. Furthermore, more extensive studies on the security of IoT will provide better understand the flaws and enhance any suggested security before real attacks happen.

6. Conclusion

The purpose of this paper is to serves as a reference point in IoT security that researchers can use as a basis for future trends. Initially, the requirements of IoT security with the limitations that need to be addressed and some of the related Works are studied. In addition, existing architectures of IoT are discussed. In particular, three layers architecture of IoT is studies. Then, several security attacks and their countermeasures based on three layer architecture are classified. It is significant to introduce the classification of security attacks to evaluate the effects of the potential attacks and the cost of protection when designing new security mechanisms for IoT applications. The last part of this work recommended some up-to-date IoT security solutions to mitigate the problems that occur due to various security attacks. These suggested solutions are intended to help researchers meet upcoming security requirements of IoT under different challenges, or limitations.

References

[1] Mazhelis, et al., “Internet-of-things market, value networks, and business models : state of the art report”. University of Jyväskylä printing House, Finland, 2013.

[2] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions”, Future Generation Computer Systems, 29.7, 1645-1660, 2013.

[3] H. Su, Z. Wang and S. An, "MAEB: Routing Protocol for IoT Healthcare," Advances in Internet of Things, 3, 8, 2013.

[4] M. Jevti´c, N. Zogovi´c, and G. Dimi´c, “Evaluation of Wireless Sensor Network Simulators,” in Proceedings of TELFOR 2009, 17th Telecommunications forum, (Belgrade, Serbia), 24–16 November 2009.

[5] IoT Analytics, “Why the internet of things is called internet of things: Definition, history, disambiguation,” https://iot-analytics.com/internetof-things-definition/, 2014.

[6] (2015) Gartner Says 6.4 Billion Connected “Things” Will Be in Use in 2016, Up 30 Percent From 2015. Available at http://.gartner.com/newsroom/id/3165317. Accessed September 16, 2016.

[7] K. on Security, “DDoS on dyn impacts twitter, spotify, reddit,” 2016.

[8] T. Heer, O. Garcia-Morchon, R. Hummen, S.L. Keoh, S.S. Kumar, K. Wehrle, Security challenges in the ip-based internet of things, Wirel. Pers. Commun.: Int. J. 61 (3) (2011) 527–542.

[9] S. Cirani, G. Ferrari, L. Veltri, Enforcing security mechanisms in the ip-based internet of things: an algorithmic overview, Algorithms 6 (2) (2013) 197– 226, http://dx.doi.org/10.3390/a6020197.

[10] R. H. Weber, “Internet of things–new security and privacy challenges,” Computer Law & Security Review, vol. 26, no. 1, pp. 23–30, 2010.

[11] K. Zhao and L. Ge, “A survey on the internet of things security,” in Computational Intelligence and Security (CIS), 2013 9th International Conference on, pp. 663–667, IEEE, 2013.

[12] D. Evans, “How the Next Evolution of the Internet Is Changing Everything”, Cisco white paper, April 2011.

[13] W. Trappe, R. Howard, and R. S. Moore, “Low-energy security: Limits and opportunities in the internet of things,” IEEE Security Privacy, vol. 13, no. 1, pp. 14–21, Jan 2015.

[14] D. Bandyopadhyay, J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization," Wireless Personal Communications, Vol. 58, No. 1, 2011.

[15] R. Tahir, H. Tahir, K. McDonald-Maier and A. Fernando, "A novel ICMetric based framework for securing the Internet of Things," 2016 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, 2016, pp. 469-470.

[16] W. Wang; P. Xu; L. T. Yang, "Secure Data Collection, Storage and Access in Cloud-Assisted IoT", IEEE Cloud Computing, 2018.

[17] M. Rebbah, D. El Hak Rebbah, O. Smail, "Intrusion detection in Cloud Internet of Things environment", 2017 International Conference on Mathematics and Information Technology (ICMIT), 2017, Pages: 65 – 70.

[18] L. Zhou and H. C. Chao, "Multimedia traffic security architecture for the internet of things," in IEEE Network, vol. 25, no. 3, pp. 35-40, May-June 2011.

[19] G. Lessa dos Santos, V. T. Guimarães, G. da Cunha Rodrigues, L. Z. Granville and L. M. R. Tarouco, "A DTLS-based security architecture for the Internet of Things," 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, 2015, pp. 809-815.

[20] M. Xin, "A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System," 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Xi'an, 2015, pp. 62-65.

[21] M. Leo, F. Battisti, M. Carli and A. Neri, "A federated architecture approach for Internet of Things security," 2014 Euro Med Telco Conference (EMTC), Naples, 2014, pp. 1-5.

[22] D. Zegzhda and T. Stepanova, "Achieving Internet of Things security via providing topological sustainability," 2015 Science and Information Conference (SAI), London, 2015, pp. 269-276.

[23] S. Raza, L. Seitz, D. Sitenkov and G. Selander, "S3K: Scalable Security With Symmetric Keys—DTLS Key Establishment for the Internet of Things," in IEEE Transactions on Automation Science and Engineering, vol. 13, no. 3, pp. 1270-1280, July 2016.

[24] T. Fischer, C. Lesjak, A. Hoeller and C. Steger, "Security for building automation with hardware-based node authentication," 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2017.

[25] L. Bisne; M. Parmar, “Composite secure MQTT for Internet of Things using ABE and dynamic S-box AES”, 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), 2017.

[26] B. Ovilla-Martinez; L. Bossuet, “Restoration protocol: Lightweight and secur devices authentication based on PUF”, 2017 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), 2017.

[27] M. Weyrich and C. Ebert, “Reference architectures for the internet of things,” IEEE Software, vol. 33, no. 1, pp. 112–116, 2016.

[28] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, “Choices for interaction with things on Internet and underlying issues,” Ad Hoc Networks, vol. 28, pp. 68–90, 2015

[29] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, “Research on the architecture of internet of things,” in Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10), vol. 5, pp. V5-484–V5-487, IEEE, Chengdu, China, August 2010.

[30] Understanding IoT Security – Part 1 of 3: IoT Security Architecture on the Device and Communication Layers URL: https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/, last accessed on: 27/01/2018.

[31] R. Acharya and K. Asha, “Data integrity and intrusion detection in wireless sensor networks,” in Networks, 2008. ICON 2008. 16th IEEE International Conference on, pp. 1–5, IEEE, 2008.

[32] Address space layout randomization URL: https://en.wikipedia.org/wiki/Address_space_layout_randomization, last accessed on: 27/01/2018.

[33] J. Garcia-Alfaro, J. Herrera-Joancomartí, and J. Melià-Seguí, Security and Privacy Concerns About the RFID Layer of EPC Gen2 Networks, in: G. Navarro-Arribas and V. Torra (Eds.), Advanced Research in Data Privacy, Springer International Publishing, 2015, pp. 303–324.

[34] Johannes Dahse , Thorsten Holz, “Static detection of second-order vulnerabilities in web applications,” Proceedings of the 23rd USENIX conference on Security Symposium, p.989-1003, August 20-22, 2014, San Diego, CA.

[35] T. Avgerinos, A. Rebert, S. K. Cha, and D. Brumley, “Enhancing symbolic execution with veritesting,” in Proceedings of the 36th International Conference on Software Engineering. ACM, 2014, pp. 1083–1094.

[36] M. Trinh , D. Chu and J. Jaffar, “S3: A Symbolic String Solver for Vulnerability Detection in Web Applications”, Proceedings of the 2014 ACM

SIGSAC Conference on Computer and Communications Security, November 03-07, 2014.

[37] L. Bauer, S. Cai, L. Jia, T. Passaro, M. Stroucken, and Y. Tian. “Run-time monitoring and formal analysis of information flows in Chromium”. In NDSS, 2015.

[38] Deian Stefan, Edward Z Yang, Petr Marchenko, Alejandro Russo, Dave Herman, Brad Karp, and David Mazieres, “Protecting users by confining JavaScript with COWL”. In OSDI, 2014.

[39] Daniel Hedin , Arnar Birgisson , Luciano Bello , Andrei Sabelfeld, “JSFlow: tracking information flow in JavaScript and its APIs”, Proceedings of the 29th Annual ACM Symposium on Applied Computing, March 24-28, 2014, Gyeongju, Republic of Korea.

[40] Athanasopoulos, E., Pappas, V., Krithinakis, A., Ligouras, S., Markatos, E.P.: xJS: “Practical XSS Prevention for Web Application Development”. In: Proceedings of the 1st USENIX WebApps Conference, Boston, US (June 2010).

[41] Victor van der Veen , Dennis Andriesse , Enes Göktaş , Ben Gras , Lionel Sambuc , Asia Slowinska , Herbert Bos , Cristiano Giuffrida, “Practical Context-Sensitive CFI”, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, October 12-16, 2015, Denver, Colorado, USA.

[42] Ali Jose Mashtizadeh , Andrea Bittau , Dan Boneh , David Mazières, CCFI: Cryptographically Enforced Control Flow Integrity, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, October 12-16, 2015, Denver, Colorado, USA.

[43] Pratik Soni , Enrico Budianto , Prateek Saxena, The SICILIAN Defense: Signature-based Whitelisting of Web JavaScript, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, October 12-16, 2015, Denver, Colorado, USA.

[44] R. Jin, X. Du, Z. Deng, K. Zeng, and J. Xu, Practical Secret Key Agreement for Full-Duplex Near Field Communications, IEEE Transaction on Mobile Computing, 2015, vol. 1233.

[45] El Mouaatamid O , Lahmer M . Internet of Things security: layered classification of attacks and possible countermeasures. Electron J 2016(9).

إنترنت الأشياء: دراسة عن الهجمات الأمنية والتدابير المضادة

م. م. أحمد عباس محسن*

المستخلص: تمثل تطبيقات إنترنت الأشياء ثورة جديدة في مجال تكنولوجيا المعلومات. يتوقع الباحثون انه بحلول عام 2020، سيتجاوز عدد الاجهزة المتصلة رقميا 50 مليار جهاز. مع ذلك ونتيجة ان تطبيقات انترنيت الاشياء تهدف الى توفير القدرة للاتصال والتفاعل لملايين الاجهزة الذكية مع بعضها البعض عبر الأنترنيت، تبقى تحديات امن انترنيت الاشياء كبيرة. لطالما كان امن انترنيت الاشياء مصدر اهتمام كبير للبحث ليس فقط للباحثين وانما ايضا للمستخدمين عند تقييم مخاطر استخدام تطبيقات انترنيت الاشياء. تطبيقات انترنيت الاشياء معرضة لأنواع مختلفة من الهجمات المتصلة بمشاكل الحماية. لذلك ازدادت الحاجة لحماية مثل هذه التطبيقات من تلك الهجمات. تم اجراء العديد من الابحاث لخفض او تقليل تأثير الهجمات على بيئة عمل انترنيت الاشياء. يهدف البحث الى تحري متطلبات الحماية وقيود انترنيت الاشياء ومن ثم تصنيف الهجمات بناء على معمارية الطبقات. اخيرا وبإيجاز تم اقتراح حلول حماية محدثة. استنتاجات هذا البحث تزود الباحثين بفهم افضل للتوجهات المستقبلية في مجال حماية انترنيت الاشياء.

الكلمات المفتاحية: انترنيت الاشياء، امن انترنيت الأشياء، طبقات العمارة، الهجمات المضادة.

*وزارة التعليم العالي والبحث العلمي