International Journal of Management, IT & Engineering
Vol. 9 Issue 6, June 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A LAYER-WISE SECURITY ANALYSIS FOR INTERNET OF THINGS NETWORK: CHALLENGES AND COUNTERMEASURES

Arun Kumar Bediya [*]

Dr. Rajendra Kumar [**]

Abstract

Internet of things is a vast domain, still spreading over different areas of the society, with a fast pace. The Connected IoT devices will increase in rapid pace and it is expected to extend up to 20 billion IoT devices till 2020. According to digital security firm Gemalto IoT endpoint spending will reach approximately $3tr by 2020 and has potential to generate $19tr in next decade. IoT is combination of hardware and software, where Hardware may consists of Sensor nodes, Radio Frequency Identification (RFID), Near Field Communication (NFC) and low energy Bluetooth devices etc. Software provides middleware, information queries, data repository and data retrieval and exchange. All WSN devices turns IoT component when it is supervised using internet and significant security issues happen just when nodes are associated with the internet. This acquires a great deal of concerns identified with the privacy and security, standardization and power management. In this paper we have depicted security issues at various layers of IoT and furthermore outlined security solutions for each layer of IoT.

Keywords:

IoT Architecture;

IoT Layers;

Security Issues in IoT.

[*] **Department of computer science,Jamia Millia Islamia university , New Delhi ,India**

[**] **Department of computer science,Jamia Millia Islamia university , New Delhi ,India**

1. Introduction

The IoT can be defined as “an overall system of interconnected objects”, these object must have

- A unique identity by which can be addressed.
- Can be accessed using internet or smart interface.
- Must be self organized and repairable.

There are numerous application areas of IoT, extending from individual to enterprise environments. IoT has numerous usage areas like agriculture, transportation, health care, production and distribution of energy. IoT devices controlled through identity management i.e. unique identity that has assigned to device, used to distinguish it from collection of homogeneous and heterogeneous devices [1] [2].

In this paper, we give a review of the IoT architecture framework (Section 2), briefly described various security issues at each layer of IoT infrastructure (Section 3), also highlighted the solutions for security issues present at each layer (Section 4), and we described a proposed mechanism to detect threats using machine learning (Section 5), and conclusion of the study (Section 6).

2. IoT Architecture

IoT architecture functionality is based on three layers named as Perception Layer or Physical Layer, Network Layer or Middle Layer and Application Layer [3]. Whereas there is distinctive point of view with respect to the quantity the layers in IoT. This paper described three layered architecture with each layer functionality and devices that are used at each layer.

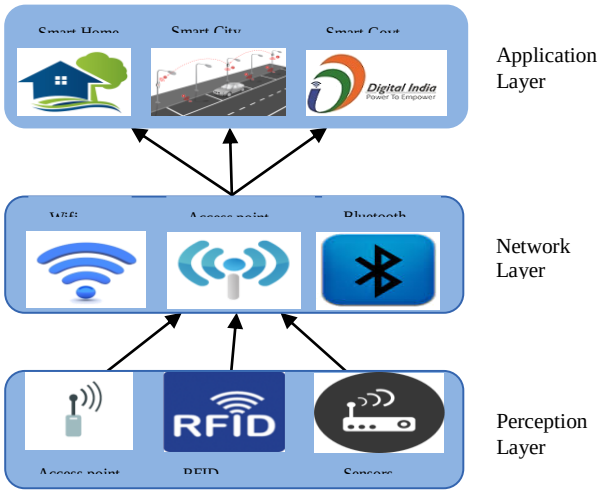

Fig. 1 IoT layer Architecture

Every layer of IoT additionally has many security issues associated beside it. Fig.1 demonstrates the fundamental three layer architecture system of IoT such as devices and technologies that encompassed in each layer [4] [5] [6].

Many security frameworks have been proposed which analyzing security issues and claim to be used to used for monitoring and analyzing security of the IoT network [7][8][9] [10].

2.1 Perception Layer

In IoT, This is the layer of sensor and sometimes it is also called "Sensors" layer. Basic function of this layer is to detect data, collect it and then processing. After processing information data is transferred to Network Layer. Data is collected from the environment by using sensors and actuators. Node collaboration is also performing on this layer for local network or short-range small networks.

2.2 Network Layer

This layer performs data transmission to different devices over the internet and data routing is also done by this layer. Devices like routing devices, internet gateways, switching devices, cloud computing devices are used at this layer. These devices work on technologies, for example, Wi-Fi, 3G, 4G and Bluetooth and so forth. The network gateway fills in as the intermediary amid various IoT nodes from sensors by combining, filtering, and transmission of information [11].

2.3 Application Layer

Smart Environment creation is the main purpose of this layer. This layer assures the data integrity, data authenticity and data confidentiality. Perception layer undertake on collection of information and data from various IoT devices towards web applications

3. Security Issues in IoT

In recent IoT botnet attacks performed like Mirai (malware), it is the biggest DDoS attack performed in the history. In October 2016 Mirai attack disturbed websites operations crosswise over North America and Europe after attackers flooded DNS service Dyn with malicious lookup requests from connected devices, like IP cameras, DVRs, switches and routers. As result various prominent websites such as Twitter, Amazon, Netflix, Airbnb, Reddit, GitHub, and many more could not navigated.

Brickerbot attack is another DDoS attack performed same as the Mirai botnet, in that it depended upon a DDoS attack and clients not changing the default username/password of their device [12] [13].

A report from F5 LABS indicated how IoT devices have been focused through botnets, numerous from a solitary facilitating supplier. As indicated by the report, IoT attacks grew 280% from the earlier half year revealing period of 2017, with a vast piece of this development coming from Mirai—malware that contaminates IoT devices and transforms them into bots [14]. In Table 1, a world's leading research and advising company Gartner predicted Worldwide Expenditure Forecast on Internet of Things security [15].

Table 1: Expenditure prediction on IoT security (in Millions of Dollars)

Year	2014	2015	2016	2017	2018
Expenditure	231.86	281.84	348.32	433.95	547.20

To secure IoT devices all kind of Security issues at different layers of IoT need to be understood. Various types of security issues at each layer are defined in brief considering the overall framework, the security issues must be settled toward the start of the design [16] [17].

3.1 Security issues at Perception Layer

Perception Layer deals with hardware's such as RFID and all sensors. Data is collected and transferred to network layer using wireless network transmission. The lack effective protection may result threat to signal as it is exposed in public place so as signal can be monitored, intercept, and disturbed easily [18] [19]. There are various types of attacks possible in IoT devices.

a) Denial of Service Attack

It is the most widely recognized attack for WSN and Internet as well. It causes waste of network assets, and frames the service out of reach from authorized users.

b) Replay Attack

Transmitting the valid data fraudulently or maliciously in repeated manner or delaying the transmission is known as Replay attack.

c) Node Capture

Capturing the node or device physically an attacker can control, leak all information, obtain security keys including group key, matching key, radio key etc. after that impact the protection of the whole framework.

d) Side Channel Attack

Electronic circuit are leaky, they produce emission as byproducts so as attacker can gather information about how data is processing and how the circuit information such as time required, energy expenditure, and electromagnetic radiation in the network. The use of emission can be used to perform reverse engineering gain the term 'side-channel analysis' or 'side-channel attack'.

e) Addition of Fake Nodes

New node inclusion to the system can be done by attackers, and feed fake date or code. This can stop system for transmitting real data by keeping busy to limited energy source; it can harm the energy source sleep, control it or can destroy the entire network.

f) Timing Information

Attacker also interested to get the information regarding the time required to obtain the key information and execution time required for encryption algorithms.

g) Attack on Routing

Routing of network transmission can be influenced by attacker utilizing fake, tampered or repeating routing information. This can contradict network transmission, create loops in routing, increment end-to-end delay, create error messages, extend or abbreviate the source way and so forth.

h) Brute force attack

Brute force attack is also most likely to suffer sensor node due to its ability of limited resource storage and computation.

i) Impersonation

Authentication in the dispersed condition is extremely troublesome to the perceptual node; taking into consideration that malicious node utilizes a fake identity to perform malicious or conspiracy attacks.

3.2 Security issues at Network Layer

Information must be secure while departing, travelling and dispatched towards web from the router. Information in travel over the system network also must be prevented against malicious movements [20].

a) Traditional Issues

Existing network for communication obtained relatively overall security assurance but there are yet many frequent issues like eavesdropping, Man in the middle attack, illegal access network, DoS attack, privacy damage, integrity damage, virus invasion, exploit attack etc. These problems can lead threat on data confidentiality and integrity.

b) Compatibility Issues

IoT network is a network of physical devices, vehicle, human, sensors, smart-phones etc. Due to heterogeneity of IoT security, coordination of network, inter-operability becoming worse. Existing web network security configuration based on human perspective, and does not certainly apply to correspondence between machines. Available security techniques will breakdowns rationale connection between IoT machines reason for compatibility issues.

c) The Cluster Security Problems

Existing IP technologies cannot be applied to large number of node identification as IoT has enormous amount of devices. Immense number of nodes traffic will probably block network if it uses the current authentication mechanism. Mutual authentication between much equipment

cause literally waste of the crucial resources

d) Privacy Disclosure

Privacy information of particular user's can also be easily hacked by attackers by using social engineering and by developing information retrieval technologies.

3.3 Security issues at Application Layer

Security at application layer is the most complex and burdensome in the IoT architecture. For different environment or industrial applications different security issues are exist. Presently there is no ubiquitous standard for development of Application Layer. Following are few common security issues applicable on Application Layer

a) Software Vulnerabilities

Hacker can find out software vulnerabilities like buffer overflow vulnerabilities exist in the software due to non standard code development by software developers. It can be exploits to carry their purposes.

b) Authentication Issues

An application can have huge number of users and different application have different users, to prevent illegal user intervention effective technologies should be apply for authentication of true users. Authentication service must also consider the spam, malicious information identification and processing.

c) Protection and Recovery Issues

User privacy can be compromised in data communication. Existing data processing algorithms and data protection mechanisms are not ideal and this can cause loss of information and disastrous vandalism.

d) Mass-Data Dealing Issues

Enormous data transmission by several number of nodes and complex environment of IoT can lead to data interruption and data loss, if the adapted ability unable to meet the requirement.

e) Privacy leak

IoT application is mainly executed on common hosting services and operating system, it is not difficult for attacker to utilize known vulnerabilities for stealing user data such as user credentials, user historical data, and social relations.

f) DoS attack

It is the similar attack like described in middleware layer, in that attacker can crush the accessibility of the application.

g) Malicious code

Fetch software virus to utilize known vulnerabilities by uploading malicious codes.

4. Security Solutions for IoT Layer

The regular security protocols devour a lot of memory and processing resources. Fig.2 demonstrates the abstract outlook of security mechanism and methods applicable on IoT layers. This section introduces security measures for each layer in IoT. The most important component of Perception Layer is RFID and WSN, this motivate to introduce RFID and WSN security measures respectively [21].

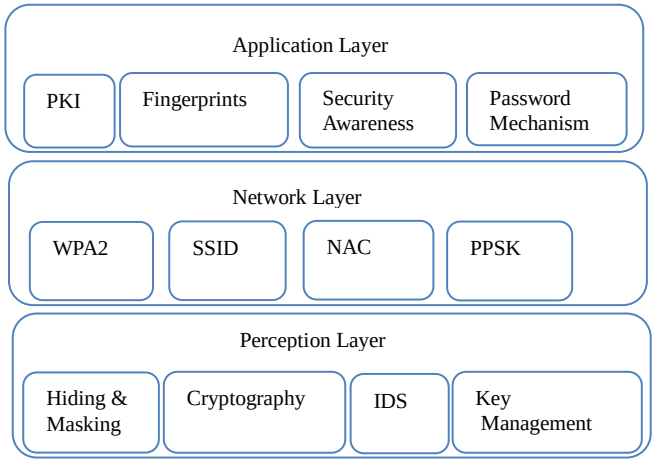

Fig. 2 Layer-wise security measures

4.1 Security Measure for Perception Layer

a) Side Channel Attack

Side Channel Attack (SCA) is a noteworthy issue in physical security. Differential Power Analysis (DPA) is a typical method for SCA. Hiding and Masking are two types of methods that can prevent DPA. Eliminating data dependencies of energy consumption is hiding mechanisms while Masking provides the middle estimations of encryption tools by randomized all the process.

b) Accessibility

Password based system can be used to protect RFID Tags and accessibility, chip security, antenna power analysis etc.

c) Cryptography

RFID can be protected by using Cryptography technology to protect confidentiality, user privacy protection, authentication and integrity of RFID systems. Hash function, Random number mechanisms, Logic Algorithm, re-encryption mechanisms and server data search algorithms are the part of security communication protocol.

d) Key Management

Security design prerequisites of Wireless sensor networks key management predominantly reflects security creation of key or algorithm modification, forward and backward protection and extensibility, source verification, freshness, and against conspiracy attacks. Four fundamental key distribution protocols are simple key distribution, hierarchical key management protocol, key pre-distribution method and dynamic key management algorithm.

e) Secret Key Algorithms

This is mainly incorporates symmetric key and asymmetric keys algorithms. Rivest-Shamir-Adleman (RAS) and Elliptic Curves Cryptography (ECC) are mainly used in Asymmetric keys algorithm, almost all current cryptographic systems internally use symmetric-key algorithms to encrypt mass messages.

f) Security Routing Protocol

An efficient routing protocol algorithm for security mainly uses following techniques Clustering, Data fusion, multiple hops routing, key management etc. For security routing mechanism SPINS security system protocols is broadly utilized, comprise of Secure Network Encryption Protocol (SNEP) and Micro Timed Efficient Streaming Loss-tolerant Authentication Protocol (μTESLA) protocol. SNEP is utilized to accomplish Confidentiality, Integrity, point to point authentication and freshness.

g) Intrusion Detection Technology

An Intrusion Detection System (IDS) is able to analyze the working of system nodes timely, and observe nodes suspicious behavior. Mechanism for protection from Cross site scripting (XSS) and cross site request forgery (CSRF) should be accomplished.

4.2 Security Measure for Network Layer

As IoT network nodes are random or irregular, autonomic, instability of energy restrictions and communication, it prompts that IoT have no foundation and dynamic topology [22].

h) Wireless Protected Access 2 (WPA2)

Wireless Protected Access 2 could settle on the organize utilization stronger unpredictable remote encryption instead of using Wireless Encryption Protocol (WEP).

i) Service Set Identifiers (SSID)

For wireless networks it is better to use many SSID instead of using only one. Thus, we may have divergent policies along each component and can allocate individual for different type of threats. Hence if any component affected by attacker, still other components will be safe.

j) Network Access Control (NAC)

Securing endpoints security technologies like antivirus, network intrusion detection system (NIDS), host intrusion prevention system (HIPS) provides better security mechanism to the network. Furthermore, it is also logical to index MAC addresses of each connected devices so that IP addresses allocate by router only to router listed devices and unknown devices can be blocked.

k) Private Pre-Shared Key (PPSK)

It is a method to connect device uniquely, securely and effortlessly in the networks. PPSK to each device connected to the network provides unique key to access network, and accessing domain might be characterized effectively to every device in the network.

l) NAT- Port Mapping Protocol Service (NAT-PMP)

The NAT-PMP is a network protocol for building settings of network address translation (NAT) and port passing configurations freely without user struggle. NAT-PMP does not follow any authentication methods and permit every host associated to the router's confined network to directly travel across the firewall. Hence, it need to be assured to examine the routers regularly regarding NAT-PMP services mis-configurations. Disabling all type of default and guest passwords from devices like routers and gateways need to be immediately finish when addition of any new network node or device. This incorporates powerful password policies, secret key management and more occasional updating of passwords.

m) IPSec Security Protocol

Authentication and Encryption can also be done using IPSec protocol. Authentication mechanisms enable the receiver to confirm the real identity of sender. Data encryption mechanisms protect data while transmission from attacker to eavesdropping and tampering data and enable confidentiality by encoding the data.

n) Authentication and Access Control

Authentication systems usually incorporate on the light weighted public key authentication techniques, random key pre-distribution authentication technology, Pre Shared Key (PSK), one-way hash functions authentication technology, utilizing auxiliary data authentication technology and so forth. Access control primarily incorporates symmetric and asymmetric cryptosystem.

4.3 Security Measure for Application Layer

There are many Utilizations application layer of IoT and it has diversity and instability. It introduce that distinctive application environment have diverse security demands.

a) Key protocol and Network Authentication

The basic mechanism are symmetric key crypto-framework, public key crypto-framework (certificates or PKI), and certificate exchange technology.

b) Privacy protection

Many techniques are available like digital watermarking, fingerprint technology, threshold cryptography, anonymous authentication etc. used to protect private information.

c) Security Awareness

IoT users must be aware of correctly use of IoT services and information security importance. So that confidential information cannot be leaked.

d) Physical Security

Physical security constraint, physical resource control security, access control using password mechanism, and data management etc. Also paired devices default password must be updated. Idle time locking and maximum attempt implementation help in securing devices.

Denial of service: a common attack at each layer

DoS is an common attack that can exercise at all the three layers of IoT, Table 2 illustrated how it is significant to every layer also how to prevent and protect by this attack at each layer of IoT [23] [24].

Table 2: Solutions for DoS attacks

IoT Layer	**Attack/Issues**	**Solutions/Methods**
Perception Layer	Jamming	All or nothing Transmission ,Strong Hiding Commitment Scheme,Packet Hiding ,Cryptanalysis and Steganography ,Cryptographic puzzle base scheme
	Desynchronizing attack	Double Authentication Scheme, Packet Authentication

Network Layer	UDP Flood , ICMP Flood	BCP38, Firewall Filtering
	DNS Flood	DNSSEC ,uRPF
	Smurf Attack	Block illegal ICMP Responses, Infrastructure Protection, Name Server Protection
Application Layer	Programming Attack	Parameterized Query, Input validation at server
	Path based DoS	Normalize input

5. Current Status of IoT Security

Existing security frameworks are not addressing overall security issues and still there is scope of improvements, hence there is need to develop a security framework that not only provides security mechanism but also be able to predict possible threats or attack. As IoT is growing technology and it has various issues related to security. It has vast domain for analysis and opportunity for researcher to develop and proposed security solutions for existing issues. Detection and identification of threats is also a major problem in IoT network [25] [26] [27].

To countermeasures the issues and challenges in securing devices connected to IoT network the machine learning methods can be used inside an IoT network to secure the framework. Machine learning is a region of artificial intelligence (AI) in which computer programs are empowered to gain from experience, illustrations, and analogies. As learning happens, the abilities inside the program turn out to be more intelligent and the program ends up plainly capable of decisions making. This phenomenon can play a vital role in IoT network security.

6. Conclusion and Future Work

This paper elaborated IoT layer architecture, problems, challenges and countermeasure for each layer of IoT structure. IoT network framework is combination of many layers and numerous problems originated from system concatenation and there are numerous issues which are not has

a place with certain layer i.e. privacy and protection is common problem in every layer some have discussed but still there can be many more issues. This paper also described protocols of each layers of IoT and included methods, technologies and mechanism to protect from several issues at each IoT layers. In future machine learning technique can be applicable on the IoT network to protect network by various security issues and attacks.

References

[1] Rajendra Billure, Varun M Tayur, Mahesh V, "Internet of Things - A Study on the Security Challenges", Department of Computer Science and Engineering, Jain University Bangalore, India, IEEE, 2015.

[2] "Internet of Things (IoT)" http//internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[3] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things perspectives and challenges", Wireless Networks, 2014, vol. 20, no. 8, pp. 2481–2501, Springer 2014.

[4] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan, "Internet of Things (IoT) Security Current Status, Challenges and Prospective Measures", Department of Computer Science & Engineering, American University of Sharjah, UAE, IEEE 2015.

[5] S. S. Basu, S. Tripathy and A. R. Chowdhury, "Design challenges and security issues in the Internet of Things," 2015 IEEE Region 10 Symposium, Ahmedabad, 2015, pp. 90-93.

[6] Lan Li, "Study on security architecture in the Internet of Things," Proceedings of 2012 International Conference on Measurement, Information and Control, Harbin, China, 2012, pp. 374-377.

[7] M. Mohsin, Z. Anwar, G. Husari, E. Al-Shaer and M. A. Rahman, "IoTSAT A formal framework for security analysis of the internet of things (IoT)," 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, 2016, pp. 180-188.

[8] B. F. Zahra and B. Abdelhamid, "Risk analysis in Internet of Things using EBIOS," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017, pp. 1-7.

[9] P. A. Wortman, F. Tehranipoor, N. Karimian and J. A. Chandy, "Proposing a modeling framework for minimizing security vulnerabilities in IoT systems in the healthcare

domain," 2017 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI), Orlando, FL, 2017, pp. 185-188.

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

[11] Gurpreet Singh Matharu, Priyanka Upadhyay, Lalita Chaudhary,"The Internet of Things Challenges & Security Issues", IEEE,2014.

[12] https//krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/.

[13] http//www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/.

[14] https//f5.com/labs/articles/threat-intelligence/ddos/the-hunt-for-iot-the-rise-of-thingbots.

[15] https//www.gartner.com/newsroom/id/3291817.

[16] Kai Zhao1, Lina Ge1, "A Survey on the Internet of Things Security", School of information science and engineering,Guangxi University for nationalitiesGuangxi, China, IEEE, 2013.

[17] Weizhe Zhang,Baosheng Qu, "Security Architecture of the Internet of Things Oriented to Perceptual Layer" International Journal on Computer, Consumer and Control (IJ3C), Vol. 2, No.2(2013).

[18] Andrea Zanella,Senior Member, IEEE, Nicola Bui, Angelo Castellani,Lorenzo Vangelista,Senior Member, IEEE, and Michele Zorzi, Fellow, IEEE "Internet of Things for Smart Cities" IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 1, FEBRUARY 2014.

[19] W. Z. Khan, H. M. Zangoti, M. Y. Aalsalem, M. Zahid and Q. Arshad, "Mobile RFID in Internet of Things Security attacks, privacy risks, and countermeasures," 2016 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), Jakarta, 2016, pp. 36-41.

[20] Luigi Atzori , Antonio Iera , Giacomo Morabito, The Internet of Things A survey, Computer Networks The International Journal of Computer and Telecommunications Networking, v.54 n.15, p.2787-2805, October, Elsevier, 2010.

[21] Leloglu, E., A Review of Security Concerns in Internet of Things. Journal of Computer and Communications, 5, 121-136, 2017.

[22] Brian Russell, Cesare Garlati, David Lingenfelter, "Security Guidance for Early Adopters of the Internet of Things (IoT)", CSA Mobile Working Group, Apr. 2015.

[23] Senthilkumar Mathi, Lavanya Dharuman, Prevention of Desynchronization Attack in 4G LTE Networks Using Double Authentication Scheme, Procedia Computer Science, Volume 89, 2016, Pages 170-179.

[24] https//www.owasp.org.

[25] I. Kotenko, I. Saenko, F. Skorik and S. Bushuev, "Neural network approach to forecast the state of the Internet of Things elements," 2015 XVIII International Conference on Soft Computing and Measurements (SCM), St. Petersburg, 2015, pp. 133-135.

[26] R. Madeira and L. Nunes, "A machine learning approach for indirect human presence detection using IOT devices," 2016 Eleventh International Conference on Digital Information Management (ICDIM), Porto, 2016, pp. 145-150.

[27] J. Cañedo and A. Skjellum, "Using machine learning to secure IoT systems," 2016, 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, 2016, pp. 219-222.