A Taxonomy of Security and Privacy Requirements for the Internet of Things (IoT)

Israa Alqassem, Davor Svetinovic
Electrical Engineering and Computer Science
Masdar Institute of Science and Technology
Abu Dhabi, United Arab Emirates
Email: {ialqassem, dsvetinovic}@masdar.ac.ae

***Abstract*—Capturing security and privacy requirements in the early stages of system development is essential for creating sufficient public confidence in order to facilitate the adaption of novel systems such as the Internet of Things (IoT). However, security and privacy requirements are often not handled properly due to their wide variety of facets and aspects which make them difficult to formulate. In this study, security-related requirements of IoT heterogeneous systems are decomposed into a taxonomy of quality attributes, and existing security mechanisms and policies are proposed to alleviate the identified forms of security attacks and to reduce the vulnerabilities in the future development of the IoT systems. Finally, the taxonomy is applied on an IoT smart grid scenario.**

***Keywords*-Internet of Things; privacy; security; requirements engineering;**

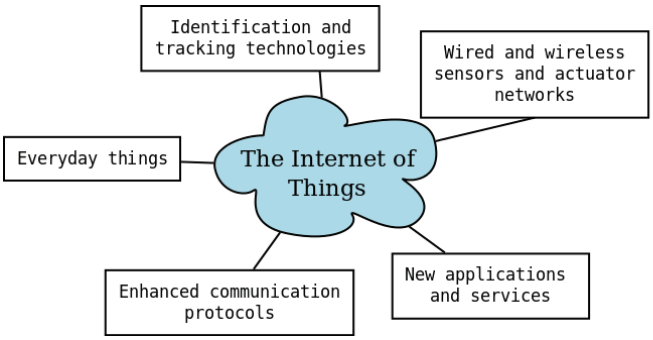

Fig. 1. The technologies and communication tools compose the IoT

I. Introduction

The idea behind the Internet of Things (IoT) is to connect not only people and computers, but also everyday objects to the Internet. This can be achieved by equipping things with computing and communication abilities thus entirely mapping the physical world to the digital one. This vision has come from the fact that people have limitations in time and accuracy when it comes to data gathering and generation, but if these processes can be done without any human interference (i.e., by having uniquely identifiable objects to report their status, location, addresses, etc.), then the costs and losses could be reduced dramatically. The IoT has the potential to change the ways of working and living with its new aspects of communication and interaction, and innovative services and applications, e.g., real-time objects monitoring, search engine for things, etc. [1], [12].

The IoT is exposed to significant privacy and security risks. They can be themselves used to both protect and violate privacy and security. For example, Atzori et al. [1] mentioned *theft application* as one of the potential applications of the IoT. The IoT will make it possible to develop an application which sends out SMS messages immediately to users whenever their personal stuff (such as television or wallet) is moved from predefined locations without their permission. Also, the architectural nature of the IoT, where billions of objects may interact with each other, will attract malicious attackers and eavesdroppers to collect data thus breaking privacy and security rules [16]. Hence, maintaining secure and private connections and transmission of information, in addition to preventing data collection, are critical requirements for the IoT.

The most complex challenge from the requirements engineering perspective is the difficulty of specifying requirements, and security and privacy requirements in particular, for a system with so many components that can be randomly integrated in various systems at various times and places. Due to the diversity and complexity of the IoT, it is difficult even to envision what system an object will be a part of. As such, we investigate security and privacy of the IoT for the early-phase of requirements engineering to help users to understand the various facets and aspects of security and privacy, and to help developers to handle them properly.

II. IoT Key Components

To obtain a basic understanding of the IoT Figure 1 shows the most relevant technologies and communication tools needed to integrate and build the IoT system [1]. The key components are RFID systems and sensor networks:

1) RFID Systems [1], [3]: The full deployment of the IoT relies on the widespread use of Radio-Frequency IDentification (RFID) tags to identify everyday objects, which enables the tracking ability of objects through space and time in a sustainable manner. RFID is considered as an enabling technology and it has a wide range of beneficial applications such as electronic toll collection systems, access management systems, airport baggage tracking logistics, etc. By using RFID, it is possible for an object to identify itself to another object, and on that account

978-1-4799-6410-9/14/$31.00 ©2014 IEEE

RFID systems form the basic structural unit of the IoT. RFID systems are composed of:

- Uniquely identifiable tags that can be assigned to different objects. Each tag is able to receive a reader's signal, and it is able to transmit its ID back to the reader.
- Readers whose responsibility is to generate appropriate signals to receive tag IDs.

2) Sensor Networks: They are currently used in various fields like e-health, military and industry. Each sensor network consists of a large number of sensing nodes, in addition to a special node called sink, where the sink node is used to collect sensing results reported by other nodes in the network. Because such networks can cooperate with RFID systems to enhance objects tracking, sensor networks have a significant role in the IoT development.

III. Related Work

In this study, a taxonomy of IoT security quality attributes are identified as specified in Firesmith's framework [5] which provides a basis for reorganizing security requirements. Firesmith argued that security and privacy requirements have less variability in contrast to functional requirements which vary significantly across different application domains due to the reason that most applications that have multiple interacting components within an environment needs to satisfy certain levels of identification, authorization, data integrity, etc. We use his framework to identify and analyze the different kinds of privacy and security requirements in a structured way as well as suggesting some solutions that take into account the dynamic features of the IoT.

Roman et al. [16] provided an explicit analysis of the distributed architecture of the IoT showing the advantages and disadvantages of the distributed approach in comparison with the centralized one.

In [25], the author defined milestones of a legal framework that copes with individual's privacy and security and covers the right to information and rules on IT-security legislation.

In [11], a detailed study of the IoT vision, possible social and political issues, usages and the involved technologies were provided.

In [9], the authors proposed a trusted security architecture for the IoT considering the various aspects of trusted user module, trusted perception module, trusted terminal module, trusted network module and trusted agent module.

Several studies have been performed in order to solve the current issues of sensor networks. For example, in [17], Said et al. suggested a new Effective Data Aggregation Protocol (DAP) that addresses the limited capabilities of sensor networks: energy consumption, small memory size, scalability, etc.

IV. Security and Privacy Analysis

In our preliminary analysis, we identified the following obstacles to defining and analyzing IoT privacy and security requirements:

1) It is challenging to determine what information should be protected, when to protect it, and to whom access should be granted/restricted.
2) The IoT consists of diverse technologies and the integration of these technologies leads to unknown risks and issues [20].
3) The changing nature of the environment plays an important role when dealing with the privacy and security vulnerabilities of the IoT.

Architecting secure and reliable IoT depends on the specification of system's security policies and the establishment of security requirements models that consider the heterogeneity, scalability and high connectivity capabilities of the IoT network as well as the context of the shared information.

In our study, security is decomposed into its quality attributes and a variety of security mechanisms are discussed to alleviate the different and the new arising forms of security attacks and to reduce the vulnerabilities in the development of the IoT.

A. Managing Access Control, Authentication and Authorization

Access control mechanisms limit access to various system's resources (e.g., data, services, hardware, etc.) by identifying who can access what resources, and constrain what a legitimate user can do by controlling who is doing what in the system. Access control is necessary to prevent unauthorized entities from gaining access to system's resources, and to ensure that authorized entities can only access the resources they are allowed to access. Therefore, reliable access control policies play a major role in preventing activities that lead to a breach of security in the IoT.

Following are the security quality attributes of access control:

1) Identification: The focus of the identification is to uniquely identify objects and manage their identities while considering security and high scalability aspects of the IoT. Reaching a consensus on how to identify objects involved in the IoT and managing their identities is fundamental for constructing robust authentication and authorization mechanisms. Currently, two groups of solutions are proposed:

- Leveraging the Electronic Product Code (EPC) technology: EPC is a structured identifier used in EPC Network (a global RFID data sharing network). EPCs identify RFID transponder while EPC network and EPC Information Service (EPCIS) facilitate the storage, process and exchange of data that is captured by EPCs. Moreover, in EPCIS different levels of access management are introduced to support secure data transfer between various systems [21].
- Developing an object identity management system (IdM): Current IdM systems are composed of two types of entities: identity providers (IdP) and service provider (SP), to manage authorization and to offer access and identity management services respectively. One approach to IdM

system is *federated identity management system (FIdM)*, such as OpenID framework. OpenID allows a user to login to different websites using a single digital identity. FIdM enables seamless sharing of identity information across several security domains. Most IdM systems support Single-Sign-On (SSO) to enhance authentication and technical interoperability. SSO is a subset of FIdM; in a system which supports SSO an entity is authenticated to access multiple resources on different security domains without having more than one account [2]. Although an IdM system enhances usability and is a cost-effective way to manage identification, authorization and authentication across or within systems, security and privacy still need to be fully addressed if this approach is followed completely or partially in the deployment of the IoT[22].

2) Authentication: While authorization defines the rights and privileges after an entity gains access to a system, authentication, i.e., identity verification, plays a vital role before establishing a communication channel between two entities. In the IoT, authentication protocol should be developed to confirm mutual trust between different objects, users or systems by verifying their identities.

- Central authentication protocols: Kerberos is an example. It is considered as a time-based authentication protocol widely used for client-server application authentication. Kerberos has two main components: Key Distribution Centre (KDC) to store authentication data, and Ticket Granting Service (TGS) which keeps record of digital tickets to identify clients and servers in a network. Kirsal and et al. investigated security in Kerberos and suggested an improved protocol [8], [10].
- Peer-to-peer authentication protocols: In [4] the authors proposed an authentication scheme for wireless peer-to-peer network, where the concept of distributed super-peers is introduced to achieve mutual authentication. Further, quick re-authentication method was specified.

3) Authorization: Authorization is the process of granting, denying or limiting access to data, resources or applications within a system. One possible approach for object and user authorization in the IoT is Role-Based Access Control (RBAC). RBAC is an access management technique for multi-user and multi-application online systems. In RBAC each role has different functions, an entity can have one or more roles and management of permission is carried out based on entity's role(s). In such a scheme functions within roles can be reassigned easily and user's roles can be reallocated efficiently [18].

Anything can be connected to the IoT network to handle the growing and dynamic features of the IoT. Data Stream Management Systems (DSMS) should be used instead of static databases. DSMS enhance dynamic data storage and real-time data access rights configurations. Moreover, object owners should define how these DSMS can access their data, i.e., user-defined access control policies should be developed where accessibility levels are presented for various types of information at the object level.

B. Data Integrity

Data integrity checking protocols aim to maintain the complete structure of stored data, ensure its correctness and protect this data from lost or corruption keeping in mind economies of scale, practicality and support for dynamic data operations.

During the past decade several protocols were designed to achieve data integrity in cloud computing. These protocols use either encryption or anonymization techniques. Due to the similarities between the IoT and cloud computing when it comes to data storage, privacy and confidentiality (i.e., both systems need to maintain the integrity of growing amounts of data stored on remote servers where the data is frequently modified), the same protocols adopted for data integrity in cloud will meet the requirements of the IoT.

In [24], data integrity checking scheme is proposed using Merkel hash tree as an authentication structure together with a third party auditor to verify the integrity of a dynamically stored data. One of the disadvantages of encryption-based data integrity checking protocols is the increasing difficulty in performing computations on encrypted data. Anonymization schemes on the other hand require high computational power when performed at client's side but nonetheless, they may be an alternative solution for instance George et al. suggested a remote data integrity protocol where a secure enclave is responsible for performing anonymization and deanonymization processes [6].

C. Contextual Integrity

Contextual Integrity is an alternative notion of privacy introduced by Nissenbaum et al. [23]. In this notion, the adequate protection of individual's privacy is tied to the norms of specific contexts. More specifically, Nissenbaum argued that privacy can be fulfilled through governing the flow of personal information to assure that data gathering and dissemination are appropriate to a given context, as such privacy cannot be narrowed to merely protecting personally identifiable information [23], [7]. Accordingly, two sets of informational norms are:

1) Appropriateness norms: to determine whether a given type of personal information is appropriate within a particular context.
2) Distribution norms: to define constraints on the flow of information within or across contexts.

Before the emergence of any new technology it is difficult to clearly articulate the norms that govern the flow of personal information as several and complex contexts are involved. Thus, to help understand and articulate privacy contexts in new emerging technologies, Nissenbaum, in her privacy framework, provided a decision heuristic (a set of guidelines divided into nine steps). Her heuristic approach can be helpful in analyzing privacy concerns in the case of IoT.

D. Intrusion Detection

Building a completely secure IoT network where attacks do not occur may not be feasible or cost effective for many reasons such as the high connectivity feature of the IoT and the proliferation of heterogeneous computer networks. As a result, it is worth investigating intrusion detection mechanisms that are able to detect attacks and preferably these mechanisms can catch attacks occurring in real-time. The purpose of intrusion detection is to identify attacks aimed to disrupt the network. Such attacks may be caused by one of two types of malicious entities: those who try to access the network without authorization and insider threats, i.e., authorized entities that try to abuse their privileges [13], [15].

Intrusion detection mechanisms analyze activities in the network. Currently, two models exist:

- Signature based detection models: compare network's current behavior against predefined patterns that are known to cause security problems such as loss of confidentiality, loss of integrity, denial of resources, etc. In such models attack signatures must be stored, which results in growing storage costs with increasing number of attacks. Another disadvantage of such models is that new attacks cannot be detected unless their signatures are added manually.
- Anomaly based detection models: Ordinary behavior is determined and any deviations from the ordinary behavior is considered an anomaly. However, such models require high computational cost and suffer from relatively high false positive and false negative rates (an alarm is triggered when no attack occurs or an attack occurs but no alarm is raised respectively).

In [15] a hybrid of signature and anomaly based intrusion detection for the IoT is investigated, which specifically targets different routing attacks, e.g., sink-hole, selective forwarding.

E. Non-repudiation

Dealing with transaction disputes to assure fair exchange is a common security concern in the business field which will be engaged in the IoT. Thus, it is necessary to build in non-repudiation into the design of the appropriate transport protocol that deals with network failures and prevents a dishonest entity from cheating, deceiving about its real identity or aborting a transaction (i.e., roll-back attack) [14]. The following is a list of the main characteristics of a good non-repudiation protocol:

- Fairness: depends on reliable and resilient communication channels in addition to evidence generation, verification and processing which in most cases involve assistance from trusted third parties.
- Efficiency: trusted third parties should intervene only when errors occur.
- Timeliness: being able to complete a transaction on a specific time frame without losing fairness especially in case of transactions delay or termination.
- Policy: to define rules for evidence generation, verification, storage and use.

V. Smart Grid AMI as an IoT Scenario

Smart grid is an electricity distributed system which uses computer intelligence with advanced networking techniques (i.e., power grid integrated with Information and Communication Technology ICT) and involves various interactive domains and systems. Smart grid Advanced Metering Infrastructure (AMI) can serve as an IoT scenario due to the similarities between the two systems when it comes to high connectivity, openness to the Internet and other corporate networks, increased use of hardware, software and standard protocols, additionally both are vulnerable to various types of internal and external cyber-attacks. However, IoT applications will have greater scope and flexibility because of the higher number of involved objects in the IoT and their various types. Additionally, in smart grid example the interaction between intelligent electronic devices might be restricted, unlike the IoT, where data can flow between any connected objects in bi-directional mode and peer-to-peer communication will be supported.

In this section we apply the security taxonomy discussed previously to the smart grid AMI where we focus mainly on the security-related quality attributes of the smart grid's information domain and its data management system.

AMI leverages distributed computing and communications to construct a network where each participating node acts as a two-way flow of electricity and information that manages energy generation, consumption and storage.

A large amount of data is produced in the smart grid AMI, with various technologies such as distributed database technology, optical communication ports and login interfaces. In AMI security should be handled properly to prevent unauthorized alteration to data (e.g., electronic billing modification) and to deliver consistent and accurate data to various users, stakeholders and applications.

Following is an outline of possible security vulnerabilities and threats that may target AMI resources or data by an adversary:

- Acquiring administrative credential to access the smart meter system
- Altering data within a storage system or tempering with data flow between customers and smart meters
- Attacking the communication links (i.e., transmitted data via the Internet) by stopping the data flow or denial of service
- Modify the data collected by smart meter systems
- Man-in-the-middle attack to the data flow in the network
- Spoofing the smart meter system
- Attacking services and system resources e.g., deleting file system, undesired traffic

Table I provides a subset of security requirements that describe what AMI smart grid should do together with the related quality attribute [19].

Quality attribute	Security requirement description
Access control	Protecting system's resources and services from various attacks such as receiving wrong command
Access Control	Protecting communication servers and database systems from disruption
Authorization	Administrative interface should be accessed only by legitimate users
Authorization	Billing data should be protected from unauthorized access
Data integrity	Increasing the memory space and computational power in smart meter, remote terminal units and intelligent electronics devices to allow more flexibility in implementing sophisticated security features
Data integrity	Transferred data should not flood in communication links
Authentication	Connected smart meters should not be allowed to use the same password
Authentication	Interacting with users should only occur after verifying their identities
Contextual Integrity	users should have an option to configure and monitor their transferred data

TABLE I
A TAXONOMY OF SECURITY REQUIREMENTS IN SMART GRID AMI

VI. CONCLUSION

In summary, analyzing security and privacy requirements in complex systems, such as the IoT systems, is essential in preventing failures and ensuring wider customer acceptance. We constructed a simple taxonomy that provides support for more investigation of expected privacy and security vulnerabilities and threats in the IoT.

It is worth pointing out that testing before adopting the existing security mechanisms and policies is a must in order to avoid any catastrophic failure in the future such as the Heartbleed bug, the vulnerability which was found in the OpenSSL cryptographic library in April 2014, and enabled attackers to read sensitive data from web servers like private keys and users' session cookies and passwords [26].

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787–2805, Oct. 2010.

[2] A. Bhargav-Spantzel, A. Squicciarini, and E. Bertino. Trust negotiation in identity management. *Security Privacy, IEEE*, 5(2):55–63, March 2007.

[3] M. Buettner, B. Greenstein, A. Sample, J. R. Smith, and D. Wetherall. Revisiting smart dust with RFID sensor networks. In *Proc. 7th ACM Workshop on Hot Topics in Networks (Hotnets-VII)*, Calgary, Alberta, Canada, 2008.

[4] G. Chen, H. Chen, L. Xie, G. Song, and T. Zhuang. An identity authentication scheme in wireless peer-to-peer network. In *Communication Technology (ICCT), 2010 12th IEEE International Conference on*, pages 473–476, Nov 2010.

[5] D. G. Firesmith. Analyzing and specifying reusable security requirements. In *Proc. Solid Freeform Fabrication Sym*, pages 507–514, 2003.

[6] R. George and S. Sabitha. Data anonymization and integrity checking in cloud computing. In *Computing, Communications and Networking Technologies (ICCCNT),2013 Fourth International Conference on*, pages 1–5, July 2013.

[7] F. S. Grodzinsky and H. T. Tavani. Privacy in "the Cloud": Applying Nissenbaum's Theory of Contextual Integrity. *SIGCAS Comput. Soc.*, 41(1):38–47, Oct. 2011.

[8] Y. Kirsal and O. Gemikonakli. Improving kerberos security through the combined use of the timed authentication protocol and frequent key renewal. In *Cybernetic Intelligent Systems, 2008. CIS 2008. 7th IEEE International Conference on*, pages 1–6, Sept 2008.

[9] X. Li, Z. Xuan, and L. Wen. Research on the architecture of trusted security system based on the internet of things. In *Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on*, volume 2, pages 1172–1175, March 2011.

[10] J. Liu, Y. Xiao, and C. Chen. Authentication and access control in the internet of things. In *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on*, pages 588–592, June 2012.

[11] F. Mattern and C. Floerkemeier. *From the Internet of Computers to the Internet of Things*, volume 6462 of *LNCS*, pages 242–259. Springer, 2010.

[12] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7):1497–1516, Sept. 2012.

[13] B. Mukherjee, L. Heberlein, and K. Levitt. Network intrusion detection. *Network, IEEE*, 8(3):26–41, May 1994.

[14] J. A. Onieva, J. Zhou, and J. Lopez. Multiparty nonrepudiation: A survey. *ACM Comput. Surv.*, 41(1):5:1–5:43, Jan. 2009.

[15] S. Raza, L. Wallgren, and T. Voigt. Svelte: Real-time intrusion detection in the internet of things. *Ad Hoc Networks*, 11(8):2661 – 2674, 2013.

[16] R. Roman, J. Zhou, and J. Lopez. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10):2266–2279, July 2013.

[17] A. M. S. Said, A. W. Ibrahim, A. Soua, and H. Afifi. Dynamic aggregation protocol for wireless sensor networks. *2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA)*, 0:356–361, 2013.

[18] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman. Role-based access control models. *Computer*, 29(2):38–47, Feb 1996.

[19] H. Suleiman, K. Ahmed, N. Zafar, E. Phillips, D. Svetinovic, and O. de Weck. Inter-domain analysis of smart grid domain dependencies using domain-link matrices. *Smart Grid, IEEE Transactions on*, 3(2):692–709, 2012.

[20] A. Sutcliffe and P. Sawyer. Requirements elicitation: Towards the unknown unknowns. In *Requirements Engineering Conference (RE), 2013 21st IEEE International*, pages 92–104, 2013.

[21] F. Thiesse, C. Floerkemeier, M. Harrison, F. Michahelles, and C. Roduner. Technology, standards, and real-world deployments of the epc network. *Internet Computing, IEEE*, 13(2):36–43, March 2009.

[22] A. Vapen, D. Byers, and N. Shahmehri. 2-clickauth optical challenge-response authentication. In *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, pages 79–86, Feb 2010.

[23] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li. Privacy as contextual integrity. *Washington Law Review*, 2004.

[24] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li. Enabling public auditability and data dynamics for storage security in cloud computing. *Parallel and Distributed Systems, IEEE Transactions on*, 22(5):847–859, May 2011.

[25] R. H. Weber. Internet of things - new security and privacy challenges. *Computer Law & Security Review*, 26(1):23 – 30, 2010.

[26] Wikipedia. Heartbleed — Wikipedia, the free encyclopedia.