# The Internet of Things Security Challenges: Survey

Inès Beggar[1]and Mohamed Amine Riahla[1]

[1] M'hamed Bougara University, Avenue de l'indépendance, Boumerdès, 35000, Algeria
i.beggar@univ-boumerdes.dz
ma.riahla@univ-boumerdes.dz

**Abstract.** The Internet of Things (IoT) and its security issues are gaining interest in recent years. It is more than necessary to take charge of them as soon as possible and to find specific solutions to the IoT. These allow it to wait for its full maturity and to take advantage of the simplicities it brings to our daily life. But to do so, it is necessary to identify and the master ins and outs of the problem which is developed in the present work. However, this paper aims on the one hand to present the Internet of Things in point form, and on the other hand to address the security of the same points as the presentation of the IoT. Moreover, the properties of the IoT are discussed and compared to traditional networks, also the level of security required according to the area of application and security from a point of view; actors of the IoT ecosystem. Besides, the existing architectures are examined in order to allow future research to self-positioning and better understand the security issue.

• **Keywords:** Internet of Things, Security, Actors of IoT ecosystem.

## 1 Introduction

The world is now digital. Cell phones with all kinds of sensors and applications are commonplace, pets with collars, autonomous cars, industrial plants, heart sensors, cameras, and so on. It seems that everything is connected and in every field, the number of online devices that work together is only growing. According to Huawei estimation, around 100 billion devices will be connected by 2025 [1]. This type of connectivity goes by the name of "Internet of Things" (IoT), which is becoming part of our daily life. The Internet of Things can be described as the interconnection of physical objects via embedded computing devices such as sensors, software, and network connectivity that allows these objects to collect and exchange data [2].

Society is becoming more and more connected to the IoT infrastructure and humans are endlessly interacting with its objects, which is driving the rapid development and commercialization of new IoT devices. The number of devices is growing exponentially creating an increase of the number of security threats and privacy expectations. This can negatively impact our lives as the damage caused by a cyber-attack in such a context has a far greater impact than those caused by the intrusion; data theft or denial of service we experience today.

The future of IoT can be jeopardized if the security aspect is not quickly taken care of. So, the protection of devices becomes essential although it poses many challenges. The first is to be able to protect the elements of a very heterogeneous IoT environ-

ment. It can integrate entities of very variable origin, a multitude of platforms, protocols, specifications must coexist [3]. The second challenge is that IoT is accepted as an extended version of some different technologies including wireless sensor networks [2], which already have various security flaws making it vulnerable to wireless security attacks such as denial of service, eavesdropping, message injection, spoofing, and jamming [4]. The third is that one cannot apply a common security solution to all IoT devices. A security solution suitable for one IoT device may not be suitable for another. But also, how to define who is responsible for the security of an IoT device; knowing that it is designed, supplied and deployed by different companies. Finally, IoT devices are lightweight, limited in sources such as energy; storage capacity (memory), and computational power. Most traditional network security countermeasures are based on gluttonous algorithms and resource intensive protocols. Thus, it will be very difficult to implement these solutions on IoT devices [3]. To overcome this kind of issue; it is essential to already understand the IoT ecosystem with all its complexity and security requirements, to identify the domain and scope of application and its sensitivity, as well as the vulnerabilities of each party in order to propose a coherent and adapted security policy based on technical solutions; such as the one that use low-cost protocols, greedy computation algorithms that can provide strong authentication and encryption to IoT devices. This is the interest of drawing up a state of the art on security in Iot, which is the objective of this work.

The present paper is organized in two main parts. The first part defines the Internet of Things in section, describes the properties of IoT, the domains, and scope of application. Moreover, the actors of the IoT ecosystem are presented in this part with the analysis of the architecture and technology of IoT. The second part details the concepts of security related to IoT. However, after the definition and presentation of the families of risks, the security will be approached according to points of view, which will be only the points treated previously such as the properties of IoT compared to traditional networks, the level of security required according to the application domain, the security from the point of view of the IoT ecosystem actors, and the security in relation to the architecture and technologies.

## 2 Definition

The IoT for "Internet of Things" is a buzzword. It is first coined in 1999 by Kevin Ashton, executive director of the Auto-ID Center at the Massachusetts Institute of Technology. The term has been widely adopted but there is no unanimously accepted definition of it. However, the common point between all definitions is that the first version of the Internet connected computers or data created by people, while the Iot connects objects or data can be created by objects (see Fig. 1). An object by definition is a physical or virtual machine, which has a capacity of calculation and memorization; therefore 'intelligent', 'autonomous', not requiring human intervention for a treatment and which can be 'connected' with any object in a transparent and flexible way [5]. A smartphone, a smartwatch, a connected television or systems of detection of presence, and so on, constitute concrete examples of connected objects.

The CERP-IoT "Cluster of European Research Projects on the Internet of Things" defines the Internet of Things as: "The Internet of Things is an integral part of the Internet of the future. It could be defined as a dynamic global network infrastructure with self-configuring capabilities based on interoperable communication standards and protocols, where physical and virtual "objects" have identities, physical attributes, virtual personalities and use intelligent interfaces, and are seamlessly integrated into the network" [6].

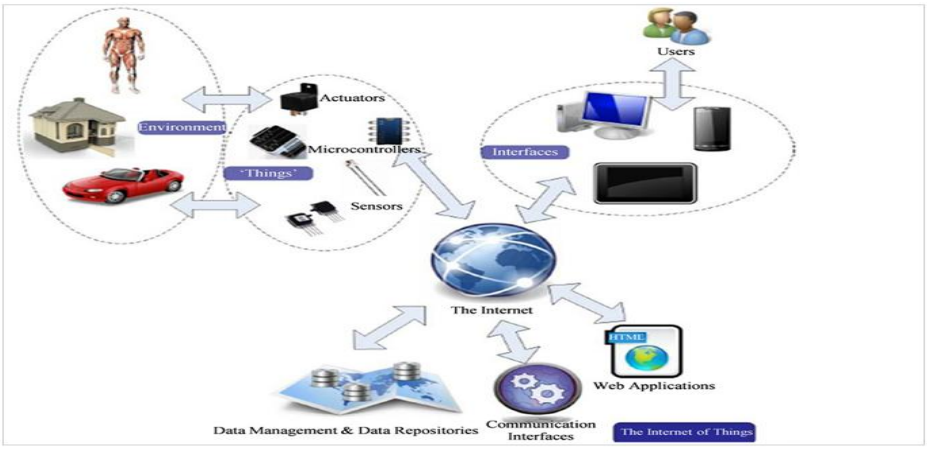


**Fig.1.**Illustration of internet of things [7]

## 3 IoT properties

For the IoT to be fully realized; a number of challenges must be addressed while considering the combination of IoT properties making it unique. Vasilomanolakis et al. [8] identified four distinctive properties: the uncontrolled environment, heterogeneity, the need for scalability, as well as the limited resources used in IoT: 1) Limited resources in terms of energy (battery), computing capacity (micro sensors) and storage space (memory) to be taken into account for security mechanisms.2) The IoT is an uncontrolled environment mainly due to the mobility of objects, the extended possibilities to access them physically and the lack of trust. 3) Heterogeneity: anIoT environment can integrate entities from very different origins (different platforms, communication protocols, suppliers ...) to take into account the compatibility of versions and interoperability.4) Scalability related to the quantity of objects that can be interconnected. It requires highly scalable protocols and influences the security mechanisms.

## 4 Areas and scope of application

The rapid growth of IoT technology and the high potential it promises if it reaches full maturity will disrupt modern life as we know it and transform every aspect of our daily lives [9]. In other words; the IoT will eventually touch almost every area of our

daily lives and cover a wide range of applications. Table 1 gives an overview of some of the main areas and sectors of application of IoT[10].

**Table 1.**Examples of IoT application areas.

| IoT application domains |
|---|
| Army |
| Energy |
| Automotive |
| Telecommunications |
| City Management/ Urbanism/ Intelligent Buildings |
| MedicalTechnology, Healthcare |
| Pharmaceutical |
| Logistics, Supply Chain Management and Retail |
| Manufacturing, Product Lifecycle Management |
| Oil and Gas |
| Safety, Security, Privacy and Recycling |
| Environment Monitoring |
| People and Goods Transportation |
| Agriculture and Breeding |
| Insurance |

When implementing a proper IoT security solution, it is critical to determine the scope of the system. Some IoT systems operate primarily on a local scale, e.g. smart homes that are largely autonomous. Other systems operate on a cosmopolitan scale, example: a system of sensors deployed across continents and collecting environmental data could feed into devices to analyze climate change or phenomena [9]. However, the data collected at a (local) scale could be integrated into a larger (macroscopic) system.

In addition, Iot systems can also be integrated into systems of systems and sometimes span more than one domain. Data collected from one domain can be used in another domain and play a role in strategic decision making; e.g. in the management of the Coronavirus 2019 health crisis, data from the air transport system, originally collected as part of the management of passenger flows, was combined with data from health systems to track the spread of the disease from one region to another.

## 5 Actors of the IoT ecosystem

The actors of the IoT ecosystem can be distinguished into two main categories: the manufacturers and the users whose priorities are different. The manufacturers are the economic actors, from different sectors including industry. Its main actors are: designers and manufacturers of connected objects, manufacturers of computer components for these objects, operators and managers of data flow transmission networks, managers of data collection and processing platforms, designers of software interfaces between objects and users, service providers who collect, analyze, and exploit user data provided by connected objects, public regulators, ensuring compliance with laws

in terms of respect for life and private data, as well as security standards for connected objects. Manufacturers' priorities are linked to several factors, including cost, preservation of the brand's image, the ability to scale up regardless of the number of users, and the identification of the objects, so that the data collected can be associated with them and value-added analysis can be performed. Several profiles are identified for users: companies, local authorities, craftsmen, or "simple" individuals who use objects on the move or at home. The priorities of users, considering their profiles, converge on several dimensions, from the price knowing that the IoT market is very competitive, to the respect of the confidentiality of information, moreover users have gained in maturity and take more and more security into consideration during acquisitions [11, 12] as well as the regulatory context which is more and more restrictive. Reliability is also considered a priority with a level of sensitivity that depends on the user's profile, his sensitivity to security issues, and also on the application domain.

We suggest considering a third actor "the authorities" in view of the important role this function plays in the future development and emergence of IoT, bringing together policy makers, public regulators, regulatory bodies and industry alliances developing standards and guidelines to secure IoT devices [11-15]. As an example, we cite the National Information Security Reference System 2020 'L06-Final version of the RNSI 2020' which applies to administrations and public sectors, as well as any infrastructure hosted on the Algerian national territory and dealing with sensitive information according to the laws and regulations in force, proposed by the Algerian Ministry of Post and Telecommunications (MPT), It provides through a set of recommendations an approach to securing information based on risk management with regard to the confidentiality, integrity and availability of information The security measures related to the Internet of Things are defined in domain 12 of the standard.

## 6 Architectures and technology

The Internet of Things, due to its complexity and peculiarities, is very broad and unlimited, which is a major problem in the implementation of its concept. There is no uniform architecture that can be applied to all domains. The development and proper functioning of IOT involves an assortment of several technologies such as RFID [16], wireless sensors and actuators, networks, protocols, machine-to-machine (M2M) communications [17], and computing, among others [18]. Researchers, authors and practitioners have proposed several architectures, the most answered is presented.

The four-layer architecture, we synthesize the works published in the literature [2, 15] and [19] presenting an architecture that can be extended to the actual development of applications and guide theoretical research(see Fig 2.). The perception (physical) layer: using its sensors, it interconnects and identifies unique devices and provides the discovery service [2, 11] collecting information from the physical world [20].The network layer: is responsible for the communication and connectivity of all devices in the system and the transfer of information collected by them to an information processing system using several protocols. It consists of network interfaces, communication channels and others. The support layer (middleware): It acquires data from the

network layer, connects the system to the database or cloud to store the data, and also involves information processing systems that take the information in one form and transform it into another form. It also meets the requirements of the application layer by providing APIs. And the last layer, the Application (Service) Layer: provides practical applications developed according to user requirements or industry specifications. In other words, it provides specific services to end users [12], hence the designation service layer.

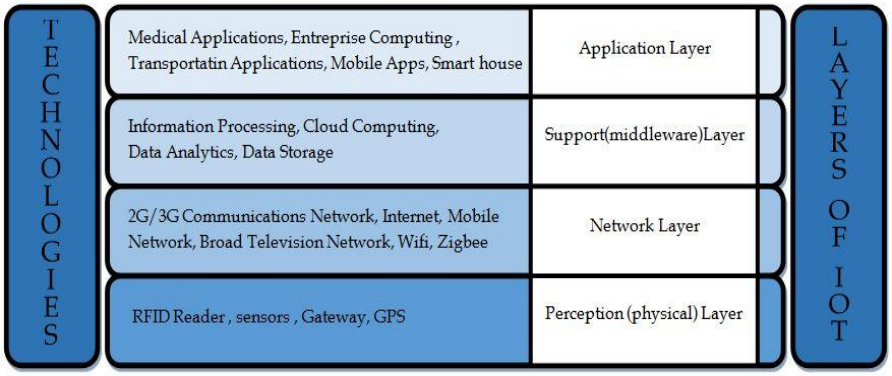


**Fig.2.**IoT Architecture

1) sensor technology, intelligence embedded technology, nanotechnology and RFID are located in the perception/physical layer.2) Fiber optic and 2G / 3G communication networks, Wifi, Zigbee, large TV networks, fixed telephone networks and others are located in the network layer.3) Databases and the cloud are located in the support/middleware layer.4) Specific applications and system integration are located in the application/service layer, e.g. smart traffic, smart home, etc.

## 7 The Security

IoT security is defined in the work of Hammi in 2018 [5] as ensuring the proper functioning of a system and guaranteeing the expected results of its design. The set of policies and practices adopted to monitor and prevent misuse, unauthorized access and modification or denial of a computer operation thus represents security. The threat of cyber-attacks makes IoT security one of the major issues, which hinder the rapid deployment and evolution of this technology of technologies.

The impact in case of an attack is varied [21], the impact differs according to the type, use and functionality of the objects. The families of risks are common to all of them, from denial of service, to loss of confidentiality and integrity of measurements made by sensors, to leakage of personal data, or even worse, to breach of personal safety [9]. The three main categories: Privacy risks, Systemic risk and Other risks associated with poorly secured IoT devices.

In what follows; security will be discussed from different perspectives.

7

### 7.1 From a point of view: properties of IoT and the security of traditional networks

IoT systems coexist with traditional systems in the same computer networks, they are faced with various cyber-attacks. To cope with the many security threats that affect computer networks; many security solutions applicable to different parts of the networks have emerged (firewalls and segmentation).The properties of IoT systems have limitations in front of the security techniques and solutions used by the traditional methods for the protection of traditional networks; such as isolation, device-level protection and network-level protection [15].Examples of these limitations are given.- Resource limitation of an Iot device (low energy; limited memory and computing power) makes it vulnerable to even the simplest attacks. Security solutions applied for device-level protection in traditional computer networks such as anti-virus or anti-malware cannot be adopted. Interoperability is the cohabitation of disjoint devices, systems and mechanisms and the possibility to make them cooperate and interact in all flexibility. Its most basic form is the accessibility of IoT objects from traditional computer networks. But the coexistence of vulnerable and insecure IoT devices and non-IoT devices is unavoidable in some cases or bridges between the two initially isolated networks are builtand eventually compromises the security of the entire enterprise network.- Heterogeneity: the heterogeneous nature of IoT systems and device types: each with its own behaviors and vulnerabilities; it is difficult for devices used for network-level protection such as a firewall or IDS appliance to distinguish between normal traffic and abnormal traffic that could be symptomatic of an attack.- Scalability: it is difficult to monitor each individual device using traditional techniques; this leads to increased maintenance costs. Also, centralized approaches, such as hierarchical public key infrastructures (PKI), and distributed approaches, such as pairwise symmetric key exchange systems, cannot scale with the IoT.

From what has been presented, it can be seen that the security problems in both networks can be similar, but different approaches and techniques are used to address each security problem depending on the network [22]. The existing conventional security architecture is limited and does not meet the properties of IoT. Therefore, it is essential to develop specific security solutions for objects with strong resource constraints having multiple wireless communication methods. e.g. of a solution, we need to design a protocol based on robust algorithms, but at the same time light and flexible, adaptable to different types of objects, from the weakest to the most powerful without degrading the security performance

### 7.2 From a point of view: area and scope of application

From what was presented in Section 4, it is clear that IoT infrastructures can almost touch all areas of our daily lives and cover a wide range of applications and but also have different scopes, so it becomes difficult to impose a standard in all these areas, as the security requirements of a home network may be different from those of a critical infrastructure [15]. Furthermore, it would be more prudent to secure the most critical parts of the IoT, namely those in sensitive areas such as the military and critical infrastructure, rather than consumer goods [9]

In addition to the application domain; determining the scope of an IoT system can tell us about the complexity of its architecture; whether its operation is at a local scale or integrated into systems of systems the security solution to be implemented will be according to its functional architecture.

### 7.3 From a point of view: actors of the IoT ecosystem

In order to reduce IoT-related cyber threats, security must be considered and assessed by all stakeholders (manufacturers, users, authorities and service providers).each as it relates to them. Manufacturers include constructers (designers and manufacturers of connected objects, and manufacturers of computer components of these objects) and service providers (operators and managers of data flow transmission networks, managers of data collection and processing platforms) as well as public regulators. We have proposed to consider a third actor in its own right "authorities" and we will distinguish the service providers in what follows from the manufacturers in relation to the requirements of more concerning them.

Manufacturers are under competitive pressure for cheaper products and shorter time-to-market; especially since there are no credible means (trustmarks, certifications, ...) for consumers to distinguish the security level of one vendor from another and cyber security skills and security testing are scarce, however, failing to react to threats will tarnish the brand image. IoT service providers are required to support the security of IoT systems which is an expensive task without the ability to quantify the security assurance provided.

Users are consumers of IoT technology; Property or enterprise managers, network managers, although these users follow strict procedures when purchasing and install in their networks only secure devices with strong encryption and proper maintenance according to the regulatory recommendations in force; they remain victims of limited skills for network monitoring; lack of sufficient knowledge; inadequate operational testing; lack of automatic resource management; which results in the installation of vulnerable devices in their networks.

Authorities: Standards and guidelines are developed by authorities; they pose other major challenges [15]: (a) limited attention to security: the system is potentially vulnerable because the standards are limited to a subset of the security aspect and create a partially trustworthy environment, (b) imprecision: the recommended guidelines are qualitative and subject to human interpretation, (c) lack of legacy support: devices that are already on the market are not regulated, the implementation of alternative solutions to control them must be provided by the regulators and (d) lack of mandate: the difficulty of imposing a standard in all of these areas has been demonstrated above.

### 7.4 From a point of view: Architectures and technology

Based on the variety, richness and specificities of the technologies located in the layers of the architecture models, the architecture of an IoT solution varies from one system to another based on multiple criteria: 1) the communication technology used (M2M or M2H);2) the data processing in the cloud (computing power) or relying on local computing capabilities (computing speed) or relying on other smart devices in the vicinity; 3) the type of object used; physical object equipped with IoT element or

digital object existing in the real world; the smart object communicates directly with the cloud or indirectly. The technological portfolio and the flexibility in the IoT architecture seem to offer infinite possibilities of IoT system solutions. The security to be implemented for IoT will strongly depend on its architecture; the technologies employed, but also its scope and the sensitivity of its application domain for the choice of the crucial parts to secure. We limit ourselves in our study to these conclusions; for the implementation of security there are multiple solutions in the literature; we cite as an example and according to the layers of the IoT architecture; the work of Leloglu[2] which classifies all types of security threats that can be critical in the development and implementation of IoT in different domains, and provide recent solutions to these threats. This could be the subject of our future research. Nevertheless, we return to the data-centric approach to security, its primary focus is the protection of (valuable) data since there will always be a way to penetrate systems even using the best cyber security tools. Understanding the infrastructure; flows and risks related to data is essential but so is the classification of sensitive data, while monitoring and controlling its use.

## 8 Conclusion

A lot of researches have been established IoT security in recent years, however, there are still many key issues that need more effort to be resolved. The importance of security in the development of the Internet of Things, which does not only depend on the possibility to make cooperate intelligent and autonomous objects with connection means or to make this technology adapt to our lives in all areas of everyday life. It is essential that reliable and above all secure infrastructures, harmonization, IoT security guidelines, and recommendations exist simultaneously to stimulate their adoption. It is important that standardization processes remain aligned with the technology.

In this article, the first part was devoted to the Internet of Things, which was discussed in detail in the form of points: its definition, its properties, the domains and scope of application, the actors of the ecosystem, and its architecture were exposed. Different technologies were located in the layers of the architectural models presented to get on a functional architecture. In the second part, it is the security concepts of the IoT that were largely reviewed according to the same points exposed in the first part. The properties of IoT compared to traditional networks, the level of security required according to the application domain and the security from the point of view of the actors of the IoT ecosystem were discussed.

### References

[1] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, D. Aharon, The Internet of Things: Mapping the value beyond the hype, (2015).

[2] E. Leloglu, A review of security concerns in Internet of Things, Journal of Computer and Communications, 5 (2016) 121-136.

[3] F. Restuccia, S. D'Oro, T. Melodia, Securing the internet of things in the age of machine learning and software-defined networking, IEEE Internet of Things Journal, 5 (2018) 4829-4842.

[4] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, Y. Jin, Internet-of-things security and vulnerabilities: Taxonomy, challenges, and practice, Journal of Hardware and Systems Security, 2 (2018) 97-110.
[5] M.T. Hammi, Sécurisation de l'Internet des objets, in, Paris Saclay, 2018.
[6] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realising the Internet of Things, Cluster of European research projects on the internet of things, European Commision, 3 (2010) 34-36.
[7] M.S. Mahmoud, A.A. Mohamad, A study of efficient power consumption wireless communication techniques/modules for internet of things (IoT) applications, (2016).
[8] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, P. Kikiras, On the security and privacy of Internet of Things architectures and systems, in: 2015 International Workshop on Secure Internet of Things (SIoT), IEEE, 2015, pp. 49-57.
[9] M. Tonin, The internet of things: Promises and perils of a disruptive technology, Science & Technology Committee, NATO Parliamentary Assembly, (2017).
[10] Y. Challal, Sécurité de l'Internet des Objets: vers une approche cognitive et systémique, in, Université de Technologie de Compiègne, 2012.
[11] I. Andrea, C. Chrysostomou, G. Hadjichristofi, Internet of Things: Security vulnerabilities and challenges, in: 2015 IEEE symposium on computers and communication (ISCC), IEEE, 2015, pp. 180-187.
[12] A. Dean, M.O. Agyeman, A study of the advances in iot security, in: Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control, 2018, pp. 1-5.
[13] M. Fagan, K. Megas, K. Scarfone, M. Smith, Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (2nd Draft), in, National Institute of Standards and Technology, 2020.
[14] I.A. Australia, Strategic Plan to Strengthen IoT Security in Australia, in, 2017.
[15] A. Hamza, H.H. Gharakheili, V. Sivaraman, IoT network security: Requirements, threats, and countermeasures, arXiv preprint arXiv:2008.09339, (2020).
[16] H. Stockman, Communication by means of reflected power, Proceedings of the IRE, 36 (1948) 1196-1204.
[17] V. ETSI, Machine-to-machine communications (M2M): Functional architecture, Int. Telecommun. Union, Geneva, Switzerland, Tech. Rep. TS, 102 (2011) 690.
[18] M. Gigli, S.G. Koo, Internet of things: services and applications categorization, Adv. Internet Things, 1 (2011) 27-31.
[19] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of Things security: A survey, Journal of Network and Computer Applications, 88 (2017) 10-28.
[20] M.U. Farooq, M. Waseem, A. Khairi, S. Mazhar, A critical analysis on the security concerns of internet of things (IoT), International Journal of Computer Applications, 111 (2015).
[21] C. Hantouche, Peut-on sécuriser l'Internet des Objets?, Sécurité et stratégie, 22 (2016) 31-38.
[22] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, M.A. Spirito, An IDS framework for internet of things empowered by 6LoWPAN, in: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013, pp. 1337-1340.