The Internet of Things: Vision & Challenges

Mahmoud Elkhodr, Seyed Shahrestani and Hon Cheung
School of Computing Engineering and Mathematics
University of Western Sydney
Sydney, Australia

***Abstract*— The Internet of Things (IoT) was of a vision in which all physical objects are tagged and uniquely identified using RFID transponders or readers. Nowadays, research into the IoT has extended this vision to the connectivity of Things to anything, anyone, anywhere and at anytime. The IoT has grown into multiple dimensions, which encompasses various networks of applications, computers, devices, as well as physical and virtual objects, referred to as things or objects, that are interconnected together using communication technologies such as, wireless, wired and mobile networks, RFID, Bluetooth, GPS systems, and other evolving technologies. This paradigm is a major shift from an essentially computer-based network model to a fully distributed network of smart objects. This change poses serious challenges in terms of architecture, connectivity, efficiency, security and provision of services among many others. This paper studies the state-of-the art of the IoT. In addition, some major security and privacy issues are described and a new attack vector is introduced, referred to as the "automated invasion attack".**

***Index Terms*—Internet of Things, RFID, Smart Objects, Ubiquitous Computing.**

I. Introduction

The definition of the Internet of Things (IoT) is still rather fuzzy and subject to debate. It may vary from ambient intelligence, ubiquitous computing, pervasive computing, smart cities, telematics, and recently everyware, to name but a few. In China and Europe, the term IoT is widely accepted. While in the US, it is more commonly referred to as smart object or smart grid. In this work, we agree to this multiplicity to ensure a common definition of what the term IoT encompasses. In 2005, the International Telecommunications Union (ITU) published their first report on the IoT [1]. The report adapted a comprehensive and holistic approach by suggesting that the Internet of Things would connect the world's objects in both a sensory and intelligent manner through combining technological developments in item identification, embedded systems, sensors, wireless networks and others. In July 2012, the ITU approved a new standard offering a definition for the Internet of Things (IoT). It stated: "a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies" [2].

Originally, the term IoT was first mentioned in 1999 by the founders of the original MIT Auto-ID Center [3]. Auto-ID refers to any broad class of identification technologies used in the industry to automate, reduce errors, and increase efficiency [4]. These identification technologies include smart cards, barcodes, biometrics, sensors and voice recognition. Therefore, the initial vision of the IoT was to tag physical objects, using RFID tags, and to uniquely identify those objects using RFID transponders or readers. This mechanism enabled users to identify and track objects. As Neil Gershenfeld noted as early as in 2000 that the price for RFID tags would continue to decrease. Today, prices for individual RFID tags have dropped below one cent, making their adoption within diverse business areas not just technically possible but economically feasible as well [5].

Nowadays, the concept has evolved to accommodate the perception of realizing a global infrastructure of interconnected networks of physical and virtual objects. The current advance in technologies has extended the vision of the IoT by encompassing other technologies such as sensor networks. The IoT has now more potential to provide a real-world intelligent platform for the collaboration of distributed smart objects via local-area wireless and wired networks, and/or via a wide-area heterogeneous network interconnection such as the Internet. This growth is inspired not only by the success of RFID technology, which is now widely used for tracking objects, animals and people [6], but also by the advance of wireless and communication networks, such as 4G, LTE and WiiMax, and their wide-range wireless connection capabilities. It is evident with the widespread use of smart phones, smart TVs, and smart fridges that IoT communication networks and application are in rapid development. Additionally, earlier form of IoT instances started to develop, mainly those which provide information services through centralized systems with remote access capabilities.

New service providers are providing a centralized interface, mainly based on smart phone or a server, to access raw sensor data worldwide. Such data can help launching

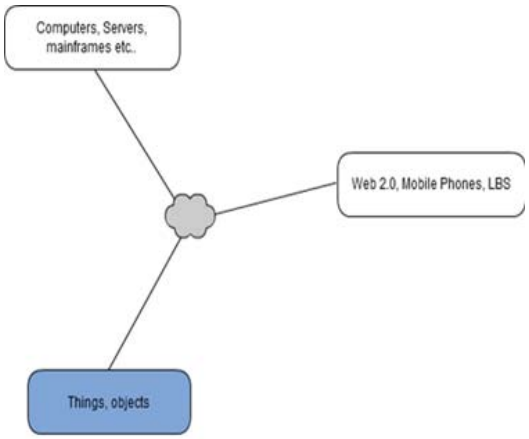

Figure 1. Objects: an added dimension to the Internet

various IoT applications. The personal network or smart environment paradigm are another examples of earlier form of the IoT.

The remainder of this paper is structured as follows: the next section introduces objects in the IoT. Section 3 discusses the key issues and challenges facing the IoT. Section 4 details the security concerns found in the IoT with a special concentration on location privacy. That section also reports security attacks on privacy envisioned in the IoT. Concluding thoughts are presented in Section 5.

II. OBJECTS IN THE IOT

The IoT extends the existent interactions between humans and applications to a new dimension of communication via objects which can be users or applications. Therefore, IoT is expected to be seen everywhere and in numerous application domains, such as manufacturing, logistics, service sector, agriculture, recycling, environmental management, intelligent homes and others. This technological revolution adds a new dimension to the Internet bringing connectivity to "objects", as shown in Fig1.

The advancement of technology and the extension capabilities of devices have led to the introduction of smart objects. In contrast to RFID tags, smart objects are expected to be able to execute applications, sense their local situation and communicate with other objects or human users. In homes, as an application domain example, a ubiquitous network of autonomous mobile devices with physical sensors, which combine advances in sensor miniaturization, wireless communications, and micro-system technology, can make accurate measurements of environmental parameters (temperature, humidity, light etc.) [7]. Rather than always interacting with the human users, objects will be interacting with each other automatically, performing actions on behalf of the users and updating their daily schedules. Devices will enter the world of the Internet, for the most part, through local-area wireless or wired networks. A smart object topology can incorporate two design dimensions [8]:

(1) Awareness: It is where an object has the ability to sense or interpret events and users' activities in the real world.

(2) Interaction: It is where an object has the ability to communicate with users (input/output and feedback) or other objects. In the IoT, objects could be part of the physical world (physical things) or of the information world (virtual things), which is capable of being identified and integrated into the communication networks [9].They range from simple connected objects, such as sensors on a sensors network, to more complex and smarter communicated objects on the Internet [10].

Therefore, an object in the IoT is regarded to as any machine, device, application, computer, virtual or physical object involved in a communication that could connect to the Internet, and could have the ability to create, request, consume, forward or have access to digital information.

III. THE IOT: ISSUES AND CHALLENGES

The first issue to consider is how objects will join the

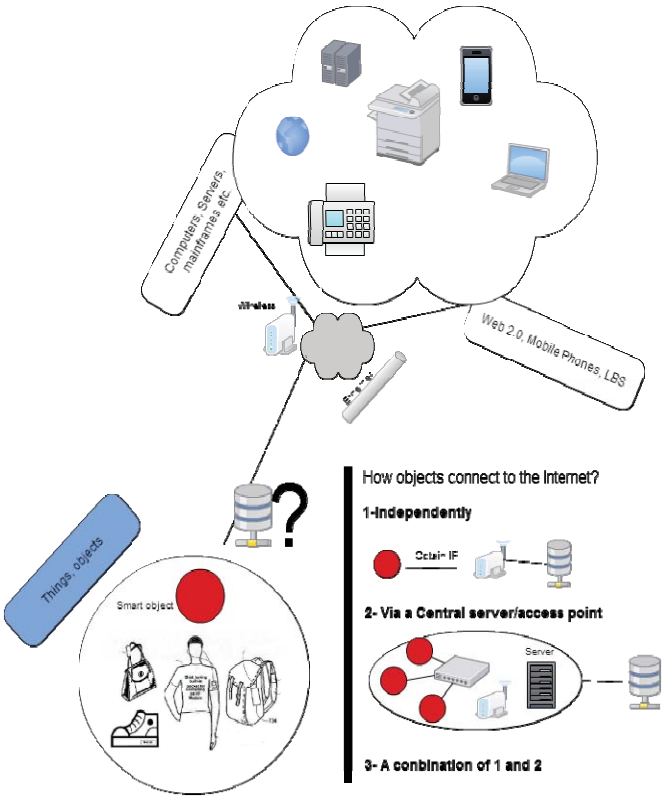

Figure 2. How Objects Connect to the Internet

Internet. As illustrated in Fig. 2, there are two ways for a typical computing device to connect to the Internet: (1) independently using a mobile broadband connection to an Internet Service Provider (ISP). Two popular examples are a laptop equipped with a mobile broadband modem and a mobile device that connect to the Internet via 3G that has an in-built modem; and (2) via a local-area wireless or wired network which is connected to a base station or a router. Examples are local area networks (LANs) that connect computers and devices, within the same geographical area together. Each device on the network is regarded as a node with one of them designated as a gateway. A gateway computing device, for instance, acts as a router, sharing Internet connection to other nodes. For the realization of both (1) and (2), these devices rely on a communication protocol for exchanging information over a network; normally the TCP/IP protocol suite. These devices are uniquely identified (via IP or MAC) by the communication protocols. However in the IoT, objects need to be identified uniquely by IoT applications on the Internet. This opens the door for numerous issues such as identifying objects, name space, object addressing and the need for a global unique ID.

A. Object naming

Currently, DNS is the Internet naming service that translates the IP addresses into human friendly host names. Object name service is among the essential and key elements in the IoT that need to be researched. The IoT will include a large number of objects which are considered on the network as nodes, each of which will produce contents that should be

retrievable by authorized users or objects. This requires effective object addressing or naming policies. Additionally, the characteristics of the traffic exchanged by smart objects, in the IoT, remain unknown at least for now. Further contributions are required to determine if the TCP protocol is adequate to use in the IoT or if a new concept of a transport layer is required. This is due to the fact that the TCP protocol is connection-oriented, by which a communication session starts with a connection setup procedure known as the three handshake. Given that some of the communications within the IoT will involve the exchange of only small amount of data generated from constrained devices, the TCP protocol cannot be used efficiently for transmission control. For example, if the amount of data, generated by an object, to be exchanged in a single session is very small, the TCP congestion control is considered to be ineffective, given that the whole TCP session will be concluded with the transmission of the first segment and the consequent reception of the corresponding acknowledgement message [11].

B. Interoperability

In typical computing environments, computing devices are treated equally when they are connected to the Internet. Their functionalities vary depending on how users use them. However, in the IoT, each object would be subject to different conditions such as power availability and communication bandwidth requirements. In addition, objects on the IoT might be made by different manufacturers that do not necessarily comply with the same standards. This difference results in heterogeneous devices that might not be able to communicate directly with each other, raising integration issues. Service description, common practices, standards and discovery mechanisms should be interoperable to allow interactions between different objects.

C. Inidentity Management

Identity management systems have been already identified by previous researchers, for instance see [12], as an essential component in the successful operation of the IoT. In the recent years, many frameworks for identity management have been developed, e.g. Open ID. OpenID describes how users can be authenticated in a decentralized manner. This decentralized technique allows users to process their digital identities quickly and reliably. Also, it eliminates the need of deploying independent ad-hoc identity management systems by the service provider. In any of these authentication processes, there is a need of preserving users' privacy in the IoT where most of the entities may be untrusted.

IV. Security and privacy

The IoT's highly distributed nature of technologies, such as embedded objects in public areas, create weak links that malicious entities can exploit and can as well open the door for a mass surveillance, tracing, tracking, and profiling of the users' movements and activities. The proliferation of portable devices into our lives has introduced new location privacy threats. As an example, HIV patients could be identified by the office of the healthcare professional they visit. A number of location privacy threats were also reported in our previous work [13]. Significantly, many technologies can determine the location of an individual using various locationing techniques such as GPS positioning, location fingerprinting and others. These geo-location methods have been reviewed in our previous work [13].

Mobile location based services (LBSs), for instance, have facilitated the exchange of location information between people, making socializing easier. While these LBSs offer numerous benefits to users, they may have impact on the users' privacy. In the IoT, the major privacy concerns with objects equipped with communication capabilities is their abilities to reveal the location of their users. Poorly designed objects, absence of policies or lack of control over the location disclosure mechanism enable untrusted entities to obtain the location of another entity.

To confront the location privacy challenges, the IoT must have strong security features built on a holistic view of security for all the IoT aspects: from object naming and identification to provision of services, from data acquisition to infrastructure governance. Security must be considered in each object's life cycle. Furthermore, many new automated attack vectors become possible whether via objects automations, environment observation, inference or data mining. These attacks are detailed as follows:

A. First-hand Attack

In a first-hand attack, the attacker obtains the information directly from the user. An objectionable disclosure of information can happen accidently, such as the presence of security holes in a system which leads to a leakage in the information; or by tricking the user using social engineering methods. For example, the Windows File Sharing Protocol can be used to obtain the users' names. Originally, this was never the aim of the protocol intended by Microsoft. Cookiejacking is another form of a first-hand communication attack wherein the attacker can gain access to the session cookies of an Internet Explorer user by tricking them and thus obtaining their username and password stored in the cookie [14]. Nevertheless, news on security flaws found on computers', and recently mobiles' operating systems are all over the web. Back in 2003, serious flaws in the authentication and data transfer mechanisms on some Bluetooth enabled devices led to the disclosure of personal information were reported [15]. Nowadays with the explosion of smart phones technologies, applications installed on the Android, iOS, windows mobile devices and others are known to have the capabilities of accessing the personal information of the users including their location information. This could form a vulnerability that might allow an attacker to obtain a live location feed of a user. WLAN cards periodically transmit traffic that contains their unique MAC ID. These are a few examples of the triggers that might lead to a first-hand attack on location privacy. Additionally, numerous electronic devices which provide constant precise location information to location based servers are seen as overly permissive. If this location information is processed by automated objects insecurely, they will form a

source of harm to the users' privacy. In a world surrounded by intelligence in the IoT, the threat of disclosing personal information unconsciously via first-hand communication is significant. At the bare minimum, these concerns must be highlighted.

B. Gossip Attack

The English definition of the word "Gossip" is an unconstrained conversations or reports about other people personal or private affairs. In digital terms, a gossip attack or communication is relaying personal information from one entity to another unauthorized entity. The main difference between a gossip and first-hand communication is that the user is no longer the direct source of information. Disclosure of the user's personal information can be done without being noticed by the user. This behavior has already been observed in some online activities and recently on some portable devices, such as tablets' or mobiles' applications that sell users' location information, their shopping behaviors, and others to advertisement companies. Our previous work in [13], reported that some service provider are actively collecting a user personal information without any consent from the user and selling them to third parties.

It is expected that this type of information, which is available via objects and fine-tuned by their technological advanced features and automation, to be similarly misused. The widespread use of objects and the deployment of IoT networks such as sensor networks, will lead to an enormous amount of data being captured by commercial and state enterprises. This presents the ability to associate data including location information, with an object and therefore a person; and concerns are raised on the appropriate use and collection of this information and the consequence of their leakage on the users' privacy. It is almost ascertain that the more a technology develops, the more the capacity to gather, organize and data mine on personal information will result, and the more the disclosure of information is going to occur, whether accidently (first-hand communication) or intentionally for someone's else benefit such as in the gossip communication. Currently in the online environment, cautions can be exercised such as controlling who is acquiring the personal information and knowing how the information is going to be used. In an object-to-object communication, in the IoT, users need to have more control over information related to them, and giving such control to a user and at the time making full use of the advantages of the Internet of things environment is a challenging task.

C. Observation Attack

One of the significant features in the IoT is the ability of objects to observe and sense their environments. Attackers may also configure objects to collect information, miscellaneously, about their environment. The most serious concerns with these objects are their ability to initiate, by themselves, exchange of information with each other's. Smart objects that log data about their environment, e.g., their locations, constitute a source of risks and vulnerabilities, with regard to privacy, to their owners. If these objects are connected together, as envisioned in the IoT, and these logs are shared among objects, there is an increased risk of personal information leakage which may be a threat to the users' privacy.

D. Inference Attack

Some studies reported the use of recorded personal information to demonstrate a privacy attack, frequently referred to as an "inference attack". The idea is to build a map reflecting on the activities, mobility behavior, and other mobile patterns of an entity using the data gathered from other attacks. An example of an inference attack is the study conducted in [16]. The authors were able to determine the names of the persons stored in their database by observing and noting the locations where people spent most of their time in the office building, and by noting who spent more time at their desk. Apart from inferring people's locations, some researchers reported the inference of other information based on context observation. For example, in [17], the authors used real time GPS traces to infer a traveling user's mode of transportation (by car, train, bus, walking etc...). They were also able to predict the user's route, based on his or her movement history.

The seamless interconnectivity of objects envisioned in the IoT will open the door to various inference attacks. When interconnected networks of smart objects in the IoT are capable of tracking the users automatically on an ongoing basis, they generate an enormous amount of potentially sensitive information leading to possible inference attacks similar to the ones described above.

E. Automated Invasion Attack

In the IoT, some of the fear about automated objects' communications is the compilation of users' profiles. After gathering large amounts of information, using for example, one of the attacks described above, an automated system can combine the data and can perform data mining or analysis that can lead to a new kind of attacks. We refer to this new attack as the "Automated Invasion Attack". An automated invasion attack could be constructed using the following gathered information:

- **Current data collected from typical computer usage including the data generated from mobile and tablets' applications:** This data is a possible source of information that an attacker can gather to infer some patterns relating to a user's activities. For instance, the IP address reflects on the location of the user. The time, date and other parameters can also be collected. A Mobile application can log its location, usage history and its interactions with a location based server.
- **Current data collected from the Internet or via social networking website**. The website "Please Rob Me" is an example of how to predict a user's presence at home from publicly available information by looking at the places where a user checks-in. With the public availability and accessibility of some of the information about a user found on various social networking websites, it is possible to infer information relating to an individual.
- **Data collected from the mobility behavior of an individual**: The movement patterns of an individual

constitute a form of fingerprinting. For instance, the attacker might be able to infer a user's points of interest. The location of user's kids' school, the time the user usually pickup their kids, their Friday weekly social activity locations are examples of a user's points of interest. Information about recurrent visits to a political party location or religious group could be used to infer a user's social, political and religious beliefs.

- **Data collected from objects in the IoT environment:** Whether a user is interacting with a particular object directly or indirectly using another object which is also owned by the user, the information generated from these interactions constitute a possible source of information that reflect on the behaviors, location, date, timing, shopping habits and other personal information of the user.
- **Linking the records of objects:** Objects' data are a possible source of information that an attacker can collect to infer a user's personal information. Additionally, in the IoT, if an object's data that contain logs about their use, location, history, and others private information, is linked with the same type of data generated from another object, they could lead to a linking attack. In a geolocation context, a linking attack works by associating the movements of an individual to the movements of an object owned and operated by the user. For example, the movement of a user can be inferred from the movement of his or her car equipped with a GPS location-tracking system, during working hours on a weekday when the car is probably being driven by the user.

Consequently, an automated invasion attack is an incremental process of inference attack in which the attacker gradually gathers more knowledge on victim user's life or activities through the combination and linking of the information collected from various smart objects owned and operated by the user.

V. CONCLUSION

With the rapid advancement of technology, the Internet of Things (IoT) is no longer seen as a vision of the future. It is becoming a reality in the present. The IoT is expanding the boundaries of the Internet we know today, by enabling a new form of interaction and communication between objects, leading to the vision of "anytime, anywhere, anyone, and anything" communications. This intercommunication results in autonomous exchange of information between object-to object and person-to-object. In this paper, we survey the state-of-art on the IoT, including the manifold definitions, enabling technologies and the major challenging issues. The core research issues remaining open for the IoT community are also described. Particular attention is given to various attack vectors for privacy attacks in the IoT and the implications of these attacks on the users' privacy. Future works will address these security concerns, specifically, those challenging the location data privacy, safety, governance and trust.

REFERENCES

[1] (2005, *The Internet of Things*. Available: http://www.itu.int/osg/spu/publications/internetofthings/

[2] ITU, "Global Standards for the Internet of Things," ed: ITU, 2012.

[3] K. Ashton, "That 'Internet of Things' Thing," *RFID Journal,* 22 July 2009.

[4] G. Santucci, "The internet of things: Between the revolution of the internet and the metamorphosis of objects," *Harald Sundmaeker, Patrick Guillemin, Peter Friess, Sylvie Woelfflé Vision and Challenges for Realising the Internet of Things.. Cluster of European Research Projects on the Internet of Things (CERP-IoT),* 2010.

[5] G. Neil, *When things start to think*: Holt Paperbacks, 2000.

[6] J. Liu and W. Tong, "Dynamic Service Model Based on Context Resources in the Internet of Things," in *Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on*, 2010, pp. 1-4.

[7] D. Brin. *The Transparent Society: Will Technology Force us to Choose Between Privacy and Freedom?* Available: http://www.davidbrin.com/ts1.htm

[8] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the Internet of things," *Internet Computing, IEEE,* vol. 14, pp. 44-51, 2010.

[9] (2012, *Y.2060 : Overview of the internet of things*. Available: http://www.itu.int/rec/T-REC-Y.2060-201206-P/en

[10] "White Paper: Smart Networked Objects and Internet of Things," Association Instituts Carnot2011.

[11] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks,* vol. 54, pp. 2787-2805, 2010.

[12] A. Cavoukian and F. Carter, *7 laws of identity: The case for privacy-embedded laws of identity in the digital age*: Information and Privacy Commissioner of Ontario, 2006.

[13] M. Elkhodr, S. Shahrestani, and H. Cheung, "A Review of Mobile Location Privacy in the Internet of Things," in *2012 Tenth International Conference on ICT and Knowledge Engineering*, Bangkok, Thailand, 2012, pp. 266-272.

[14] J. Cashion and M. Bassiouni, "Protocol for mitigating the risk of hijacking social networking sites," in *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2011 7th International Conference on*, 2011, pp. 324-331.

[15] A. Laurie and B. Laurie, "The Bunker í Serious flaws in Bluetooth security lead to disclosure of personal data," ed: The Bunker, homepage, 2004.

[16] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *Pervasive Computing, IEEE,* vol. 2, pp. 46-55, 2003.

[17] D. Patterson, L. Liao, D. Fox, and H. Kautz, "Inferring high-level behavior from low-level sensors," in *UbiComp 2003: Ubiquitous Computing*, 2003, pp. 73-89.