2014 IEEE 7th International Conference on Service-Oriented Computing and Applications

IoT Security: Ongoing Challenges and Research Opportunities

Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh, *IEEE Fellow*
Department of Computer Science
National Chiao Tung University
Hsinchu, Taiwan
e-mail: {skyzhang, michcho, wangcw}@dsns.cs.nctu.edu.tw, {hsucw, ckchen, ssp}@cs.nctu.edu.tw

Abstract—**The Internet of Things (IoT) opens opportunities for wearable devices, home appliances, and software to share and communicate information on the Internet. Given that the shared data contains a large amount of private information, preserving information security on the shared data is an important issue that cannot be neglected. In this paper, we begin with general information security background of IoT and continue on with information security related challenges that IoT will encountered. Finally, we will also point out research directions that could be the future work for the solutions to the security challenges that IoT encounters.**

Keywords - Internet of Things, information security, naming, identification, authenticity, malware.

I. Introduction

When the term "Internet of Things" (IoT) was first introduced, the initial question could be what is considered as "Things". Till recent years, groups of researchers and organizations tried to clarify the definition of IoT. Haller et al. [1] proposed a definition of IoT with *"A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business process."* To extend the coverage of IoT definition, Sarma et al. [2] defines the "Things" from physical objects to virtual objects which represents as the identities with Internet connectivity. Although IEEE IoT Initiative is proceeding to draft a white paper [3] for the formal definition of IoT, there are still no common agreements for the definition of IoT. In this article, we define a "Thing" on IoT that indicates a physical or virtual object which connects to the Internet and has the ability to communicate with human users or other objects.

Along with the growth of IoT, new security issues arise while traditional security issues become more severe. The main reasons are the heterogeneity and the large scale of the objects. The impact factors can be further divided into two categories: the diversity of the "Things" and the communication of the "Things". It is divided into two categories given that each of the category encounters different security problems.

First, the security problem for the "Things" is created by vulnerabilities produced by careless program design; this creates opportunities for malwares or backdoors installation. Based on the heterogeneity and the scale of the "Things" in IoT, such security problems are more complex compared to the security problems that we have faced now.

As for the communication medium of the "Things", it is expected that the networking environment for IoT will be heterogeneous. Various communication media may face different security challenges. Overlooking these security problems will compromise the availability of the "Things". As for the contents of the communication, the heterogeneous data structure and protocols also make content protection more complex.

In this article, we will briefly state related research areas in IoT and address the challenges in these research areas.

II. Ongoing Research in IoT Security

In this section, the ongoing research areas will be briefly described for the aspects of IoT infrastructure, cryptography, software vulnerability, malware, and mobile devices.

A. *Object Identification and locating in IoT*

To uniquely identify an object is the first important issue that came before other security issues. A proper identification method is the foundation of IoT. An ideal identification methodology not only identifies the objects uniquely, but also reflects the property of the object. For example, DNS (Domain Name System) is a good identification method which uniquely identifies a host on the Internet; it also reflects host's property through FQDN (Fully Qualified Domain Name) naming policy, and provides address mapping through DNS resolution. Based on the success of DNS, Object Name Service (ONS) [4] is published by the EPCglobal board in 2005 to locate the metadata and services associated with a given Electronic Product Code (EPC). The proposal of ONS gives a hint that a similar structure could be applicable to the object identification in IoT.

Since the objects are connected to the network, the network location of the objects is also an important issue. Currently, the most widely used locating method is based on IPv4/IPv6. Although IP addressing may still be one of the candidates in the future Internet, Named Data Networking (NDN) [5] is proposed as a naming infrastructure of Future Internet Architecture (FIA). In contrast to host-oriented IP addressing, NDN is a data-oriented method which combines naming and addressing where packet routing is based on object names directly.

B. *Authentication and Authorization in IoT*

How to authenticate the objects is also an important research area. Traditionally, authentication is achieved through many methods such as ID/password, pre-shared

978-1-4799-6833-6/14 $31.00 © 2014 IEEE
DOI 10.1109/SOCA.2014.58

IEEE computer society

secrets, and public-key cryptosystems. Authorization can be achieved by database-based or crypto-based access control. Due to the heterogeneity and complexity of the objects and networks in IoT, traditional authentication and authorization methods may not be applicable. For instance, authenticating and authorization through cryptographically pre-shared keys is not applicable. The rapidly growing number of objects will make the key management become a difficult task. Although research [6][7] has attempted to resolve the problem of object authentication and authorization, there are still no common agreements or standards in this area.

C. Privacy in IoT

At the current stage, information about user behavior whilst browsing the Internet is collected to enrich the user experience on the Internet. As for IoT, the amount of information collection is not limited to Internet browsing behavior; information about a user's daily routine is also collected so that the "Things" around the user can cooperate to provide better services that fulfill personal preference. Owning to the collected information that describes a user in detail, preserving the privacy of the collected data is an issue to be addressed in the case of personal information misusage.

D. Lightweight Cryptosystems and Security Protocols

In IoT, there are various resource-constrained devices such as sensor nodes, smart devices, and wearable devices, which only have limited computing power and battery capacity. Although many proposed cryptosystems and security protocols are considered secure and robust, they may not be suitable for the resource-constrained devices. For instance, some recent research work [8][9] targeted on this research area.

E. Software Vulnerability and Backdoor Analysis in IoT

In additional to the authentication and authorization problems, software vulnerability plays an important role in current security research domain. During the development stage of a piece of software, programming bugs produced by developers are unavoidable. Bugs that result in security incidents are known as software vulnerabilities. Upon discovery of new software vulnerabilities, AKA 0-day, attackers can leverage this knowledge to exploit a large number of machines.

In the traditional PC industry, system architectures are similar amongst the machines. For example, Windows operating system on x86 machine architecture dominates the commercial market. Developers can focus on this mainstream and implement popular software. Therefore, security awareness on software programming is relatively easy to enforce with proper education. In the heterogeneous IOT, diversified hardware platforms and customized operating systems make it difficult to educate programmers on security awareness. Furthermore, with the explosive increase of software complexity, it is rigorous for software developers to take care of every aspect of secure programming. At the current stage, a number of research works identified that IoT devices have vulnerabilities exposed to attackers. [10][11]

Program analysis can discover software vulnerabilities before the product is released. To verify a program, the dynamic analysis approach monitoring the targeting program in a controlled environment is an effective approach. It empowers many advanced analysis techniques such as taint analysis and symbolic execution. These analysis tools, which usually require intensive computation power, are inadaptable to IoT devices due to the resource-constraint problem. Moreover, most of these advanced analysis techniques are highly dependent on the underlying system platform. Building these analysis techniques require ad-hoc development for different platforms in the diversified IOT environments [12][13].

Software vulnerabilities can lead to a number of backdoor problems. First, with software vulnerabilities, attackers exercise malicious intents without any artifact in a victim's system. Consequently, a backdoor can be planted in a vulnerable device by attackers to control the device. Due to the resource-constraints of IoT devices, security mechanisms such as IDS or antivirus that requires fair amount of computation power are not applicable in IoT. Therefore, it is relatively easy for attackers to inject backdoor into victim's machine.

Another type of backdoor is deliberately inserted in a software product by vendors for management or testing purposes. However, these backdoors may be discovered and used by adversaries to steal user data. A skillful adversary can examine code and discover this type of backdoor by applying reverse engineering techniques. Even though users can examine the device before deployment, the examination requires knowledge of reverse engineering skills and significant human effort. Moreover, the examination has to repeat with system upgrades. This procedure becomes a daily operation when software received patches for security updates. Therefore, this kind of backdoor is easy to deploy but hard to examine. That is the main reason why some government agencies impose certain security policies on the deployment of untrusted devices.

F. Malware in IoT

In Nov. 2013, Symantec confirmed the finding of the first IoT malware, Linux.Darlloz, which brings up the malware issue for IoT security. The IoT services embrace the great connectivity among various devices while attracting adversaries as a hotbed to widely spread out their crafted malware. Upon connection to a victim user, any of the infected IoT devices could contaminate a device held by the victim and thus get one step further to the targeted critical device with the massive data of interest it stored. In addition to the rapid propagation advantage, malware can also simply lurk in an end-device, which is rarely equipped with strong security defense, for the long-term profiling/control of IoT devices such as surveillance cameras. This seriously violates the privacy of Internet users. Previous research works [14][15][16] also give the discussion over the possible threats caused by malware against IoT and further clarify its importance. However, to our best knowledge, at present there is little research work dedicated to the countermeasure of IoT-targeted malware. The reason could be the small population of real-world IoT malware instances and thus hard to generalize an effective solution. Nevertheless, the existence of Linux.Darlloz indicates that the IoT malware is no longer an imaginary enemy, but a serious threat to IoT devices. The malware threat and countermeasure in IoT will become critical and should addressed.

G. *Android Platform*

Android platform, the most popular mobile operating system, has overwhelmingly taken the mobile market share. Based on Android, more and more smart devices have been developed as personal assistants that surely headlined the IoT [17]. With its open and embedded-system oriented design, the Android platform attracted IoT developers' attention in many aspects. Many Android features have been adopted in IoT devices, such as power saving, near-field communication, multi-sensors, voice control. Namely, Android already has been part of IoT. Although there are other contenders such as Apple iOS, Windows phone, and Mozilla Firefox OS, Android is supported by a large development community bootstrapping IoT toward many possible directions.

III. Challenges in IoT Security

As discussed, the main challenges for IoT security are from the heterogeneity and the large scale of objects. In this section, we will discuss these security issues with more details.

A. *Object Identification*

The main challenge of object identification is to ensure the integrity of records used in the naming architecture. Although the Domain Name System (DNS) provides name translation services to Internet users, it is an insecure naming system. It remains vulnerable to various attacks, such as DNS cache poisoning attack, and man-in-the-middle attack. This poisoning attack injects counterfeit DNS records into victims' cache and directly compromises the resolution mapping between naming architecture and addressing architecture. Therefore, without the integrity protection of the records, the entire naming architecture is insecure. Domain Name Service Security Extension (DNSSEC, IETF RFC4033) is deployed as the security extensions of DNS. DNSSEC can ensure the integrity and authenticity of a Resource Record (RR), and at the same time serve as a vehicle for the distribution of cryptographic public keys. Although DNSSEC seems to be a remedy for naming services, it is still challenging to deploy DNSSEC properly in IoT. DNSSEC incur high computation and communication overhead and may not be suitable for IoT devices. A new naming service is desirable.

B. *Authentication and Authorization*

Although public-key cryptosystems have advantage for constructing authentication schemes or authorization systems, the lack of a global root certificate authority (global root CA) hinders many theoretically feasible schemes from actually being deployed. Without the global root CA, it becomes very challenging to design an authentication system for IoT. Furthermore, it may be infeasible to issue a certificate to a object in IoT since the total number of objects is often huge. Therefore, the concept of delegated authentication and delegated authorization must be taken into consideration for IoT.

C. *Privacy*

In the previous section, we elaborated the importance of preserving privacy in IoT. In this section, we will depict the challenges to IoT deployment on preserving privacy. The challenges can be divided into two categories: data collection policy and data anonymization. Data collection policy describes the policy during data collection where it enforces the type of collectable data and the access control of a "Thing" to the data. Through the data collection policy, the type and amount of information to be collected is restricted in the data collection phase. Since the collection and storage of private information is restricted, privacy preservation can be ensured. The second challenge is data anonymization. To ensure data anonymity, both cryptographic protection and concealment of data relations are desirable. Given the diversity of the "Things", different cryptographic schemes may be adopted. For example, lightweight cryptographic schemes are more suitable to devices that have resource-constraints. The second category, concealment of data relation, investigates the removal of direct relations between the data and its owner. This also can be achieved by applying data encryption where scrambled data has resistance against data analysis. However, information needs to be shared amongst "Things" in IoT; therefore, computation on encrypted data is another challenge for data anonymization. To cope with the problem, some of research works in homomorphic encryption may be applicable.

D. *Lightweight Cryptosystems and Security Protocols*

Compared with symmetric-key cryptosystems, public-key cryptosystems generally provide more security features but suffer high computational overhead. However, public-key cryptosystems are often desirable when data integrity and authenticity are needed. Therefore, computation overhead reduction for public-key cryptosystems as well as complex security protocols remains a major challenge for IoT security.

E. *Software Vulnerability and Backdoor Analysis*

Dynamic analysis is an effective approach to the discovery of vulnerabilities before product release. Due to resource constraints, dynamic analysis may be inefficient to deploy in an IoT device. Therefore, the emulation, which can emulate the behavior of devices in a server with more computing power, is needed to make dynamic analysis applicable. However, the semantic gap between real device and emulated system is an important issue to be addressed. The discrepancy between device and emulated system is difficult to avoid. Moreover different components in a device such as GPS and gyroscope make it even more difficult to close the semantic gap.

Many analysis techniques, such as taint analysis and symbolic execution, are highly dependent on the underlying system. With highly diversified environments, an analysis system must be flexible enough to adopt different systems. Proper interface and intermediate layer must be provided to separate system dependency. Thus, the extensibility can be achieved to adopt a variety of systems.

To eliminate backdoors, the aforementioned dynamic analysis technique is also a promising solution. However, it is not merely a technical issue. Both management and policies also play an important role. Multi-level examination to reduce software vulnerabilities, discovery of backdoors with reverse engineering, and software auditing are all useful to prevent the usage of backdoors.

F. Malware in IoT

As aforementioned, the threat of IoT-targeted malware is serious due to the limited resources of IoT devices. Moreover, conventional security mechanisms against malware can be infeasible while being shifted directly from the common x86 architecture platforms to the IoT platform. For instance, it is believed that the antivirus is one of the most effective security tools to detect known malware in the real-time paradigm. However, unlike the x86-architectured PC, the computing power of the IoT devices is relatively small. The real-time scanning functionality of antivirus may results in unaffordable overhead to IoT devices. Meanwhile, malware authors considering the computing power issue of IoT will also craft their malware into the separated downloader and the main body. The downloader as a pioneer to infect any of IoT devices has tiny program body and thus embarrasses the extraction of its unique, malicious signature. In addition to the example above, there are still the other issues such as the divergence of hardware architectures among various devices. Without a generic abstraction of the IoT malware, current solutions can be ad-hoc and even inapplicable.

G. Security Issues from Android

If heterogeneous devices connect to the Android system forming personal area network (PAN), the security issues specifically for Android will be brought into IoT. The main concern is sensitive data leakage. The current permission protection only provides course-grain management, namely all-or-nothing choice, to restrict the type of connected devices and disable the runtime control. Complicated environments and application scenarios should be considered to include more possible granted permissions. Google accidentally released runtime permission control, AppOps, in Android 4.3, but soon removed in 4.4. AppOps shows that dynamic management is feasible. On the other hand, Android malware is another serious problem when IoT meets Android. Unlike iOS, Android is open-sourced. That makes it easy to discover vulnerabilities of the system. Once malware compromises front end devices, the network of IoT is exposed to threats. These ubiquitous devices provide abundant computing power and information for interested attackers to exploit. Although Google announced the Bouncer for vetting apps, the price of being penetrated rises and the attack will be amplified when IoT is involved. Deeper apps analysis such combining static and symbolic [18] is desirable. On the other hand, users may violet the policy enforced by an organization. Military and companies should carefully use even it will be more convenient with IoT. Insider's attacks are always the most challenging issue to deal with. So far this issue is not well addressed, but some research [19][20] made attempts to address policy enforcement. A good auditing system is necessary while IoT comes into the map. Audit logs can help developers refine the access control mechanism of Android. It is a more passive way without disturbing users. Leveraging Android and its experience, developers and manufacturers can facilitate IoT technology and enrich our life soon after.

IV. Conclusion

The main features that differentiate IoT security issues from the traditional ones are the heterogeneous and large-scale objects and networks. These two factors, heterogeneity and complexity, make IoT security much more difficult to deal with. This article addressed ongoing challenges and research opportunities in IoT security. New research topics and their possible solutions are also discussed.

Acknowledgement

This work is supported in part by Ministry of Science and Technology (MOST), Ministry of Education of Taiwan, Taiwan Information Security Center (TWISC), ITRI, III, iCAST, HTC, D-Link, Trend Micro Inc., Promise Inc., Chungshan Institute of Science and Technology, Bureau of Investigation, and Chunghwa Telecomm.

References

[1] S. Haller, S. Karnouskos, and C. Schroth, "The Internet of Things in an Enterprise Context," in *Future Internet – FIS 2008 Lecture Notes in Computer Science* Vol. 5468, 2009, pp 14-28.

[2] A. C. Sarma, and J. Girão, "Identities in the Future Internet of Things," in *Wireless Personal Communications 49.3*, 2009, pp. 353-363.

[3] Roberto Minerva, Abiy Biru, "Towards a Definition of the Internet of Things," *IEEE IoT Initiative white paper.*

[4] GS1, *Object Name Service (ONS) Standard* [Online]. http://www.gs1.org/gsmp/kc/epcglobal/ons/, accessed on October 8, 2014.

[5] L. Zhang, A. Afanasyev, J. Burke, claffy, L. Wang, V. Jacobson, P. Crowley, C. Papadopoulos, B. Zhang, "Named Data Networking," in *ACM SIGCOMM Computer Communication Review*, July 2014

[6] W. Shang, Q. Ding, A. Marianantoni, J. Burke, and L. Zhang, "Securing building management systems using named data networking," *IEEE Network Special Issue on Information-Centric Networking*, April 2014.

[7] J. Liu, Y. Xiao, and C. L. P. Chen. "Authentication and Access Control in the Internet of Things," In *IEEE 32nd International Conference on Distributed Computing Systems Workshops*, June 2012.

[8] Cole, Peter H., and Damith C. Ranasinghe. "*Networked RFID systems and lightweight cryptography*," London, UK: Springer. doi 10 (2008): 978-3.

[9] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," in *IEEE Sensors Journal*, Vol. 13(10), 2013.

[10] A. Cui and S. J. Stolfo, "Reflections on the engineering and operation of a large-scale embedded device vulnerability scanner," In *BADGERS. ACM*, Apr. 2011.

[11] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti. "A Large Scale Analysis of the Security of Embedded Firmwares," In *USENIX Security Symposium*, August 2014.

[12] D.Davidson, B.Moench, S.Jha, and T.Ristenpart. "FIE on Firmware: Finding Vulnerabilities in Embedded Systems Using Symbolic Execution," In *USENIX Security Symposium*, August 2013.

[13] J. Zaddach, L. Bruno, A. Francillon, and D. Balzarotti. "Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares," In *Network and Distributed System Security Symposium*, February 2014

[14] R. Roman, P. Najera, J. Lopez, "Securing the Internet of Things," *Computer* , vol.44, no.9, pp.51,58, Sept. 2011

[15] H. S. Ning, H. Liu; Y, L.T. "Cyberentity Security in the Internet of Things," *Computer*, vol.46, no.4, pp.46,53, April 2013

[16] X. Xu, "Study on Security Problems and Key Technologies of the Internet of Things," *Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on* , vol., no., pp.407,410, 21-23 June 2013 doi: 10.1109/ICCIS.2013.114

[17] “Android will power the Internet of things,” InfoWorld, 06-Feb-2014. [Online]. Available: http://www.infoworld.com/article/2610361/big-data/android-will-power-the-internet-of-things.html. [Accessed: 08-Oct-2014].

[18] Z. Yang, M. Yang, Y. Zhang, G. Gu, P. Ning, and X. S. Wang, "Appintent: Analyzing sensitive data transmission in android for privacy leakage detection," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 1043–1054.

[19] M. Conti, V. T. N. Nguyen, and B. Crispo, "Crepe: context-related policy enforcement for android," in *Information Security*, Springer, 2011, pp. 331–345.

[20] K. Z. Chen, N. M. Johnson, V. D’Silva, S. Dai, K. MacNamara, T. R. Magrino, E. X. Wu, M. Rinard, and D. X. Song, "Contextual Policy Enforcement in Android Applications with Permission Event Graphs," in *NDSS*, 2013.