Assessing Identity Theft in the Internet of Things

Stilianos Vidalis*
University of Staffordshire
Stafford, U.K.
stilianos.vidalis@staffs.ac.uk

Olga Angelopoulou
University of Derby
Derby, U.K.
o.angelopoulou@derby.ac.uk

Abstract

In the Internet of Things everything is interconnected. In the same context that "man-made fire" got the party started for human civilisation, "man-made TCP" enabled computing devices to participate in our lives. Today we live in a socially-driven knowledge centred computing era and we are happy in living our lives based on what an Internet alias have said or done. We are prepared to accept any reality as long as it is presented to us in a digitised manner. The Internet of Things is an emerging technology introduced in Smart Devices that will need to be intergrated with the current Information Technology infrastructure in terms of its application and security considerations. In this paper we explore the identity cyberattacks that can be related to Internet of Things and we raise our concerns. We also present a vulnerability assessment model that attempts to predict how an environment can be influenced by this type of attacks.

Keywords: Internet of Things, Vulnerability, Information security, Identity theft

1 Introduction

The Internet of Things (IoT) is a set of objects that can cooperate to reach a common goal. [1] include Radio-Frequency IDentification (RFID) tags, sensors, actuator and mobile phones in their list of quoting Nicolas Negroponte: "When we talk about an Internet of things, it's not just putting RFID tags on some dumb things so we smart people know where that dumb thing is. It's about embedding intelligence so things become smarter and do more than they were proposed to do." Herein lays the problem as never before human beings have allowed their lives and their societies to be affected by machines by such a magnitude.

The Internet of Things promotes ubiquity, while it connects objects between the physical and the digital world. We ourselves have become nothing more than dumb members of the Internet of things as we have transferred the honours of cultivating our intelligence to smart devices. [7] discuss the challenges of such integration, while [11] discuss the vision of the IoT and the interrelation of people, devices, protocols and networks in the future. Apropos, no matter the sophistication of those devices, no matter how advanced the applications that use those devices are, the truth of the matter is that everything is based in a few word acronyms: IP, ARP, TCP, SSL and the odd ICMP. Of course we can include more protocols' acronyms, but in the IoT transparency, usability and performance are paramount, so anything else would be out of the scope of this study.

Although vendors support that data authenticity and integrity are equally important, those two attributes are not adequately considered as they upset the users with added complexity. Furthermore, although cryptography is considered to be the cornerstone for informational infrastructure protection, it offers

IT CoNvergence PRActice (INPRA), volume: 2, number: 1, pp. 15-21

*Corresponding author: Faculty of Computing, Engineering and Sciences, K244, Octagon Building, Staffordshire University, Beaconside, Stafford, Staffordshire, ST18 0AD, UK, Tel: +44-(0)1785 353270, Web: http://www.staffs.ac.uk/staff/profiles/sv3.jsp

limited flexibility, and the devices that participate to it are extremely limited, so we can forget high maintenance algorithms such as AES. We could try to be symmetric and proactive; but of course there is always the risk of dealing with all types of attacks and breaches. Information Technology needs to excplicity consider the convergence of security and privacy to IoT for a smooth transition.

2 Cyberattacks and IoT

The salami attack [9] is a well-documented attack, mainly related to financial and identity crimes, where a perpetrator sniffs packets from a network, modifies them and inserts them back into the network without disrupting their availability attribute. The main characteristic of the salami attack is the little significance it makes each time to the individual victim in relation to the extent of the attack overall. In other words, as the name indicates, it reminds a salami slice.

Later in this the paper we will explain how ID theft involves one or more forms of spoofing; so getting back to the attacks we can concentrate on spoofing attacks. Spoofing attack is considered any attack that leads the victim in a correct decision for an imaginary environment, with misleading effects for the real environment [4]. IP and Arp spoofing relate to ID theft types of attacks.

- IP spoofing: one device impersonates another using the IP address as the means of the impersonation.
- Arp spoofing: one device impersonates another using the MAC address as the means of the impersonation.

We parallel a salami attack to the IoT to a party, where all the joining members interact with the host. An example to a spoiler party can be as simple as:

(1) Perpetrator: Spends some time determining the IP addresses of target and victim systems. Determining trust relationships can be easily done with utilities like Wireshark, or running who, ps, or last from previously stolen (or wide open ”guest” style) accounts.

(2) Perpetrator: Runs Metasploit, attaches himself to the subnet and joins the party.

(3) Perpetrator: Starts ARP relay daemon, prepares RST daemon entry for use later, sets option to enable host name resolution (for convenience).

(4) Victim: Joins the party from a device and starts accessing target devices. Runs application to check up on his fridge/freezer and review what he has for food and what he needs to order.

(5) Perpetrator: Sees new connection; lists active connections to see if this one is potentially ”interesting.” If it is, perpetrator can either watch the session (packet sniffing) or hijack the session. Decides to hijack.

(6) Victim: Sees strange new prompt. Tries pressing RETURN and doesn’t know what to think. Tries web browser and notices that it still works fine (not a network problem). Not sure what to think.

(7) Perpetrator: Finds this is a user session and decides to give it back (resynchronizes TCP/IP stream).

(8) Victim: Sees prompt for keystroke, follows request, gets session back. Puzzled, decides to log in to other home devices using his root account to take a closer look.

(9) Perpetrator: Turns on RST daemon to prevent new connections, waits to hijack root session.

(10) Victim: Runs ssu to get protected root shell.

(11) Perpetrator: Completes hijack after seeing root login.

(12) Victim: Sees strange prompt. Tries pressing RETURN again. Same result as before. Tries web browser again. Same thing. Tries getting a new session. Fails. Tries SSH. Fails.

(13) Perpetrator: Sets up backdoor, disables command history, resets session, turns off RST daemon.

(14) Victim: Finally gets a new session. Original session is now gone. Assumes network outage or TCP/IP stack corruption. Reboots system and everything is back to ”normal”.

(15) Perpetrator: Waits for sessions to all disappear, and then logs in using a new backdoor. The perpetrator installs a rootkit, more backdoors or a sniffer and cleans all the log files.

Of course no self-respected threat agent will initiate a targeted attack without spending some time socialising with the victim. As we mentioned in the introduction, many users readily accept information from smart devices as facts of life. We do believe the biggest threat to the success of the IoT to be the ID theft related crimes, as application vendors will be forced to discontinue vulnerable services, an action which will eventually affect hardware vendors. Since the IoT maintains a strong profile of the user in its sensors, an attack as described above could be prominent.

3 The Identity Implications

Personal identity is increasingly being stored and used in a range of digital forms. This can leave individuals exposed to possible threats as a result. There is a significant concern in the literature about identity management in the IoT [5], [3].
We should embrace the specific identity terminology in order to identify the nature and the intention of this type of crime.

> *Identity is defined as the characteristics determining who or what a person or thing is* [8]

ID theft is the use of your personal identity in the form of personal information by another individual for their financial gain although it may be argued that the gain in not necessarily always financial. It may be aimed at satisfying some other objective; espionage, terrorism, revenge, illegal immigration or assuming a new identity to avoid criminal charges. However, it is generally accepted that the end objective of ID Theft is usually some form of financial gain. Therefore, ID theft can be defined as

> *someone's action of using any sort of an individual's (or a corporation's) private information with fraudulent intention mainly for financial gain.*

ID theft is part of the broader term Identity Fraud. The terms are quite often confused and used improperly. [10] differentiate the terms and give the following definition for Identity Fraud:

> *Identity fraud is the subsequent crime when a false identity is used in order to gain goods, services, benefits or avoid obligations.*

ID theft involves the actual theft of someone's identity and often leads to Identity Fraud that deals with the actual fraudulent action. [2] gives the following definition for Identity Fraud

the use of that stolen identity in criminal activity to obtain goods or services by deception.

Stealing an individual's identity does not on its own constitute identity fraud and this is an important distinction. Moreover, any type of crime that deals with forged identities is referred to as Identity Crime. According to [2], Identity Crime is

a generic term for identity theft, creating a false identity or committing identity fraud.

It is fairly difficult to prevent ID theft incidents. ID theft has a significant human component being strongly influenced by the way people treat personal information. ID theft developed in the digital environment and transformed from a traditional, offline type of crime to a cybercrime. In a similar way it could easily transform in the IoT to a Smart-crime.
The IoT is based upon identity related services [6] and the communication of the objects is based upon the identity. With the IoT we will run out of paper before being able to compile a holistic list of associations between devices and attacks. Instead we propose to use vulnerability trees; a method for calculating the complexity of each attack by decomposing the vulnerabilities of each target device.

4 Complexity Calculation

Vulnerability trees are hierarchy trees constructed as a result of the relationship between one vulnerability and other vulnerabilities and/or steps that a perpetrator has to carry out in order to reach the top of the tree. The top of the tree is known as the top vulnerability or the parent vulnerability and we will symbolise it with a capital 'V'. There is a large number of ways that such a top vulnerability can be exploited. Each of these ways will constitute a branch of the tree. The branches will be constructed by child vulnerabilities. Consequently the child vulnerabilities can be exploited by steps that the perpetrator will have to perform in order to get to the parent. We will symbolise the child vulnerabilities with the lower case 'v' and the steps with the lower case 's'. Each vulnerability will have to be broken down in a similar manner. This will give us more than one level of decomposition. When the point is reached where the branches contain only steps, and no child vulnerabilities, then we know that we have reached the lowest level of decomposition. We will call that level the "step-only" level.
If we think of the vulnerability as being an IoT object, like all objects, it has some attributes. An attribute is any property, quality, or characteristic that can be ascribed to a person or thing. Attributes describe values to be exclusively manipulated by the services of the object. A service is defined as an activity carried out to provide people with the use of 'something'. The services of the vulnerability object fall outside the scope of this paper (at least in its current state), hence they will not be analysed. The attributes of the vulnerability object that have been identified in this initial stage are the following:

- `Vulnerability ID`: Unique vulnerability identifier
- `Name`: Vulnerability name
- `Type`: Indicates if node is vulnerability or step.
- `Category`: There are six categories of vulnerabilities that can exist in any system, and these are: Physical, Natural, Hardware/Software, Media, Communication, and Human. Each type will have to be approached in a different way.
- `CV` (complexity value): The complexity value is defined as:

> *The complexity value 'CV' of a vulnerability X is defined as the smaller number of vulnerabilities/steps that a threat agent has to exploit/utilize in order to achieve his objective.*[12]

The above identifies the way with the least obstructions for a perpetrator to achieve his goal. Each vulnerability has an educational complexity (EC) associated with it though; hence the first definition might not always be adequate. There is a need for showing the 'EC' of each step. The 'EC' is closely related to the educational level of the perpetrator; hence different perpetrators will follow different paths/techniques to achieve their goals. An additional feature is the Time to Exploit (TTE). The 'TTE', according to the device will vary in importance. According to the perpetrator's capabilities, the 'TTE' attribute might drastically affect the perpetrator's path in exploiting the goal vulnerability. The TTE of any vulnerability/step will be unique to each type of perpetrator.

- EC (educational complexity): Everyone can open a door and step into the server room, if the door is unlocked, but not everyone can use 'nmap' to perform a port mapping. The educational complexity is defined as:

  > *The educational complexity 'EC' of a vulnerability X is defined as the educational qualifications that a perpetrator has to acquire in order to exploit that vulnerability.*[12]

Educational complexity is related to the educational level of the perpetrator. Consequently, the educational level of the perpetrator is related to the capabilities and the resources that they already possess or can acquire in the future. Hacking is a "hands-on" activity. Just by knowing the theory does not automatically put a perpetrator in a certain category. The following table presents the different educational levels.

The table is not meant to tie the educational complexity to the academia and/or to a certain academic qualification. Most perpetrators do not have academic qualifications on "hacking" or on computers in general. The qualifications are only there for reference purposes, and for understanding the level of expertise that can be expected under each category. We aim to conduct a series of reverse engineering experiments in a secure laboratory were individuals from different threat agent categories will be using different methodologies for exploiting vulnerabilities in a controlled manner so as to collect primary data for substantiating our 'educational complexity' approach.

- TTE (time to exploit): The TTE is defined as the time required for a perpetrator to exploit a specific vulnerability. Because the exploitation of a vulnerability has a number of steps, TTE is the sum of the time needed to perform each of the required steps. Because different perpetrators have different capabilities, they have different TTEs. The golden rule is that as long as our sensors are able to identify the attack inside the time window presented by the TTE, and still have enough time to deploy the necessary countermeasures, then the asset is secure.

- FP (family position): The level of the node: 0 indicates parent or top vulnerability and any other number indicates child and how "far" is the child form the parent.

- Head: Identifier of the head vulnerability (needed for producing automated tool in the future)

- Asset ID: Unique asset identifier, which links the asset with the vulnerability.

- Tree ID: Unique tree identifier, which links a tree with the vulnerability. There can be more than one instances of the same vulnerability as different assets may have the same vulnerabilities.

Educational Complexity	*Qualifications*	*Alias*
1	None - No computing education	
2	Primary education – Familiar with term "computer"	
3	Secondary education – Computer user	
4	GCSE – User, Basic knowledge of operating systems (OS) and Internet	
5	A level – User, Basic knowledge of OS and Internet, Basic programming skills	Script kiddy
6	University Level 1 – Power user, Knowledge of OS and Internet, Basic programming skills, Basic networking	Amateur
7	University Level 2 – Power user, Medium knowledge of OS, Internet, programming and networking, Familiar with Linux	Amateur
8	University Level 3 / BSc – Administrator, Advanced internet, programming, networking and OS, Basic scripting, Basic Linux	Amateur
9	MSc – Root, Expert internet, programming, networking, scripting, Medium Linux	Hacker
10	Post MSc – Root, Expert internet, programming, networking, scripting, Advanced Linux, active hacking	Expert Hacker
A	PhD – all the above, known entity to hacking community	Professional Hacker
B	Post PhD – all the above, criminal record	Computer Criminal
C	All or most of the above, extreme low level knowledge of computers, involved in the development of "computers"	Case C

Table 1: Educational Complexity Table

- Description: Additional details to describe the vulnerability

At the end of our calculations we will have identified how an environment could be affected by the introduction of a smart device so that we might be able to make the most appropriate and informed decisions regarding its management. Apropos, the user will always constitute the biggest and less complex vulnerability of a system.

5 Conclusion

We have presented some of the cyberattacks that could be incorporated in the IoT. We also presented a vulnerability assessment methodology to measure the introduction of smart devices and the threat of ID theft. The presented methodology is not evaluated in an IoT environment. At a later stage we aim to practically experiment with the presented methodology and test with smart devices. Our assumption is that since IoT is a digital environment, hence prominent to cyberattacks; a vulnerability assessment is required before the deployment of a new system. Technological innovations contributed in the increase of ID theft in the digital environment and it would be wise to accept it as a significant threat that needs proactive countermeasures. IoT is still an emerging environment and the associated threats in relation to the individual's identity are still being evaluated.

References

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

[2] M. Button, C. Lewis, and J. Tapley. Fraud typologies and the victims of fraud literature review. 2009.

[3] L. Caviglione and M. Coccoli. Privacy problems with web 2.0. *Computer Fraud & Security*, 2011(10):16 – 19, 2011.

[4] E. W. Felten, D. Balfanz, D. Dean, and D. S. Wallach. Web spoofing: An internet con game. *Software World*, 28(2):6–8, 1997.

[5] S. Horrow and A. Sardana. Identity management framework for cloud based internet of things. In *Proceedings of the First International Conference on Security of Internet of Things*, SecurIT '12, pages 200–203, New York, NY, USA, 2012. ACM.

[6] G. M. Lee and J. yun Kim. The internet of things - a problem statement. In *Information and Communication Technology Convergence (ICTC), 2010 International Conference on*, pages 517–518, Nov 2010.

[7] H.-D. Ma. Internet of things: Objectives and scientific challenges. *Journal of Computer Science and Technology*, 26(6):919–924, 2011.

[8] O. E. D. Online. Oxford english dictionary online. `http://www.oxforddictionaries.com`, March 2014.

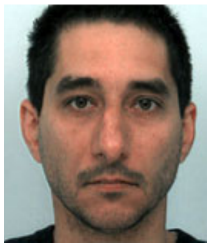
[9] M. L. Rustad. Private enforcement of cybercrime on the electronic frontier. *S. Cal. Interdisc. LJ*, 11:63, 2001.

[10] S. Sproule and N. Archer. Defining identity theft–a discussion paper. *Prepared for the Ontario Research Network in Electronic Commerce (ORNEC) Identity Theft Research Program*, pages 1–37, 2006.

[11] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, et al. Internet of things strategic research roadmap. *Internet of Things-Global Technological and Societal Trends*, pages 9–52, 2011.

[12] S. Vidalis and A. Jones. Using vulnerability trees for decision making in threat assessment. In *ECIW2003: Proceedings of the 2nd European Conference on Information Warfare and Security*, page 329. Academic Conferences Limited, 2003.

Author Biography



Stilianos Vidalis is a lecturer at the University of Staffordshire. He received his PhD in Threat Assessment under the context of Information Security in July 2004. His research interests are in the areas of Information Security, Information Operations, Digital Forensics, Threat Assessment, Profiling and effective computer defence mechanisms and he has published a number of papers in those fields.

Olga Angelopoulou is a lecturer and the programme leader for the MSc Computer Forensic Investigation at the University of Derby. She obtained a doctorate in Computing with the title: 'Analysis of Digital Evidence in Identity Theft Investigations' from the University of Glamorgan. Her research interests include Digital Forensics, Identity Theft, Online Fraud, Digital Investigation Methodologies and Online Social Networking.