Internet of Things, Internet Service Providers and Unsuspecting Users

Christos Beretas

Abstract— **Internet of Things along with Internet Service Providers are a different philosophy and architecture but with a common denominator the Internet access. In both cases, users are unsuspected about the data being transferred but also collected for further analysis**

Index Terms—**Internet, ISP, Users, IOT**

I. INTRODUCTION

Internet of Things along with Internet Service Providers are a different philosophy and architecture but with a common denominator the Internet access. In both cases, users are unsuspected about the data being transferred but also collected for further analysis. When an internet of thing connects to the Internet it is difficult to ascertain that it sends data and the type of data it sends, on the other hand Internet Service Providers collect data, such as when a user was connected to the Internet but also what activities had, these data are stored and are accessible by the government when needed, in some countries users are also allowed to ask in writing from Internet Service Providers to send them a list of the websites they have visited. In both cases, users are literally unsuspected of being aware of the collection and processing of information that concerns them.

THE 5, 9 AND 14 EYES

"This Project" consists of 5, 9 and 14 countries that, depending on the agreements they have each other, cooperate and exchange information that according to their goals is considered to be of the utmost importance. The countries in this project are exchanging electronic information with the ultimate purpose of organizing of information sharing in conjunction with direct information and later planning further steps. The systems used (Echelon, Carnivore, WAN Sniffers, etc) have the ability to intercept information such as telephone communications, fax, real-time computer-based information exchange and e-mail. Some of the information monitoring systems have been installed in Internet Service Providers so that information collection is more efficient, and some information collection and analysis systems have also been deployed outside of the Internet Service Providers, but they have the ability to collect and analyze information. In theory, the citizens of the countries participating in the above project are exempt from the collection of information which, however, can not be proved in practice. So unsuspecting users are using the internet thinking that behind a computer screen they can not be identified for what they are doing and looking for on the internet, as well as various anonymous proxy servers that pop up like mushrooms and promise high level anonymity have been created by state agencies with in order to lure users that they offer anonymity, which in fact are "honey pot" systems that intercept in real time the user's Internet traffic, sometimes it is more secure to use the Internet as it is rather than using anonymous Proxy Servers of undoubted location, privacy and security.

II. RETHINK ABOUT IOT PRIVACY

There are everywhere today, in the homes in the form of smart devices, smart TVs and refrigerators, in cars using vehicle tracking and providing information to us, Chip-based software written in Chip-powered machine and running processes with power supply, networking devices which are adapted to networks with Servers for the purpose of not detected remote management, and much more. All of these smart devices send valuable data to the internet, which raises several questions:

- The kind of data they send and where.
- Data sent by smart devices is passed through Internet Service Providers of undoubtedly infrastructure and privacy.
- How secure are the networks that transfer the data.
- The Importance of Information.
- How much specialty is there about IoT safety.
- Who and if processes the data sent by smart devices.

A smart device can be a memory card, a computer memory, a chip on a Motherboard, etc. A smart device may be installed on a network with Servers and allow external users to access the internal network without this device being detected for years, such devices being "Snoopy" that are not visible to network administrators and have the ability for external users to have full access to the internal network. Smart devices can also negatively affect our lives, think of someone often recording our own routes and always knowing where we are going and watching without knowing it, even worse if someone would get illegal access to "Echo" devices, which are often connected to household appliances, besides having a complete profile about our habits, would have access to our home appliances even at times when we would not be at home with consequences that would be it.

A nightmarish but real-life scenario is someone installing harmful firmware on car driving systems, camera systems, medical and device monitoring systems, and other systems that are used for our safety, that would have incalculable consequences for our lives as well. we were literally trapped through intelligent systems. Every smart device is almost certain to have at least one security issue. Hackers when they lock up their target will try to take advantage of these security gaps.

Christos Beretas, Member of Alpha Beta Kappa Honor Society, Ohio, USA https://www.christosberetas.com

It is worth noting that companies that manufacture smart devices around 12% of their investments are used for security by applying techniques such as:

- Information and device security during design.
- Encrypt sensitive data
- No security for the transfer and use of data.

III. Conclusion

There are no secure electronic data transfer infrastructures, information security is “sacrificed” in the name of citizen security. Governments want and can watch other people about their habits. Users believe that by various anonymous means such as VPN, Proxy Servers are adequately protected. Smart devices still present vulnerabilities, which should be improved immediately by giving priority to research and development of systems that will restrict and protect people from the interception of their personal data when they use smart devices.

References

[1] Jack O'Neill (2005) ECHELON: Somebody's Listening.

[2] Brian Russell (2016) Practical Internet of Things Security.

[3] Dunham, Griffin S (2002) Carnivore, the FBI’s E-Mail Surveillance System: Devouring Criminals, Not Privacy.

[4] Nitesh Dhanjani (2015) Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts.