# MEMORANDUM

**Computer Science and Engineering**
**University of Washington**

**Date:** 01/23/2015

**To:** Whomever it may Concern

**From:** Mahir Kothary MK

**Subject:** Data Security and Privacy Issues Created By Internet Based Devices in Home Automation

In the context of the internet, security and privacy are among the most important current issues - for government, corporations and individuals. As technologies advance they generate increasingly complex threats to these issues, which take more than a few tweaks to change. One such category of disruptive technology is the Internet of Things (IoT), specifically in the domain of home automation. IoT is the all-pervading interconnected network of various devices and applications over the internet with the ability to communicate with internal or external environments. Collecting and sending data through wireless sources has dichotomously been a curse and a boon for data security and privacy. The dawn of 'IoT', which takes personal information and preferences, daily routines, mundane tasks, location security, etc., and uploads it to the internet, has given a virulent rebirth to these phenomena. Any byte of information can be unlawfully accessed, modified, manipulated and perpetrated. This memo discusses the security and privacy issues to an American home that uses such interconnectivity in its devices, provides some topical solutions and approaches to the problem, describes implications and concludes with key takeaways.

## IoT – What and Why

Since the advent of the Internet in the 1960s, emerging from ARPANET[1] to the present, there is a base of nearly 45% of the US population with access to the internet, and nearly 500 million home devices[2] are connected to the internet, with an average of 5.7 devices per household. This swiftly increasing percentage of access and of connected devices is a proportionate result of the addition of internet-based micro devices and other such technologies within the home. 'IoT' within a home could encompass everything from refrigerators to TVs to garage doors to security systems, creating the ideal 'connected' home. At the Black Hat Conference in 2013 (Annual Hacker Conference), one of the main themes was the vulnerability of such devices. As a demonstration, a hacked $6000 Japanese toilet bidet proved to be the turning point of IoT device security[3]. Through it, hackers opened up front door locks, accessed power outlets, and converted baby monitors to their own little spy machines. IoT brings out several issues which include, but are not limited to, loss of privacy and data protection, autonomous communication, unlawful profiling, malicious attacks and the repurposing of data. While manufacturers scurry to search for ideas for new IoT devices, engineers are frenetically searching ways to completely secure the connectivity. The Consumer Electronics Show (CES) 2015, heavily focused on proving the success of IoT by overcoming the security flaws and creating seamless connection between different devices.

## The General Problem and Leveraging New Technologies to Secure IoT

In reference to the numbers and context mentioned above, CISCO[4] predicts that nearly 25 billion devices, all across the world, will be connected by 2015, giving IoT an overall market value of $14.4 trillion. For a market of this size, with these many devices, a high degree of reliability is needed. To

tackle these reliability issues[5], there are several security requirements which need to be addressed. These mainly include: Data Authentication, Endurance towards Attacks, Client Privacy and Access Control. The following paragraph briefly describes how each is addressed.

*Data Authentication*: All information retrieved from the devices, as well as general device information should require special user identity data to access. *Endurance towards Attacks*: if the devices are ever attacked by hackers, the system should be resilient enough to not only keep them at bay, but also not fail. *Client Privacy*: Measures should be taken such that only the information provider is able to infer from observing the use of the lookup system related to a specific customer; at the least, inference should be very hard to conduct. *Access Control*: those who do provide this information - both the users and the service provider - must be able to implement security protocols on the device.

One of the primary concerns is that the current IoT regulatory model is based on parameters created within the service provider itself, paying scant attention to legislations such as '*IT-Security*'[5], which cover initiatives and directives for IT-Security Standards for a device, and to '*Prohibition*', which lists areas where use of devices is forbidden for security purposes. Experts say that the volatility of the internet requires a specific and varied legal framework which recognizes the span, pervasiveness and density of various internet-based operations and devices[5].

IoT in home automation is becoming more affordable[6] because the base has widened and the platform is now on the mobile, so that many apps are available. But that means multiple wireless protocols and hence the security/privacy issue gets more complicated.

A few existing privacy enhancing technologies have been employed: these include Virtual Private Networks (VPN)[i], a network created between partners; Onion Routing[ii], a network with multiple layers of encryption – like an onion; Private Information Retrieval (PIR) systems as well as use of Peer-to-Peer (P2P) networks. However each of these has their own shortcomings, which make it impractical to implement in home automation. For example, VPNs can only be used over certain networks, so a homeowner will not have constant access to the internet devices connecting the home. Onion routing, while a strong security method, is inefficient because of the inordinately higher time (and hence expense) taken in encoding and decoding the data through various sources. Lastly, PIR systems have similar issues as Onion routing and VPNs where because of security protocols, there are associated performance and scalability issues. P2P's fix all of the following, however the primary issue being that the data/user is not encrypted but the channel via which the data being sent is, so simple access to the authorization keys may allow data access. However these are rare cases.[5]

Credible not-for-profit organizations such as OWASP (Open Web Application Security Project) have presented specific solutions/approaches to the Top 10 issues that directly affect the IoT space. They recognize that security and privacy are the key impediments to progress here, and hence have committed resources to continuously monitor developments.[7]

Other than these, there are suites of prevention software for IoT devices to detect possible threats and therefore send alerts to increase security on the device before an attack can happen. These include threat analysis, anti-malware and anti-virus protection, physical security and incident reports. Specifically, at the US National Cyber Security Partnership[8], a public-private initiative, specific recommendations are given in terms of usage of security measures which can mitigate or eliminate the risk factors associated with IoT in a home automation situation. The article also states a simple thing: If the end point in a home automation system is going to be a cell phone, then it is imperative to study and understand the security measures associated with the latter, including the simple habit of using its PIN feature. This point underscores how weak the link can be in the chain of safe computing.

One ‘fix’ that keeps appearing for security in the IoT infrastructure is pervasive device identification. Whilst this is not panacea, it significantly reduces the probability of the problem occurring. Continuous research is being done including DARPA’s recent initiative to use transparent computing as the basis for a permanent solution.[9]

## Securing the future through Jobs, Research and Development

FTC Chairwoman Edith Ramirez, recently, said that IoT has the potential to improve everything from global health to economic growth, but stressed that along with the benefits of connected devices come serious privacy and security risks[10]. While IoT generally, and in home automation specifically, does pose a threat to certain jobs, it does create a plethora of other jobs and opportunities from software to hardware, and from business management to sales, while simplifying daily tasks. Fixing the security and privacy problems, would require several experts, legal representatives, test users, as well as engineers; then, one would be able to work towards a solution that matches legal frameworks, cost considerations and system efficiencies. Employment opportunities and entrepreneur idea monetization should help solve the problem, because customer pressure has often solved problems in the past. Because of the global nature of the issue, intense R&D would be required, encouraging large corporations/business houses to make investments and help growth.

## Always staying a step ahead

The potential market for IoT is large, but currently is niche. Among other things, the cost of purchase is yet to come down, even though the cost of manufacturing is reducing. With enhancement of security and privacy features in internet based devices, engineers can develop a ‘smart system’ in small homes, offices and stations, thereby increasing the comfort levels of the average human being. But we must remember that technology does tend to catch up, both positively and negatively, and new solutions may get followed by new attacks. The only way to continue ensuring that all devices are safe is to allow the data to run via channels which can be easily updated and changed as security concerns rise and adapt to the previous framework which was created. This game of cat and mouse opens up doors to a lot more criminal attempts and hackers aiming to disrupt the industry, causing harm to the common man. It will be important to remain one step ahead by sticking to tested solutions and incorporating new ones to make IoT in home automation as ubiquitous as the mobile phone[11].

## Works Cited


[1] S. Babar, "Proposed Security Model and Threat Taxonomy for the Internet of Things," Springer-Verlag Berlin Heidelberg, 2010.

[2] PostScapes, "Internet of Things Market Size," PostScapes.

[3] H. Kelly, "'Smart homes' are vulnerable, say hackers," CNN, 2 August 2013. [Online]. Available: http://www.cnn.com/2013/08/02/tech/innovation/hackable-homes/. [Accessed 15 January 2015].

[4] A. Collins, "The Internet Of Things Part 2: The Old Problem Squared," Morrison & Foerster LLP, 2014.

[5] R. H. Weber, "Internet of Things – New security and privacy challenges," Computer Law & Security Review, vol. 26, no. 1, pp. 23-30, 2010.

[6] P. Moorhead, "The Problem With Home Automation's Internet Of Things (IoT)," Forbes, September 2013. [Online]. Available: http://www.forbes.com/sites/patrickmoorhead/2013/09/26/the-problem-with-home-automations-iot/. [Accessed January 2015].

[7] OWASP, "Internet of Things Top Ten Project," OWASP, [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_10_for_2014. [Accessed 18 January 2015].

[8] A. Sacco, "Cyber security expert: Internet of things is 'scary as hell'," InfoWorld, 26 March 2014. [Online]. Available: http://www.infoworld.com/article/2610666/intrusion-detection/cyber-security-expert--internet-of-things-is--scary-as-hell-.html. [Accessed 20 January 2015].

[9] DARPA, "Broad Agency Announcement: Transparent Computing (TC)," DARPA, Arlington, 2014.

[10] E. Ramirez, "Opening Remarks of FTC Chairwoman Edith Ramirez," FTC, Las Vegas, 2015.

[11] The Economist, "Home, hacked home," The Economist, 12 July 2014.


[i] **VPN**: These are private networks established by partners, where only partners have access and can be accessed over certain networks.

[ii] **Onion Routing**: An Internet-based system to avoid eavesdropping and data extraction via multiple layers of encryption