https://doi.org/10.48009/2_iis_2020_57-63

PRIVACY AND SECURITY CONSIDERATIONS OF THE IOT: APPROACHING PRIVACY BY DESIGN

Christopher B. Davison, Ball State University, cbdavison@bsu.edu
Edward J. Lazaros, Ball State University, ejlazaros@bsu.edu
Jensen J. Zhao, Ball State University, jzhao@bsu.edu
Allen D. Truell, Ball State University, atruell@bsu.edu
Brianna Bowles, Ball State University, blbowles@bsu.edu

ABSTRACT

The Internet of Things (IoT) is an ever-expanding network of sensors and devices. These devices and sensors can present several privacy and security concerns regarding the human activity that is monitored and logged. In military environments, the consequences of privacy leakage can be enormous. Engineers and designers of the IoT would do well to adhere to privacy by design principles when creating IoT sensors or devices and expanding the IoT.

Keywords: Privacy, IoT, Design, Data, Security.

INTRODUCTION

The Internet of Things (IoT) is a growing network of connected devices and sensors. As the IoT grows, so does the privacy, legal and security concerns. The authors of this paper will present discussions on a number of these concerns within the framework of the IoT. The purpose of this phenomenological paper is to provide awareness of IoT privacy and security issues within the IoT and advocate for a holistic approach to address these issues.

To present privacy in the IoT context, a substantive review of the literature is presented. The literature review will set the context and provide definitions associated with IoT privacy and information privacy as well as discuss legal aspects of IoT. The genesis of machine to machine communication is presented as well as recent work in privacy and IoT.

Following the literature review, a section on military considerations of IoT and the Internet of Battle Things (IoBT) will be highlighted. In this section, a discussion of individual privacy concerns as well as information leakage is provided

Finally, a discussion of the concept of Privacy by Design (PbD) will be presented. PbD is the concept that privacy should be engineered into systems at every stage of development. This puts privacy on par with other design principles during systems creation. In addition, a discussion on the concept of Differential Privacy (DP) as a privacy enhancing technology is shared.

LITERATURE REVIEW

The Internet of Things

The Internet of Things (IoT), is the concept of connecting the digital world to the physical world. This is accomplished through a variety of communication technologies (e.g., Radio Frequency Identification (RFID), WiFi, Bluetooth, ZigBee), sensorized technologies (e.g., phones, motes, wearables, embedded sensors) as well as storage and analysis systems (e.g., context-aware computing, cloud-based architectures, ubiquitous computing) that are continuously generating and processing vast amounts of data (Suresh et al., 2014). The data can be sensorized human activity generated or even Machine to Machine (M2M) generated.

Since the 1800s, the idea of machines communicating with one another has been envisioned. The first steps in that area date back to the 1830s when the telegraph was invented, and then advancing on to the first radio voice transmission in 1900. Following shortly after, the development of computers began by the 1950s. The Internet itself began as a part of the Defense Advanced Research Projects Agency (DARPA) in 1962 and evolved into ARPANET in 1969. The year 1993 introduced Global Positioning Satellites (GPS) and the Department of Defense enabled twenty-four functional satellites and soon to follow was the use of commercial satellites. Another important component of the development of IoT was TCP/IP and the subsequent creation of IPV6 in order to increase address space.

The first use of the IoT was in the early 1980s via a Coca Cola machine at Carnegie Mellon University. The soda machine was linked to a computer that informed programmers how many sodas were in the machine and what their respective temperatures. In 2013, the IoT began using multiple technologies including the Internet, wireless communication, micro-electromechanical systems (MEMS), and embedded systems. In addition, the IoT is also supported by traditional fields of automation, wireless sensor networks, GPS, and control systems. Radio Frequency Identification (RFID), an automatic identification technology allowing things to be linked with virtual identities through identification numbers has also played a crucial role in the evolution of the IoT (Foote, 2016).

Modern IoT connects real world sensors, electronic devices and systems to the Internet. These devices and systems consist of consumer services, smart houses, smart objects, smart energy (meters and grids), smartphones and tables, Internet connected cars, wearable devices (health and fitness monitoring devices, watches, smart clothing, smart pet collars or implanted RFIDs, and human implanted devices (e.g., pacemakers) (Murrill et al., 2012). The IoT also consists of environment sensors and wireless sensor networks that can measure spaces, weather, perform health care monitoring, industrial monitoring, data logging, and spatial monitoring (Andrea et al., 2015).

The implementation of the IoT uses various existing network technologies to facilitate data communication. RFID technology uses microchips for data transmission in wireless data communication. Tags/labels are attached to objects acting as electronic barcodes. Wireless Sensor Networks (WSN) are geographically distributed small sensors that monitor physical environment conditions (Lopez et al., 2012). Additionally, Cloud Computing enables the sensing and processing of data and allows data to be stored and used for smart monitoring and analysis. .

There are many laws in the U.S. concerning the Internet, data security, and privacy, of which the Privacy Act of 1974 creates a solid foundation (NortonOnline). The Privacy Act established control over the collection, maintenance, use, and dissemination of personal information by agencies in the executive branch of the U.S. government. The following laws currently in place to solidify rights as a consumer include: Electronic Communications Privacy Act (ECPA), Computer Fraud and Abuse Act (CFAA), Cyber Intelligence Sharing and Protection Act (CISPA), and Children’s Online Privacy Protection Act (COPPA).

The ECPA (passed in 1986) allows the U.S. government to access digital communications (emails, social media messages, information on public cloud databases, etc.) without a warrant if the information desired is 180 days old or older. The government is given the information from companies. In addition, the ECPA also determines when the government is allowed access to GPS tracking via cellular devices. The CFAA was passed in the late 1980’s and revised nearly ten years later. This act allows for protection against unlawful access and sharing of protected information. CISPA was introduced as an amendment to the National Security Act of 1947 (which does not cover cyber-crime). This Act involves how to share information on possible cyber threats with the federal government. Finally, COPPA’s last amendment was implemented in 2013. It requires websites that collect information on children under 13 years of age to comply with the Federal Trade Commission (FTC). The FTC is responsible for investigating a website’s language, content, advertising, graphics and features, and intended audience to make sure it is child appropriate.

As the interconnection of devices with the real world continues, there are an abundance of advantages that must be put into perspective. For instance, changes in the way the world works and lives by saving time and resources, presenting new opportunities for growth, innovation, and the ease of knowledge exchange between multiple entities. Maayan (2019) reports that there were more than 20 billion IoT devices connected in 2019. Many experts predict up to 25 billion connected IoT devices by 2021. Due to this growth and use of IoT, there are concomitant concerns such as security, privacy and trust threats associated with putting personal or privacy-related information on the devices.

Andrea et al. (2015) defines (1) security and privacy and (2) trust in the IoT. Those researchers state that data security and privacy refer to the protection of any collected or stored data in any IoT system. This means that at any moment the IoT system needs to provide data confidentiality with integrity and availability. This can be achieved by utilizing authentication, access control, data encryption, and data availability and redundancy through back-ups, etc. They define trust simply as the reinforcement of the security goals previously mentioned, consisting of further objectives as well. These objectives include trust relations between each IoT layer, trust for the security and privacy at each IoT layer, and trust between the user and the IoT system. They go on to explain a broader overview of security vulnerabilities and attacks in IoT systems.

Andrea et al. (2015) classify IoT vulnerabilities in four classes: physical, network, software and encryption attacks. Physical Attacks consist of eight sub-categories, all of which are attacks focused on the hardware components of the system and the attacker must be physically close or into the system to achieve a successful attack. Network Attacks consists of nine sub-categories in which take place on the IoT system network. Software attacks are the main source of security vulnerabilities, in which the system is exploited using Trojan horse programs, worms, viruses, spyware and malicious scripts that can steal and/or harm information. Encryption Attacks break the encryption scheme within an IoT system.

Privacy/Security and the IoT

Many IoT devices use the unlicensed commercial Radio Frequency (RF) spectrums (900 MHz, 2.4 Ghz, 5.8 GHz). This includes common WiFi and Bluetooth enabled devices. As these spectrums are widely known and standardized protocols are commonly used, this invites privacy issues and security concerns in many forms (Handel et al., 2018).

Privacy and security are often overlapping concepts. That which is private is secure and that which is secure is private. The IoT adds another layer of security concern: physical security.

As Hwang (2015) points out, the IoT is closely related to our non-virtual lives. This means that IoT devices, due to the nature of their close proximity to users, are in direct physical contact with users. In the past, security was related to information leakage and theft. With IoT and the added physical locality threats, IoT users can face direct physical threats to their safety and security. With this spatial information, an attacker who is intent on causing physical harm to their target will know the target’s location down to a granular level.

As new IoT devices come online, the sophistication of attacks and damage from these attacks increase (Zhou, Zhang, Liu, 2018). Statista, The Statistics Portal (2017), projects the number of IoT devices to be online by 2025 to be over 75 billion. As many IoT based attacks are Distributed Denial of Services (DDoS), this provides an astonishing number of devices to an attack platform.

The Mirai Botnet attack on Dyn (a DNS provider) in 2016 is an example of a successful DDoS attack. Netflix, Twitter and a number of other companies were impacted by this attack. The attackers infected routers and cameras to launch their attack on Dyn.

Mirai is also reported to be responsible for the *Cold Attack* against two apartment buildings in the Finish city of Lappeenranta. As another DDoS attack, the heating controllers of the buildings were overwhelmed with IP packets and this caused them to continually reboot. The effect of this attack was that the controllers could not turn on the heating in the buildings and left the residents with no heat in November.

The TOR-based Brickerbot is another example of a DDOS attack that targets IoT devices. This malware infects cameras and other devices through a Telnet port (TCP port 23) like Mirai. Once inside, the malware will permanently destroy the device and *brick* the target device.

More traditional forms of attack exist with IoT devices: bluejacking, bluesnarfing, spoofing, and snooping. Bluejacking refers to the practice of sending unwanted information to a bluetooth enabled device (e.g., pairing with unsuspecting headphones on an airplane). Bluesnarfing is when an attacker downloads information (e.g., contact lists, photos) from a vulnerable device without consent. A spoofing attack is when an attacker fraudulently impersonates a device on a network (usually for nefarious purposes). Finally, a snooping attack is the passive monitoring of devices on a network looking for information such as credit cards, user IDs, passwords or other sensitive information. In any of the cases, the attacks are clearly invasions of privacy with security ramifications.

Special Considerations: Military Environments

Military environments present unique circumstances for IoT and privacy. As the US military moves toward the Internet of Battlefield Things (IoBT) and smart, sensorized environments, privacy and the perception of privacy may degrade. Archer et al. (2020) discuss DARPA-funded IoT privacy research onboard a Navy vessel. The researchers found that privacy was a concern across the entire chain of command spectrum. From the newly enlisted to the career officers, privacy and the perception of privacy was a continual discussion and topic of concern. This concern was especially prevalent within the domain of onboard IoT and human-sensing devices.

According to Castiglione et al., (2017) , the IoBT "involves the full realization of pervasive sensing, pervasive computing, and pervasive communication, leading to an unprecedented scale of information produced by the networked sensors and computing units" (p. 18). The concept is to have an integrated battlefield. This ranges from individuals wearing sensors to entire branches of service coordinating information. What is apparent is the network and security implications of this massive amount of data. What is not so apparent is the issue of individual privacy.

Privacy and situational awareness in the IoBT are often at odds. Sfar at al. (2017) discuss this dichotomous situation in their research (case study) on military IoBT. These researchers point out that not all IoBT information (e.g., data) is required to be passed to the higher layers of decision makers. It is logical to conclude that this data may even be counterproductive: irrelevant IoT information may congest the network and provide no actionable information. Sfar et al. (2017) conclude that sensitive information should be hidden, and only essential information be passed to the relevant battle applications.

Another privacy aspect of the IoBT is information leakage used by adversaries to target an individual for assassination or capture. Consider a well-informed attacker that uses IoT/IoBT devices to triangulate a target. The attacker will know the location of the target and the time the target is at that location. If the attacker only possesses a one-use weapon (e.g., bomb, IED) the IoBT information leakage (location, time, personnel information) will increase their likelihood of a successful attack. In this example, privacy loss due to the IoBT could be fatal.

FINDINGS: ADDRESSING PRIVACY

Privacy by Design

As discussed in the previous sections, the IoT presents many security and privacy issues. One possible solution to these issues is to adopt the Privacy by Design (PbD) principles introduced by Cavoukian (2011). According to Li and Palanisamy (2018), careful applications of privacy enhancing technologies (PETs) such as PbD, can help meet legal and functional requirements of privacy within the IoT environment.

PbD is a beginning-to-end framework that infuses privacy and privacy mitigation strategies in every aspect of the technology design process. Instead of post-de-facto retrofits of privacy-flawed technologies, Cavoukian (2011) is a proponent of building in privacy by design principles (see Figure 1) from inception. This alleviates the need to retrofit privacy into technology once the technology is released, or worse yet: cracked, hacked, attacked or otherwise infiltrated.

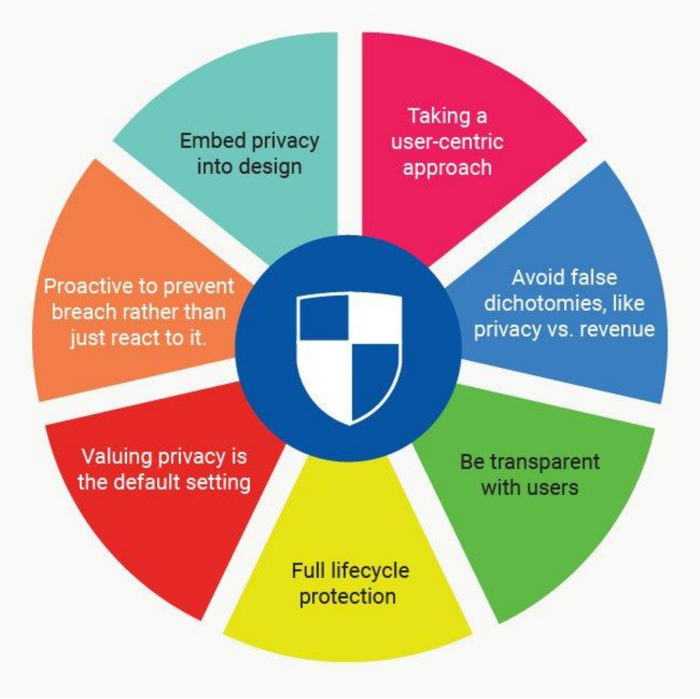
Embed privacy into design
Taking a user-centric approach
Avoid false dichotomies, like privacy vs. revenue
Be transparent with users
Full lifecycle protection
Valuing privacy is the default setting
Proactive to prevent breach rather than just react to it.

Figure 1. Privacy by Design. This figure illustrates the seven principles of Privacy by Design (Mackie, 2018).

PbD is crucial in decreasing privacy risk and increasing trust. The creation of systems, products, processes and projects using this infrastructure upholds various beneficial aspects. First, identification of potential problems in the early stages and addressing them quickly. Second, it strengthens data protection and privacy across organizations. Finally, organizations meet legal obligations instead of breaching data protection act.

The Role of Privacy by Design in Protecting Consumer Privacy (2010), describes the use of PbD in behavioral advertising. Advertisers are able to track, collect, and combine information about a consumers' browsing activities, and keep the information for extended periods of time. By implementing PbD, trade associations and companies within the behavioral advertising ecosystem could prevent deceitful practices (re-spawning and spying on browser histories), as well as help build rapport with consumers in hopes they will become more willing to share their data for behavioral advertising. The consumers willing to allow for collection would feel confident knowing what is being collected is transparent, limited in scope, secure, and accessible to them.

Privacy and the Invasion of Privacy

One aspect of the IoT that invites privacy scrutiny is the always-on nature of the sensing environment. The majority of these sensors are designed to continuously monitor and transmit data. In the most benign case of misuse, data is repurposed by organizations beyond the original intent of the data collection (Walker, 2014). However, continuous monitoring of people and spaces provides a data rich environment for a potential adversary to develop *priors* regarding a target. Priors are learned behaviors or other information that assists an adversary in developing a targeting portfolio on a victim.

Consider an adversary that wishes to invade the privacy of an intended target. The adversary can passively monitor a parking lot visually or with any manner of IoT network analysis tools. If the target is the first in the parking lot in the morning, this prior can be utilized to build a larger portfolio of activity. If the target triggers other IoT sensors after exiting the car and entering the building, the adversary can reasonably deduce the location, path, trajectory, speed, and destination of the target. With some amount of skill (or luck) the adversary can sense the RFID, WiFi, or Bluetooth signature of the target's devices (e.g., cell phone, RFID badges, etc.) or take advantage of other information "leakage" (A. I. T., 2019) during computation. Using those priors, the adversary can build a reasonably accurate schedule of the target that includes dates, times, activities, and associations.

Differential Privacy as a Privacy Enhancing Technology

To mitigate the leakage effects of large data sets on privacy, work in the field of Differential Privacy (DP) is expanding. Dinur and Nissim's (2003) work on the Fundamental Law of Information Recovery demonstrates that privacy can be lost with a few well-designed queries into large data sets. This leads to the observation that *noise* can be injected into the data for privacy preservation purposes. Dwork et al. (2006) provided a formalized framework, the concept of ε-differential privacy, to quantify the amount of noise required to provide privacy. More recent work in the field (Wagh et al., 2020) investigates privacy (injection of noise) versus utility (accuracy of information from a DP data set) and sensitivity of information release mechanisms (Laud et al., 2020).

CONCLUSION

In this paper, the phenomena of privacy and security issues related to the IoT was presented. As the IoT increases in size and scope, privacy and security become more important. The paper begins with a literature review providing a background for the genesis of the IoT dating back to the telegraph. From that point, the literature review explored the evolution of the IoT up to current research work in that domain. Selected IoT attacks were presented in the literature review as well. Additionally, a discussion of military considerations of the IoT and the IoBT. Privacy is a concern within the military from all strata of personnel: enlisted and officers alike. It was shown that information leakage from IoT/IoBT devices could assist adversaries in targeting.

In order to address privacy considerations in the IoT, two significant privacy-enhancing technologies are advocated: Cavoukian's (2011) Privacy by Design, and Differential Privacy. Each of these technologies can contribute to a more secure and more private IoT.

Cavoukian's (2011) Privacy by Design approach is advocated as a design methodology for IoT technologies. This approach is such that privacy is an integral aspect of systems engineering and is prevalent in all design stages. This serves to put privacy as a design principle and not as an after-thought.

The continuous sensing nature of IoT devices presents a problem. As these devices were engineered to continually be reporting data, a surveillance society becomes a reality. Priors are continually generated and research work in this area demonstrates that only a small number of queries over a significantly large data set can result in privacy loss.

Differential Privacy is a privacy enhancing technology that addresses information leakage within large data sets. With Differential Privacy techniques, it is show that privacy can be enhanced with the injection of noise into data. However, there is a tradeoff between the amount of noise injection (e.g. privacy enhancement) and data accuracy.

REFERENCES

A. I. T. (2019). *Cross Sectoral Cybersecurity Building Blocks.* Cyber Security for Europe. Retrieved from https://cybersec4europe.eu/wp-content/uploads/2020/01/D3.2-Cross_sectoral_cybersecurity_building_blocks.1.0.final-Submitted.pdf

Andrea, I., Chrysostomou, C., Hadjichristofi, G. (2015). Internet of Things: Security vulnerabilities and challenges. *2015 IEEE Symposium on Computers and Communication (ISCC)*, Larnaca, 2015, pp. 180-187

Archer, D., August, M.A., Bouloukakis, G., Davison, C. B., Diallo, M. H., Ghosh, D., Graves, C. T., Hay, M., He, X., Laud, P., Lu, S., Machanavajjhala, A., Mehrotra, S., Miklau, G., Pankova, A., Sharma, S., Venkatasubramanian, N., Wang, G., & Yus, R. (2020). *Transitioning from Testbeds to Ships: An Experience Study in Deploying the TIPPERS IoT Platform to the US Navy.* Manuscript in preparation.

Castiglione, A., Choo, R. K., Nappi, M., & Ricciardi, s. (2017). Context Aware Ubiquitous Biometrics in Edge of Military Things. *IEEE Cloud Computing*, *4*(6), 16-20.

Cavoukian, A. (2011). Privacy by design: origins, meaning, and prospects for assuring privacy and trust in the information era. In *Privacy protection measures and technologies in business organizations: aspects and standards* (pp. 170-208). IGI Global.

Dinur, I., & Nissim, K. (2003, June). Revealing information while preserving privacy. In *Proceedings of the twenty-second ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems* (pp. 202-210).

Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In *Proceedings of the Third conference on Theory of Cryptography (TCC'06),* Shai Halevi and Tal Rabin (Eds.). Springer-Verlag, Berlin, Heidelberg, 265–284.

Foote, K. D. (2016) A Brief History of the Internet of Things. *DATAVERSITY*. Retrieved from www.dataversity.net/brief-history-internet-things/#.

Handel, T., Schreiber, M., Rothmaler, K., & Ivanova, G. (2018). Data Security and Raw Data Access of Contemporary Mobile Sensor Devices. In *World Congress on Medical Physics and Biomedical Engineering 2018* (pp. 397-400). Springer, Singapore.

Hwang, Y. H. (2015, April). Iot security & privacy: threats and challenges. *In Proceedings of the 1st ACM workshop on IoT privacy, trust, and security* (pp. 1-1).

Laud, P., Pankova, A., & Pettai, M. (2020). A Framework of Metrics for Differential Privacy from Local Sensitivity.

Proceedings on Privacy Enhancing Technologies, 2, 175-208.

Li, C., & Palanisamy, B. (2019). Privacy in Internet of Things: From Principles to Technologies. *IEEE Internet of Things Journal*, 6(1), 488-505.

López, T. S., Ranasinghe, D.C.,Harrison, M., McFarlane, D. (2012) Adding sense to the Internet of Things. *Personal and Ubiquitous Computing, 16*, 291-308. https://doi.org/10.1007/s00779-011-0399-8

Maayan, G.D. (2019). *The IoT Rundown For 2020: Stats, Risks, and Solutions.* Security Today. Retrieved from https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx

Mackie, J. (2018). *Privacy by Design.* Terms Feed. Retrieved from https://www.termsfeed.com/blog/privacy-design

Murrill, B. J., Liu, E. C., & Thompson, R. M. (2012, February). *Smart meter data: Privacy and cybersecurity*. Congressional Research Service, Library of Congress.

NortonOnline. (n.d.). *What Are Some of the Laws Regarding Internet and Data Security?.* Retrieved from https://us.norton.com/internetsecurity-privacy-laws-regarding-internet-data-security.html

Sfar, A. R., Chtourou, Z., & Challal, Y. (2017, February). A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges. I*n 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C)* (pp. 101-105). IEEE.

Statista: The Statistics Portal. (2017). *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions).* Retrieved from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Suresh, P., Daniel, J. V., Parthasarathy, V., & Aswathy, R. H. (2014, November). A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. In 2014 *International conference on science engineering and management research (ICSEMR)* (pp. 1-8). IEEE.

The Role of Privacy by Design in Protecting Consumer Privacy. (2010, January 28). Retrieved from https://cdt.org/insights/the-role-of-privacy-by-design-in-protecting-consumer-privacy-1/#3

Wagh, S., He, X., Machanavajjhala, A., & Mittal, P. (2020). DP-Cryptography: Marrying Differential Privacy and Cryptography in Emerging Applications. arXiv preprint arXiv:2004.08887.

Walker, K. (2014, July 16). *The legal considerations of the Internet of Things.* Retrieved from https://www.computerweekly.com/opinion/The-legal-considerations-of-the-internet-of-things

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, *6*(2), 1606-1616.