Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2018 Proceedings | Southern (SAIS)

Spring 3-23-2018

EXPLORING USER PRIVACY BASED ON HUMAN BEHAVIOR WITH INTERNET OF THINGS DEVICES AT HOME (FORMATIVE RESEARCH)

Jeffrey P. Kaleta
Georgia Southern University, jeff.kaleta@gmail.com

Russell Thackston
Georgia Southern University, rthackston@georgiasouthern.edu

Olajide Ojagbule
Georgia Southern University, olajide_o_ojagbule@georgiasouthern.edu

EXPLORING USER PRIVACY BASED ON HUMAN BEHAVIOR WITH INTERNET OF THINGS DEVICES AT HOME (FORMATIVE RESEARCH)

Jeffrey P. Kaleta
Georgia Southern University
jkaleta@georgiasouthern.edu

Russell Thackston
Georgia Southern University
rthackston@georgiasouthern.edu

Olajide Ojagbule
Georgia Southern University
olajide_o_ojagbule@georgiasouthern.edu

ABSTRACT

The proposed research initiative is aimed at investigating potential security and privacy vulnerabilities in home based Internet of Things (IoT) smart devices, such as Amazon Echo, Google Home, and smart home appliances, by analyzing the type, nature, and frequency of its encrypted, network communications. Such communications may reveal private information about the activities occurring within a home, as well as behaviors, relationships, and habits. Regardless of the quality of encryption used for network communications, digital messages expose certain information in much the same way as a sealed envelope sent via the postal service. The results of this formative research initiative will encourage better design of future home based IoT smart devices for security and privacy, as well as educate consumers on risks.

Keywords

Internet of Things (IoT), privacy, security, networking

INTRODUCTION

Current trends in innovation include the injection of Internet of Things (IoT) smart devices into homes to assist and improve people's lives. Smart devices range from products that control home heating and cooling (e.g. NEST thermostats), room by room lighting, personal-style assistants (e.g. Amazon Show), and human-like assistants delivering information and home automation through simple voice commands (e.g. Amazon Echo). On the surface, these devices appear as benevolent additions to a home, enabling users to control their living environments more efficiently. However, unbeknownst to most users, home based IoT smart devices operate on an expanded network connected to sources outside the home, transmitting data to distant servers, collecting information about users' habits and private behaviors. Best practices suggest encryption schemes are applied to these transmission, yet the nature of the passage, the frequency, and the device type may enable third parties eavesdropping, allowing them to ascertain information about the occupant's daily behaviors. Similar to data transmission that occurs while users interact with internet browser, an IoT smart devices within residential homes transmit information which, if captured, could reduce one's privacy and place them at risk for malicious attacks.

The purpose of this formative research initiative is to investigate vulnerabilities that may be present in IoT smart home devices. Furthermore, we plan to use the findings from this study to develop a basis to research other areas where home based IOT smart devices and other similar devices can be used to detect occupant behaviors within a home. These finding may also provide opportunities to studies focusing on the convergence of humans and information technology including privacy and ethical concerns.

APPROACH

To plan of study for this project includes the purchase and installation of a variety of IoT smart devices designed for home use. The smart devices will be connected to wireless access point which will log all network traffic between devices and servers for analysis. Using software analysis tools, like Wireshark (wireshark, n.d.)(see Figure 1), the captured data packets will be analyzed to help identify unique profiles of packets during transmission. Using machine learning tools, unique features discovered in the packets will be further analyzed looking for behavioral patterns associated with the living activities of the home occupant.

To illustrate how this will be accomplished, consider typical behaviors surrounding the use of a smart home lighting device (e.g. TP-LINK device) in a residential environment. Common use activity for a light bulb placed in living room has the potential to indicate when the room is occupied in the absence of natural light, such as in the early evenings close to sunset, or early mornings near dawn. The signal transmitted to the light bulb, indicating an on or off state, can be evidence of a person's wake

time (e.g. turning it on in the mornings), a person's leisure time (e.g. turning it on in the evening), or a person's sleep time (e.g. turning it off in the evening). Continual monitoring of this data can quickly provide behavioral indicators of a home's occupants. Related studies using smart home sensors have determined similar outcomes when monitoring daily health related behaviors of senior citizens for the purpose of tracking their health **(**Botón-Fernández and Lozano-Tell, 2011; Park et al., 2010**)**.

The above example creates an opportunity for malicious attackers seeking opportunities to exploit user vulnerabilities **(**Mitchell & Chen, 2015**)**. Similar to monitoring "snail mail" received through the postal service, monitoring of a household's data packets, regardless of the content of the messages, can be revealing about occupants' behavior leading to privacy concerns (Hartogs, 2013; Nixon 2013).

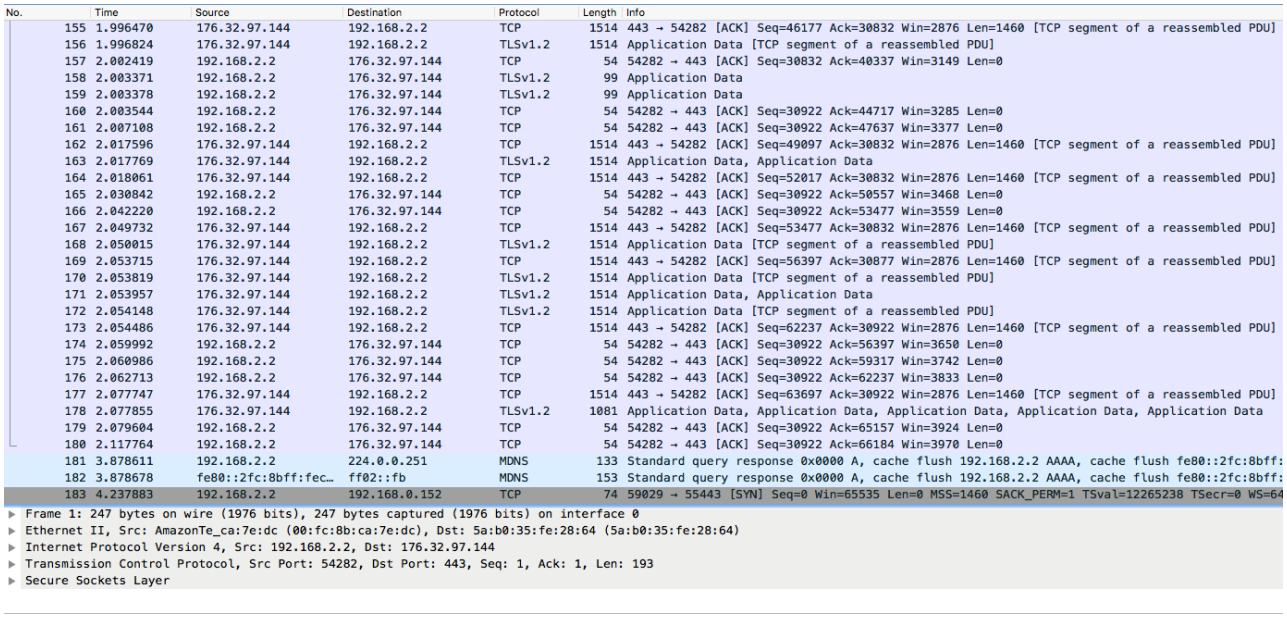

Figure 1. Data capture from the Wireshark network analyzer

EXPECTED OUTCOMES

The anticipated outcomes of this study are aimed at identifying the degree of vulnerabilities and loss of privacy associated with home IoT smart devices. We intend on gaining an understanding of the types of attack home owners can be vulnerable to and what type of information is available to third parties. These outcome will highlight the extent to which home IoT smart devices may hinder people's privacy and bring awareness to homeowners regarding the degree of privacy forfeited for the conveniences gained. Understanding these boundaries can provide a baseline to investigate the degree to which people are willing to surrender levels of privacy, or alter their usage of home IoT smart devices, when home IoT smart devices are introduced into the home and the limitations to privacy are communicated to home owners.

With the evidence collected, additional outcomes from this study can also provide pathways for remedies to home owners that care to operate their home IoT smart devices in a manner to gain preferred levels of privacy. This can include technical solutions available to developers of home IoT smart devices, or those who install home IOT devices, assisting in the prevention of malicious attacks to home IoT networks.

Finally, we'd hope that with the investigation of technology within the home will provide a baseline approach for evaluating new home-based technology. This work may also inspire other research activities, similar in nature, which can improve upon the evaluations resulting from this study. This will benefit researchers investigating individual level behaviors using home based IoT smart devices, developers interested in providing new home IoT smart devices, and finally all parties interested in maintaining a higher degree of privacy and security for home IoT smart device users.

REFERENCES

1. Boton-Fern´ndez, V., & Lozano-Tello, A. (2011). Learning Algorithm for Human Activity Detection in Smart Environments (pp. 45–48). *IEEE*. https://doi.org/10.1109/WI-IAT.2011.80
2. Hartogs, J. (2013, July 4). Report: Postal Service uses "spying" programs similar to NSA. Retrieved October 15, 2017, from https://www.cbsnews.com/news/report-postal-service-uses-spying-programs-similar-to-nsa/
3. McFadin, P., & Cassandra, A. (2015). Internet of Things: Where Does the Data Go? Retrieved October 5, 2017, from https://www.wired.com/insights/2015/03/internet-things-data-go/
4. Mitchell, R., & Chen, R. (2015). Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. *IEEE Transactions on Dependable and Secure Computing*, 12(1), 16–30.
5. Nixon, R. (2013, July 3). U.S. Postal Service Logging All Mail for Law Enforcement. *The New York Times*. Retrieved from https://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html
6. Park, K., Lin, Y., Metsis, V., Le, Z., & Makedon, F. (2010). Abnormal human behavioral pattern detection in assisted living environments. *In Proceedings of the 3rd International Conference on Pervasive Technologies Related to Assistive Environments* (p. 9). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1839305
7. Wireshark · Go Deep. (n.d.). Retrieved January 4, 2018, from https://www.wireshark.org/