**Examining the Threats From IoT in Home Networks**

In 1966, German Computer Scientist Karl Steinbuch is reported as saying “In a few decades time, computers will be interwoven into almost every industrial product,” [6]. This prediction has indeed come true, as computers or computing devices form the backbone of nearly every modern convenience, product, or service. The pace of innovation in computing is such that computers and computing devices have moved from the realm of enterprise business and government research to mainstream use by home users, small businesses, and classes in only 73 years. The ENIAC computer came into service in 1946 [2], after the end of World War Two; though and ever decreasing number, there are still Veterans alive who fought in the battles of World War Two, and civilians who lived through those times. The entire existence of modern computing, from vacuum tubes to Quantum Computing is measured in less than a human lifetime. This rapid pace of development and deployment creates a unique set of problems in which the products sold to consumers are released before society and the legal system has time to catch up. While government regulation has largely kept pace with industrial standards since at least the turn of the 20th Century, regulators generally posses a great deal of uncertainty about the newest innovations in computing, creating a loop of inaction which stifles further creativity and adoption [5].

Of interest is the Internet of Things (IoT) and so called “smart homes” in which numerous Internet connected devices, many of them mundane household appliances, occupy space in the home’s network connected infrastructure, exchange

data, and communicate both within the local network and over areas of geographical distance via web and mobile applications. Many of these devices are “always on”, or constantly providing updates and communicating with various end points, whether a server or the homeowner’s phone. As stated by the National Institutes of Health through the National Center for Biotechnology Information: “Application of the IoT model to smart homes, by connecting objects to the Internet, poses new security and privacy challenges in terms of the confidentiality, authenticity, and integrity of the data sensed, collected, and exchanged by the IoT objects. These challenges make smart homes extremely vulnerable to different types of security attacks, resulting in IoT-based smart homes being insecure. Therefore, it is necessary to identify the possible security risks to develop a complete picture of the security status of smart homes,”[1].

This research paper will focus on one commercially available IoT household appliance with no previously reported vulnerabilities, the Instant Pot Smart WiFi 6

Quart Multi-use Electric Pressure Cooker, [3],[4]. Any vulnerabilities found will be accessed, disclosed to the vendor, and reported within the research paper as

appropriate. Additionally, measures to mitigate any found vulnerabilities will be discussed, with a focus on home users and consumers of varying degrees of networking, computing, electronic, or technical knowledge. The result will be a concise discussion of IoT vulnerabilities as they relate to consumers, and how these vulnerabilities may be countered, which will include a specific example.

**References**

[1] Ali, Bako, and Ali Ismail Awad. “Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes.” US National Laboratory of Medicine and National Institutes of Health, MDPI, 8 Mar. 2018, www.ncbi.nlm.nih.gov/pubmed/29518023.

[2] History of Computers, The University of Rhode Island Department of Computer Science and Statistics, homepage.cs.uri.edu/faculty/wolfe/book/Readings/Reading03.htm.

[3] “Instant Pot Smart WiFi 6 Quart Multi-Use Electric Pressure, Slow, Rice Cooker, Yogurt, Cake Maker, Sauté, Steamer and Warmer, Silver.” Amazon, Amazon, www.amazon.com/Instant-Pot-Smart-Electric-Pressure/dp/B0777XQ4S8?ref\_=bl\_dp\_s\_web\_3031632011.

[4] “Instant Pot Smart Wifi.” Instant Pot, instantpot.com/portfolio-item/instant-pot-smart-wifi/.

[5] Mariani, Joe. “Guiding the IoT to Safety.” Deloitte Insights, www2.deloitte.com/insights/us/en/focus/internet-of-things/regulating-iot-technology-role-of-government.html.

[6] Ruß-Mohl, Stephan. Die Informierte Gesellschaft Und Ihre Feinde Warum Die Digitalisierung Unsere Demokratie gefährdet. Herbert Von Halem Verlag, 2017.

[7] “Smart WiFi 60 Pairing.” Instant Pot, instantpot.com/smart-wifi-60-pairing/#tab-id-2.