Elita Danilyuk
Zachary Lowe
Tyson O'Leary

D1: Detailed Abstract
Internet of Things: Security

The security of the Internet of things (IoT) is a relevant issue in our society because of the sheer number of IoT devices in the market and in use right now. As the number of devices is growing, the number of vulnerabilities and privacy issues are growing exponentially. We need to keep up with the increasing need for IoT security by continuing the research. As a group, the systems security course at CSU (Colorado State University) is a big part of our interest in this topic. The class opened our eyes to the importance of security and privacy considerations in technology, as well as the constant need for improvements. The Internet of things is such a huge topic in computer science right now, so we feel it is important to understand the current discussion. Mixing IoT with security makes the topic all the more enticing.

This topic is important now and will continue to be important in the future because software security and privacy should always be considered, especially with the vast growth of the IoT. Privacy concerns with the IoT most often stem from the use of RFID (Radio-Frequency Identification) chips in devices (Weber, 2010). These chips use radio frequency to uniquely identify a device, which can then uniquely identify a person. Security concerns vary, but many are similar to known security issues in DNS (Domain Name System) (Weber, 2010) and the method of routing used by IoT (Airehrour et al, 2016). Many concerns also have to do with the way information is transferred between the IoT classification layers (Alaba et al, 2017). None of these concerns have perfect solutions, so the issue of IoT security is not temporary, it will be everchanging, as computer science is itself. To understand how the IoT has changed, it is important to understand where the term and history came from.

The IoT is the general term for how the internet has, and is, connecting various "things," both object-to-object and person-to-object communications. The initial popularization of IoT began in the late 1990s and early 2000s. It was popularized by the idea of connecting home appliances to the internet. The term was first popularized by Kevin Aston who was the executive director of the Auto-ID center at Procter and Gamble (P&G) in 1999 (Corcoran, 2016). Aston made the term the title of a presentation that linked the idea of RFIDs within P&G's supply chain. In the same year, Neil Gershenfield spoke about the principles of the IoT in his book *When Things Start to Think* (Madakam et al, 2015). The following year, 2000, LG announced the plans for the first Internet refrigerator. For the next few years, several more devices with RFID chips began development. The development of these devices quickly expanded to everyday consumers.

The consumer use of the IoT has grown to such a large scale that most people interact with it daily. It has spread from smart refrigerators, thermostats, phones, vehicles, sensors, and a vast amount of other consumer goods and products (Chapin et al, 2015). The IoT has transformed how people live and communicate with various devices. It has unified almost all devices within our grasp, which has led to a great deal of personal control as well as an abundant amount of individual and group data. As the IoT continues to grow at such a large scale, a concern for security and surveillance has erupted. New legal and development policies and challenges continue to appear. As these challenges emerge, it is clear that the IoT has become a complex and intertwined web of network connections. With how closely these "things" are communicating with one another, it is important to understand the risks and rewards of how the data is being shared, whether it is public or private, and how secure it truly is.

Considering the fact that an increasing amount of our daily life involves the internet in some fashion, security becomes a much more important concern for the average person. Whether we are connected through traditional devices such as computers and phones, or through our internet-enabled appliances and other IoT devices, security is a vital aspect of the tech we use. Any breach of security runs the risk of exposing more personal information than ever before, and as we become more and more attached to these devices, we also become more and more vulnerable. In its current form, IoT devices communicate through various existing protocols. NFC, RFID, Bluetooth, and Wi-Fi for example are all commonly used for IoT interconnectivity (Sain et al., 2017). Although the adoption of smart home technology and other IoT appliances is growing, (with nearly twice as many IoT devices as people on earth) there are still major improvements that can be made to their security (Sivaraman et al., 2018). Each of these comes with its own security standards, and currently, there is no common communication standard that can be shared between all IoT devices regardless of their communication medium. This presents one of the most immediate issues facing security within the IoT. The current state of the art for Internet of Things security is that while these systems have preexisting security standards on an individual basis, there is not yet a standard that unites them all. The creation and adoption of such a standard would allow IoT to progress in new and exciting ways, furthering its usefulness to our relationship with technology.

Citations

D. Airehrour, J. Gutierrez, and S. K. Ray, “Secure Routing for internet of things: A survey,” *Journal of Network and Computer Applications*, vol. 66, pp. 198–213, May 2016.

F. A. Alaba, M. Othman, I. A. Hashem, and F. Alotaibi, “Internet of things security: A survey,” *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, Jun. 2017.

L. Chapin, S. Eldrige, K. Rose, The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World. Geneva, Switzerland: Internet Society, 2015. https://d1wqtxts1xzle7.cloudfront.net/48790442/ISOC-IoT-Overview-20151014_0-with-cover-page-v2.pdf?Expires=1654050599&Signature=Y7S9d2~9qCP9jfubuEoga4BkRaG-e-~T2sbAmThorzdGdfQr7wDPzN~df0KRAsUYBxvvB1XZkedYTxbiNm2oYDsO1pD4mh2DV1RVlCeMhAO4vJkycIhcUp6r~Q9kfxsEWfDbwvazawKAweAo1VJ-QeyYkYnq0n~EUvWm8RmEzG6aK1OZr1eaZ7BNEKZVJS44LGPm5QJnjSYxFzrw3arUFDMi8gotMV6Ua29QlZl-ljMvdqNUPaz-jW40RdB6500CwPg-UqMsi~VVomOFU2o7inHvF2Euk-Q9AWQuvopom~c~3xz0HgRoInFkX7eeKNxewTe~tZtjtuE1WuR4qBGpHQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

P. Corcoran, The Internet of Things: Why now, and what's next? *IEEE Consumer Electronics Magazine*, vol. 5, no. 1, pp. 63-68, 2016. https://ieeexplore.ieee.org/abstract/document/7353271?casa_token=zzA9xE_hYRwAAAAA:PD5AXGPkQeQahR35eFiWJrOqHeWbrFsm_WalZzDuwx_RAwZugAlsgXD1hMEDR73nI92nCVT7anM

R. H. Weber, “Internet of things – new security and privacy challenges,” *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, Jan. 2010.

S. Madakam, R. Ramaswamy, S. Tripathi, Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, 2015. https://www.scirp.org/html/56616_56616.htm?pagespeed=noscript

Sain, M., Kang, Y. J., & Lee, H. J. (2017). Survey on security in internet of things: State of the art and Challenges. *2017 19th International Conference on Advanced Communication Technology (ICACT)*. https://doi.org/10.23919/icact.2017.7890183

Sivaraman, V., Gharakheili, H. H., Fernandes, C., Clark, N., & Karliychuk, T. (2018). Smart IOT devices in the home: Security and privacy implications. *IEEE Technology and Society Magazine*, *37*(2), 71–79. https://doi.org/10.1109/mts.2018.2826079

Zalewski, J. (2019). Iot safety: State of the art. *IT Professional*, *21*(1), 16–20. https://doi.org/10.1109/mitp.2018.2883858