Internet of Things and the Information Technology Industry

Jeremy Ogle

Arkansas Tech University

March 11, 2018

The Internet of Things (IoT) is making a name for itself as more and more common products and household items are WiFi or Bluetooth enabled, allowing them to gather user input, or monitor a surrounding environment, and then provide real time feedback over a network to a centralized or de-centralized location for processing. Working in the Information Technology (IT) industry, one must be cognizant of these devices and understand how they work to ensure the privacy and safety of the consumers that they serve. Failure to adhere to the rules, regulations and laws that surround data collection can lead to steep penalties and fines for a company. A true IT professional is one that is always learning and ready to adapt to the changing environment, and the IoT is no exception to this rule.

Literature Review

How big is the IoT, and why does it matter? Due to growth of the IoT devices, the wirelessly connected footprint of devices on the Internet is estimated to be 26 billion units by the year 2020 (Koskela, Majanen, & Valta, 2016). Maras (2015) notes that the rush to bring IoT enabled devices to the market has created security vulnerabilities, such as hard-coded passwords and backdoors, due to a lack of standards for practices in this realm. With approximately half the world's population connected to the Internet, according to Constantinescu (2015), the need to create standards for the IoT sector in the areas of privacy, usage, and energy consumption will only increase with time as more and more people come online.

Compare the projected number of 26 billion Internet enabled units in 2020 to only 0.9 billion actual units in 2009 and we can see that the pace of growth is staggering, which leads to increasing concerns for how IoT devices send and receive data, and how that information is kept secure and private (Koskela et al., 2016). Recognizing this increase, Koskela et al. (2016) have sought to combat the energy usage associated with so many devices being connected, especially as it relates to wireless network usage and power consumption. The proposal is based on reducing the size of the network packet headers through compression to enable less energy consumption and use less traffic on the network to send and receive data. Results from their latest research were mixed as they did find energy saving on a slower wireless band, but on higher frequencies (LTE and WLAN) the savings in transmission time power consumption were equal to the energy needed to run the compression process, resulting in no gain of efficiency. Although these results didn't produce the outcome they had hoped, they did not that there is less loss of packets as a result, giving this an overall positive outcome. Further research and efforts could yield a solution that reduces the needed energy to compress the packet header and still allow for the decrease in packet loss.

Severe legal implications are at stake when proper practices and measures are not put in place to ensure that IoT devices meet already established security protocols. Maras (2015) gives the example of TRENDnet's home security and baby monitoring devices that were Internet enabled allowing the users to view the feeds remotely. A backdoor exploit was exposed by a hacker allowing them to provide a live feed over the Internet of over 700 consumers in use of the TRENDnet product. Life and death situations are also now at risk as devices in the medical field become Internet enabled to allow for remote setting and use. In light of this information, Maras (2015) urges that proper analysis in conducted in the area of IoT securities, and that proper legal representation and action are taken to prevent the security and privacy issues that will arise if no action is taken.

As we move into this area of IoT devices, Constantinescu (2015) warns of the issues that will be faced as we move from a communication model that is based on human to artificial intelligence to a model that is based on artificial intelligence to artificial intelligence. She warns that the lack of preparation for this change through proper legislation could lead to issues in the middle class due to loss of job markets. The proposed theory is that IoT devices will become capable of communicating with each other regarding the needs of consumers based on big data that has been gathered, leading to decreases in IoT device costs, and also decreases in price to purchase these products. It is because of this theory that the need to continue to work by Koskela et al. (2016) becomes important as it relates to the sustainability to adding more IoT devices to our environment.

Conclusion

IoT devices have begun to flood our everyday lives, and will continue to do so as more and more companies look to add functionality that gives a personalized experience and ease of use for promoting repeated use of the product. It is because of this push for new devices to be created and implemented in the market that IT professionals must truly understand the local and global rules, regulations and laws that apply to the consumer’s security and privacy. Failure to follow laws that are already in effect can lead to hefty government fines, such as the case with the TRENDnet camera exposure.

IT professionals must also be prepared to participate in active dialog about the future of the products they will help develop, and speak to the practices they will use to provide proper security of a device, and protect the privacy of the consumer. They can participate by working with local and federal government agencies, conducting research that leads to more secure practices, and by looking for ways to reduce the consumption of power and bandwidth that is used by the increasing number of devices that are Internet enabled.

References

Constantinescu, E. M. (2015). THE INTERNET OF THINGS. BETWEEN EFFICIENCY AND PRIVACY. *Knowledge Horizons.Economics, 7*(4), 69-71. Retrieved from https://libcatalog.atu.edu:443/login?url=https://libcatalog.atu.edu:2409/docview/1777746319?accountid=8364

Koskela, P., Majanen, M., & Valta, M. (2016). Packet header compression for the internet of things. *Sensors & Transducers, 196*(1), 43-51. Retrieved from https://libcatalog.atu.edu:443/login?url=https://libcatalog.atu.edu:2409/docview/1770514345?accountid=8364

Marie-Helen Maras. (2015). Internet of things: Security and privacy implications.*International Data Privacy Law, 5*(2), 99-104. http://libcatalog.atu.edu:2097/10.1093/idpl/ipv004 Retrieved from https://libcatalog.atu.edu:443/login?url=https://libcatalog.atu.edu:2409/docview/1704856770?accountid=8364