Byte Back: Guidelines for Improving Security in Connected Devices using Actor Network Theory

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Malcolm Miller

Spring 2020

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

"[T]here will be a time when we must choose between what is easy and what is right."

-J.K. Rowling, Harry Potter and the Goblet of Fire

Introduction

Due to the advancements of technologies such as nanoelectronics and cloud computing, many devices can be connected to the internet to bring added utility and convenience (Vermesan & Friess, 2013). As of 2011, there were over 15 billion connected devices worldwide, with forecasts for more than 30 billion by 2020. This network of connected devices, or the internet of things (IOT), is present in a wide range of industries including healthcare, energy, manufacturing, and transportation (Hassan, Khan & Madani, 2018). Although connected devices benefit society in numerous ways, in many cases, the advancement of IOT has outpaced privacy and security protections. This has led to vulnerabilities, many of which have the potential to reduce reliability, intrude on privacy, or cause physical harm to human beings.

According to the researchers at the CSIRO ICT Center in Australia, 14 cyber-attacks are launched every second (Jan-Jaccard & Nepal, 2014). These authors go on to explain the increase in cyber-attacks over the past decade (p.973).

> [Cyber] attacks are cheaper, convenient and less risky than physical attacks. Cyber criminals only require a few expenses beyond a computer and an Internet connection. They are unconstrained by geography and distance. They are difficult to identify and prosecute due to [the] anonymous nature of the internet.

Thus, by connecting previously offline devices to the web, the IOT has made the tools of our society more susceptible to attack. As estimated by Cybersecurity Ventures, cyber-crime cost the world $3 trillion in 2015 and is projected to increase to $6 trillion by 2021 (Morgan, 2017). Therefore, increases in connectivity should be accompanied by increases in security.

This paper discusses guidelines for the design and implementation of connected devices. These guidelines are derived from both my technical work and a collection of research papers addressing the cybersecurity and privacy issues of the internet of things. In this paper, I argue that while connected devices often bring great improvements to the safety and productivity of society, they ought to be designed and tested with higher scrutiny in order to minimize or negate security and privacy shortcomings. This research will apply the actor network theory (ANT) framework to clearly portray the tradeoffs of connecting devices to the internet. Additionally, I will demonstrate the utility of ANT by applying it to a self-powered location tracking device that was designed for my capstone project.

Instead of taking shortcuts and creating vulnerabilities, IOT developers can apply the guidelines outlined in this paper to create products that are safe and reliable.

Part I: Connected Devices Present Security and Privacy Concerns

Technological advancements have enabled connected devices to be deployed in a wide variety of situations. One such advancement is low power electronics. As electronics fabrication has improved, circuits have decreased significantly in size (shown in Figure 1) and power draw. Makimoto and Sakai discuss in their paper, “Evolutions of Low Power Electronics and its Future Applications” (2003), how these improvements have led to more nomadic devices. Since IOT devices often take readings and relay information from environments that are not directly connected to the power grid, advancements in nomadic devices have improved the versatility of connected devices. Another key research contribution to the development of nomadic devices is the improvement of battery technologies. As discussed by Ajith Amerasekera (2010), batteries are projected to double in capacity every decade, which enables wireless communication devices (such as IOT sensors connected to the internet) to remain operational for extended periods of time. Alongside improvements in energy storage technology, there have been great advancements in energy generation. As a result of improvements in the efficiency of solar panels developed in research laboratories (NREL), commercially available panels have greatly increased in efficiency and decreased in price. Makimoto and Sakai define a figure of merit for nomadic devices as being equal to $\frac{Intelligence}{Size \times Cost \times Power}$ (2003) thus, these three innovations have significantly contributed to the utility of connected devices. If the generation (from solar panels for example) and storage of energy is large enough that the device does not require additional energy input, it can operate independent of a central power grid. These self-powered devices are useful in that they can be deployed in a wide variety of locations and they last for a considerably long amount of time.

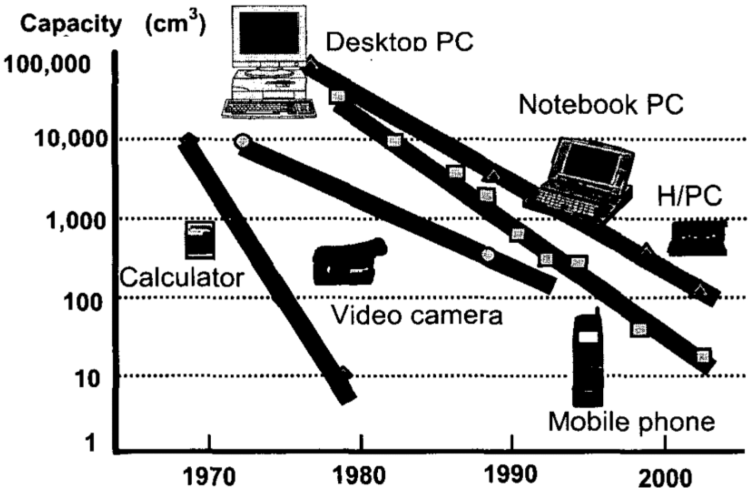

Figure 1: Increased Spatial Efficiency of Computers

As manufacturing technologies have improved, computers have become both smaller and more powerful.

(Makimoto & Sakai, 2003, p.2)

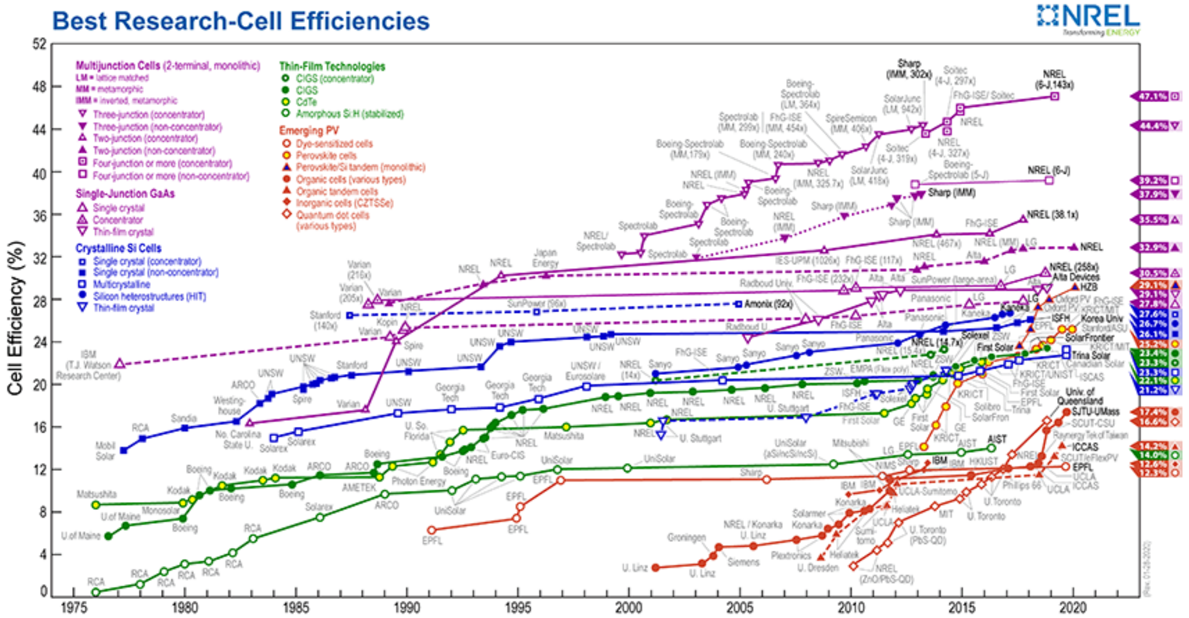

Figure 2: Efficiencies of Research Solar Cells

The improvements of photovoltaics research have increased the cost-effectiveness of commercial solar.

(NREL)

Due to these improvements in energy storage, energy generation, and low power electronics, many connected devices have been deployed worldwide. As stated in the introduction, connected devices have benefited a wide range of industries with an estimated 30 billion connected devices being present worldwide in 2020 (Vermesan & Friess, 2013, p.14).

One example of such benefit is the collection and communication of location information. With the global positioning system (GPS) being widely available to both individuals and companies, it is now possible to obtain fairly accurate location information from a particular device in real-time. This collection of data can improve and enable a wide range of IOT applications. In agriculture, location data can be used to associate attributes of a farm such as humidity, irrigation, and soil temperature, with precise locations (Maia et al., 2014). By analyzing such data, farmers can better understand their fields and therefore make more informed decisions about crop rotation, irrigation and pesticide use. This can significantly reduce costs, increase overall production, and decrease the amount of water and pesticides used every season. In public transportation, GPS devices have been attached to school busses allowing commuters to track their locations in real time (Chung, 2019). This capability helps students to better plan their commutes and provides parents peace of mind with regard to their child's location.

Despite these added benefits, IOT devices can have clear drawbacks. For example, in order to meet the rigid power budgets of self-powered and low-power applications, security tradeoffs are often made (Jan-Jaccard & Nepal, 2014). Additionally, by connecting devices that were previously offline to the internet, they are made much more susceptible to hacking. Electronics that are isolated from any network require someone to physically alter them to modify their operation. On the other hand, internet-connected devices have the potential to be maliciously controlled by anyone with an internet connection. One example of this is the 2015 Jeep hack (Greenberg, 2015), where two engineers were able to remotely control a model of Jeep by sending signals over a wireless network. Although only the multimedia system of the car was connected to the internet, it was able to send signals to the control system of the car. Thus, the hackers could remotely shut off the car, putting its passengers in physical danger.

Another downside of connecting devices to the internet is privacy. For instance, many GPS tracking devices similar to the one discussed expose the location of individuals. While the visibility of someone's location in real time can put them in direct danger, the logging of one's location history is also something that ought to be avoided. Any location data connected to a person—even if it is intended to be used solely for their work—can be used to link an individual to a church, school, home, or protest (O'Keefe, 2018). As discussed by Michael and Clarke

(2013), the ability to extract personal information from individuals using location means that such data collection is deeply intrusive into privacy.

Although advancements in technology have enabled many industries and individuals to benefit from IOT, there are key drawbacks to connected devices which need to be addressed. A heightened consideration for these issues during the design and testing of connected devices could potentially reduce the threat of cyber-attacks and improve privacy.

Part II: Actor Network Theory Clarifies the Vulnerabilities of Connected Devices

It is likely that there is a lack of consideration towards privacy and cyber-security in the Internet of Things because designers have only focused on the technical sides of their devices. Downey addresses these concerns in “Are Engineers Losing Control of Technology?” (2005) by proposing a new form of engineering education: problem definition and solution (PDS). In the PDS model, engineers seek to “abandon the mental model that puts technical problems at the core of engineering education” by framing the problem with the interests and roles of all stakeholders in mind. To accomplish this, Downey recommends that all parties affected by the project ought to be interviewed. In the case of connected devices, this could include those who use the device, those who interact with users, the designers of the device, and government officials who regulate the device. This interview process helps the engineering team to both identify the various roles of stakeholders and to understand how they view the problems at hand.

It is hard to satisfy all parties and meet all of a project’s requirements by focusing on either the human or technical components alone. As Venturini states in “Diving in Magma” (2009), “To understand how social phenomena are built, it is not enough to observe the actors alone nor is it enough to observe social networks once they are stabilized. What should be observed are the actor-networks." (p.264). Thus, I believe that engineers ought to employ actor network theory (ANT) while designing and deploying connected devices. By analyzing both human and non-human actants within a system, this framework can reveal much more to an engineer than the analysis of one component alone. To examine the roles of security and privacy within the internet of things, I will consider the cultural, technical, and organizational effects of connected devices.

Culturally, it is important to begin by identifying what goals ought to be prioritized in a project. As discussed earlier, most connected devices are designed to replace or augment previously deployed offline devices. Therefore, a worthwhile goal should be to output a device that is sufficiently superior to the pre-existent solution. To accomplish this, the new device must outperform the old by at least one metric such as speed, cost, ease of use, size, longevity or energy efficiency. After a goal is defined, one must reflect and decide if its impacts will be good or bad for society. Often, they are both. As discussed above, advanced functionality and improved performance are clear benefit to IOT while privacy and security vulnerabilities are drawbacks. Shifts to accommodate such security and privacy concerns have benefits and drawbacks as well. For instance, although security improvements can protect the data of individuals, the required development process increases costs for companies and can delay the release of a product. Another important matter is to analyze what is seen as culturally inappropriate. For instance, why might society reject the 2015 Jeep after the hack was exposed and not reject mobile applications which collect data that infringes upon an individual's privacy?

To answer questions like this, it is useful to examine the organizational aspects of connected devices. Namely, which stakeholders make the decisions that lead to a device's acceptance or rejection. Companies play a large role in deciding what is released to society, but they are strongly influenced by consumers and governments. Sometimes, when a certain group doesn't sufficiently exert its influence, a technology can fall short of its goal. For instance, in the case of Boeing's 737 Max failures, the Federal Aviation Agency failed to voice concerns about the angle-of-attack sensor and its accompanying software (Matthews & Choi, 2019). This ultimately resulted in two crashes. Downey argues that by training students to "work with people who define problems differently than one another." (2005, p.590), engineers that enter the government private sector will lead through technical mediation and be prepared to avoid such errors caused by miscommunication.

In terms of technology of connected devices, there are many things to consider. First of all, engineers need to decide what goes into a particular product. In most cases, IOT devices have at least one sensor to acquire data such as a GPS unit, a camera or a microphone. Additionally, each device needs, a computer to process the data, a transmitter/receiver to communicate over the internet, a power supply, and software to guide its operation. Actor network theory allows for the technical performance of these components to be compared and analyzed alongside their surrounding society. A useful way to do this is through anthropomorphism. As Latour discusses in "Where are the Missing Masses" (1992), "every time you want to know what a non-human does, simply imagine what other humans or non-humans would have to do were this character not present." (p. 155). With this technique, instead of viewing an IOT device as a collection of sensors that mindlessly takes readings and transmits information it can be viewed as a member of society that dutifully observes the world and reports its findings to higher management. The effects of privacy invasion and cyber security are viewed more clearly through this lens. Cyber-criminals are no longer just modifying bits in a server far away, they are intruding into people's personal lives and changing the way they live. A phished bank account is a wallet stolen out of a someone’s pocket, access to GPS data is a cloaked figure following you around, and a hacked Jeep is a criminal entering your car. Defenses against such attacks can be treated in the same way. Amanda O’Keefe, a privacy, technology, and intellectual property lawyer, discusses how companies can practice “data minimization” by only collecting pertinent location data and avoiding collateral data that could compromise the privacy of their users (2018). For example, if a shipping company wanted to track the location of their packages, they could minimize their data collection by only recording the position of their employees during the hours of their shift. I believe that a useful alternative to this approach is data decoupling, in which the data that is being collected is not directly associated with a particular individual. The next section will highlight an example of how data decoupling can be implemented.

Part III: Engineering with an Actor Network Mindset Results in Secure Devices

Engineers ought to perform a similar actor network analysis while inventing, designing and testing connected devices. The first and possibly most important step in this process is problem definition. As stated earlier, most connected devices are replacing previously-invented offline solutions to the given problem. Thus, the main goal of engineers is to maximize improvements and minimize drawbacks with respect to the initial solution. In most applications, the requirement should be to have zero drawbacks that effect safety, reliability, or privacy. This is because in many cases, connected devices have an impact on the safety of human beings. Although the 2015 model of Jeep had internet connectivity features, the added benefit was greatly overshadowed by the significant threat it opened up. Oftentimes, the benefits of such devices are much more obvious to the users than the drawbacks. One main reason for this is that companies benefit by marketing their new functionalities. Additionally, many of the drawbacks may not be obvious and might even be unknown by the developers of the system. I believe this is due to an imbalance in priorities when defining the problem addressed by a particular connected device. Developers focus on the improvements from one product to another instead of analyzing how solving one problem could create many more. One way to view these transitions more clearly is to, as Downey discusses, create a workspace with people who define problems differently. A team that diversifies its outlook will have greater foresight into potential problems.

My capstone team sought to minimize vulnerabilities while developing our IOT project. Our device was a GPS tracking device used to transmit live location data from a moving vehicle. As we defined our problem, we considered similar devices that already attempt to solve the problem of broadcasting a location in real time. Current GPS trackers are either powered by a battery or through a connection to the electrical system of a vehicle (El Khoury, 2018, p.7). Batteries require recharging periodically, which can make systems less dependable and more expensive to maintain. Connections to external power systems are reliable, but they restrict the compatibility of trackers to specific vehicles. Additionally, as seen with the Jeep, installing an internet-connected device to a vehicle can often introduce unintended cyber vulnerabilities.

Shortcomings in tracking devices can mean reduced safety and dependability for public transportation systems (Chung, 2019). Powering such devices with batteries also has significant drawbacks. Without the ability to be recharged on site, batteries are inconsistent. From an actor network perspective, this means that an engineer cannot be certain when the device will stop speaking to others. On the other hand, direct connecting systems might not know how to speak (because they are not compatible with the electrical system) or worse, instead of sharing a car’s location, they could drive it off of the road (due to a cyber-attack). With the current commercially available solutions in mind, my capstone group sought to devise a technical solution that could eliminate these concerns. To ensure compatibility across all devices, we decided to make our device self-powered. Without the need to connect to a specific part of a vehicle, we could simply install our device on its exterior. This also eliminated the threat of cyber-attacks creating the possibility of physical danger. Since our device has no connection to the control system of the vehicle, a hacker has no way of controlling it remotely. The other key decision we made was to make our device self-powered. With access to high capacity batteries, low power electronics, and efficient solar panels, we were able to design our device to remain powered indefinitely by harvesting solar energy.

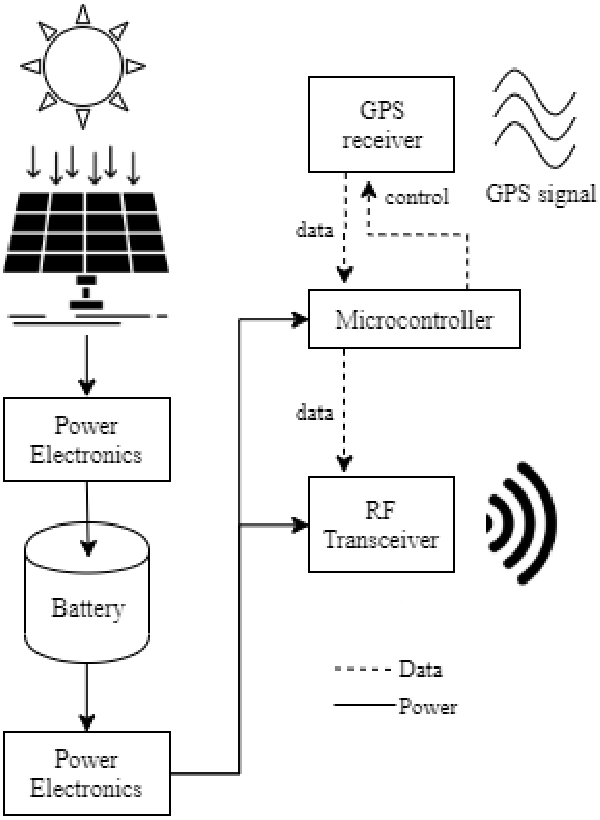

Figure 3: Block Diagram of Self-Powered GPS Tracking Device

Solar energy is collected and used to charge a battery, which powers logic and transceivers. (created by the author's capstone team)

In our actor network, the device doesn't listen to hackers that want to put people in danger. Instead, it obediently reports its location with high reliability. By treating our device as a human, we were able to frame the issues of other devices within the network. This method also allows the security benefits to be more easily understood by non-engineers. I believe that this outlook could allow companies to better market security and privacy benefits to their customers. Thus, the IOT industry could shift away from primarily prioritizing performance and features to promoting reliability and security. Perhaps, this outlook on technological developments could shift the focus of companies from releasing a new product on time to releasing the right product when it is ready. In the case of Boeing's 737 Max planes, their goal was to release an upgraded plane in time to maintain their competitiveness with Airbus (Matthews & Choi, 2019). This urgency resulted in a product being released that had significant reliability concerns. If instead, they worked towards the goal of improving fuel economy *and* ensuring reliability, they might have not felt the pressure to prematurely release a product. Thus, Boeing could have spent more time testing and verifying their designs and consequently may have detected the issues in the maneuvering characteristics augmentation system (MCAS).

In order to minimize vulnerabilities in connected devices, engineers ought to have a pessimistic view of their own work. For example, in our project, we assumed everything that was possible to be hacked in our system was a potential vulnerability. This was a key reason we decided on a self-powered design. By assuming that any wireless transceiver would be maliciously accessed, we forced ourselves to electrically isolate our device from the car's control system. If Boeing were to scrutinize their systems similarly, they would have assumed that their angle-of-attack sensor would eventually fail and consequently install human-overrides to their MCAS. Additionally, although we were confident in our design, we assumed that our initial implementations would have errors. Therefore, we constructed our system to be easily testable. During the development process, we spent just as much (or more) time testing our system as we did building it. With this approach, the issue of the Iowa Caucus mobile application would have been prevented (Schneider, 2020). Instead of yielding to self-confidence and deploying a technology without sufficiently testing it, Shadow, the mobile application development company, would have spent a considerable amount of time simulating real-world conditions in order to identify errors in the voting app before it went live.

Finally, engineers ought to consider the societal impacts of their work before releasing it to the public. Although a product satisfies technical requirements, it could have adverse organizational and cultural effects. As discussed in “Towards an Integrated View of Technology”, engineers must envision the consequences of a device before introducing it into society (Neeley, 2011). This paper discusses the idea of “thintelligence”, the action of creating novel technical inventions and releasing them into society without considering their ethical implications. If modern-day companies act “thintelligently” and incorporate GPS tracking into many human activities, perhaps it is up to society itself to regulate what data we allow to be collected. One group that has strictly controlled the introduction of new technologies into their lives is the Amish. As discussed in “Look Who’s Talking” (Rheingold, 1999), the Amish community is quite strict with what technology they bring into their lives. While many outsiders believe that the Amish are strictly against innovation, Howard Rheingold uncovered that they are simply against devices that encroach upon their way of life. Perhaps this techno-selectivity employed by the Amish could aid engineers in determining the ethical viability of connected devices *before* deploying them in society. Instead of acting like Boeing by viewing failure as the inability to deliver an upgraded device to market on time, techno-selective engineers would view failure as releasing a device that would do more harm than good.

After considering these case studies, a set of guidelines for improving security in connected devices. First of all, designers should compare the desired device to its offline predecessor. This will serve as the baseline for all changes in functionality and security. Thus, if the finished product is worse in any way than its offline variant, the engineering team should strongly consider redesigning the system or defaulting back to its known and reliable version. Second, engineers should assume every component with wireless connectivity can and will be hacked. With this in mind, ANT can be applied to consider what a human would do in place of the device. By framing the devices operations in this way, the causes and implications of cyber-attacks are more tangible. Finally, throughout the entire engineering process, a diverse group of stakeholders ought to be consulted in order to make sure the finished product is acceptable in its cultural, technical, and organizational aspects.

Conclusion

Connecting devices to the internet can introduce new functionalities and great improvements to the machines used in our societies. However, in many cases, security protections have lagged behind the technological advancement of IOT. Throughout this paper, I explore how cutting corners in engineering practice has resulted in massive failures such as Boeing’s MCAS and Shadow’s voting app. Through synthesizing the concepts of actor network theory (Latour, 1992) and Downey’s problem definition and solution model (2005), I have developed a set of guidelines to protect against such vulnerabilities.

Although these guidelines will help engineers to prevent security flaws in their devices, they don’t offer specific directions for how to implement any particular solution. What these guidelines lack in specificity, they make up in versatility. In order to solve real-world engineering problems, engineers cannot simply follow predetermined directions. Rather, they must base their decisions off of their device’s impact on the human and non-human actants within a network. Actor network theory is necessary to fully understand how a connected device interacts with society. Therefore, ANT is needed to identify and correct all security concerns. As Downey discussed in his lecture on engineering education (2005), “[T]he process of generating technical solutions includes the non-technical work of assessing the implications of alternative solutions for stakeholders.” (p. 591). Instead of replacing the pre-existent technical processes involved in creating connected devices, these guidelines serve as a supplement. Although it may be easier to construct connected devices without regard for their security, IOT firms that choose to implement these guidelines will deliver safer, more reliable products.

References

Amerasekera, A. (2010). Ultra low power electronics in the next decade. *Proceedings of the 16th ACM/IEEE International Symposium on Low Power Electronics and Design - ISLPED 10*. doi: 10.1145/1840845.1840892

Chung, J. (2019, August 23). Parents will be able to track NYC school buses with an app. *New York Public Radio*

Downey, G. (2005). Are engineers losing control of technology? From 'problem solving' to 'problem definition and solution' in engineering education. *Chemical Engineering Research and Design, 83*(Ag): 583-595

El Khoury, F. (2018). Building a dedicated GSM GPS module tracking system for fleet management: Hardware and software. Boca Raton: CRC Press. doi: 10.1201/9781351201391

Fliev Maia, R., Netto, I., & Lan Ho Tran, A. (2017, December 25). Precision agriculture using remote monitoring systems in Brazil.

Greenberg, A. (2015, July 21). Hackers remotely kill a Jeep on the highway-with me in it. *Wired*

Hassan, Q. F., kan, A. ur R., & Madani, S. A. (2018). *Internet of Things Challenges, Advances, and Applications*. Boca Raton, FL: CRC Press.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. doi: 10.1016/j.jcss.2014.02.005

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. In Bijker, W. E. and Law, J., eds. *Shaping technology/Building society: Studies in sociotechnical change.* Cambridge, MA: MIT Press, pp. 225-258.

Makimoto, T., & Sakai, Y. (n.d.). Evolution of low power electronics and its future applications. *Proceedings of the 2003 International Symposium on Low Power Electronics and Design, 2003. ISLPED 03.* doi: 10.1109/lpe.2003.1231823

Matthews, M. Q., & Choi, C. Q. (2019, December). Compass course. *PRISM*, 24–29. *American Society for Engineering Education*

Michael, K., & Clarke, R. (2013). Location and tracking of mobile devices: Überveillance Stalks the Streets. *Computer Law and Security Review: The International Journal of Technology and Practice*, 29(3), 216 - 228.

Morgan, S. (2019, September 18). Global cybercrime damages predicted to reach $6 trillion annually by 2021. *Cybersecurity Ventures*

Neeley, K. A. (2011). Toward an integrated view of technology. In *Technology and Democracy: A Sociotechnical Systems Approach* (pp. 37–45). San Diego, CA: Cognella.

NREL. (n.d.). Best Research-Cell Efficiency Chart. Retrieved from https://www.nrel.gov/pv/cell-efficiency.html. *National Renewable Energy Research Laboratory*

O'Keefe, A. (2018, February 6). Balancing the benefits of location data with privacy protection. *International Association of Privacy Professionals*

Reingold, H. (1999). Look who's talking. *Wired*, *7*(01), n.p. Retrieved from https://www.wired.com/1999/01/amish/

Schneider, A. (2020, February 4). What we know about the app that delayed Iowa's caucus results. *National Public Radio*

Venturini, T. (2010). Diving in magma: How to explore controversies with actor-network theory. *Public Understanding of Science, 19*(3), 258-273.

Vermesan, O., & Friess, P. (2013). *Internet of things: converging technologies for smart environments and integrated ecosystems*. Aalborg, Denmark: River Publishers.