C1C Henry, C1C Hermanson, C1C Pak, C1C Singh

WPT Ethical Considerations

This capstone project attempts to expand upon the vulnerabilities that exist within the emerging technology of wireless power transfer (WPT). First, known vulnerabilities will be observed by recreating a WPT hijacking and eavesdropping experiment conducted by graduate students at the University of Tennessee. Afterwards, the threat of these vulnerabilities will be assessed and strategies for improving attacks on the vulnerabilities will be created. Finally, potential mitigations for these threats will be explored and implemented into the experiment. The goal for track one of this ongoing capstone project is to share how data transmitted through wireless non-networked point-to-point communication can be protected with the government. This will directly benefit the National Reconnaissance Office (NRO) and future capstone groups at the United States Air Force Academy (USAFA) as they work to implement these defensive strategies on a much larger scale (Bluetooth, Radio Frequency Identification, Light Fidelity, Lasers, etc.).

As previously mentioned, the main stakeholder for this project is the NRO. The NRO is a member of the United States Intelligence Community and an agency of the Department of Defense. This agency operates reconnaissance satellites and provides critical intelligence to the military and civilian organizations within the government. As such, they rely heavily on various forms of wireless, non-networked, point-to-point communication to perform their job. This technology is rapidly expanding and becoming much more capable, and as a result, there are vulnerabilities associated with it. Wireless charging is perhaps the most basic form of this technology, and this capstone will serve as a baseline as for other wireless technologies, such as Bluetooth, RFID, and lasers, by future capstone groups and researchers. At the termination of this ongoing capstone project, the NRO will be provided with the risks associated with using technology and defensive strategies for protecting the sensitive information they are transmitted through it.

One area for ethical consideration regarding wireless power transfer is its ability to cause harm. According to section 1.2 of the ACM Code of Ethics, computing professionals must attempt to avoid harm by avoiding negative consequences of their products (ACM Code of Ethics and Professional Conduct). Attackers can cause harm on various scales by means of WPT. On a smaller scale, these attacks cause property damage. In the University of Tennessee experiment, the researchers were able to cause damage to both the phone and the wireless charger by means of overcharging. This can potentially cause more catastrophic effects on larger technologies using WPT such as electric cars and satellites. On the other hand of hijacking attacks, malicious users can stop the power transfer process completely. This can be life-threatening with devices such as pacemakers (Researchers Explore Wireless Charging of Pacemakers, Internal Medical Devices via Wearable Metasurface) that people rely on to constantly work.

Further, with this research we must consider section 1.1 of the ACM Code of Ethics which states that a computing professional should “contribute to society and to human well-being, acknowledging that all people are stakeholders in computing”. Our research, while demonstrating vulnerabilities that could have possibly life-threatening implications, still serves to benefit society as we seek to expose and fix these weaknesses so such vulnerabilities cannot be exploited by those actively seeking to do harm or otherwise cause disruption. Not everyone today uses or is directly involved with wireless charging but the Qi standard is merely in its infancy and is being adopted and marketed in more and more products. Further, beyond simply charging a device this research serves as an initial step into side-channel attacks within other non-networked point-to-point communications systems which have impacts into various facets of people's everyday life, such as the ability for a satellite to securely communicate – both uplink and download – with a ground station.

When looking at the ethical implications of the more technical features of WPT vulnerability research the issue of privacy arises. Section 1.3 of the ACM code of ethics stipulates one must strive to be “honest and trustworthy” while section 1.6 explicitly states one must work to “respect privacy.” The attack vectors associated with WPT include the interception of Qi protocol packets which contain information about both the power transmitter and victim receiver. Much of the data does not present any significant privacy concerns. One area of concern, however, exists in the possibility of unique device identification via fingerprinting. This is a concern as it allows a way to uniquely identify and potentially track a device between WPT charging stations. Individuals are often very cautious of “tracking.” As such, our research includes ways to protect against malicious applications of such features and how one can detect their use. This research remains consistent with the various tenants of the ACM Code of Ethics. The negative ethical applications are actively considered by the researchers in order to ensure no line is crossed and that we seek to discover malicious applications so they can be identified and mitigated.

With these ethical concerns of fingerprinting, causing damage, and denial of service, our research hopes to address the issues for the future of technology. By reverse engineering the attack vectors, we can derive defensive protocols. A product of our and future research is a more secure transfer of information between the transmitter and receiver in WPT. For example, an encryption method could be implemented to obscure the data an attacker is able to snoop off a device. Additionally, the transmitter and receivers could have their own keys which ensure they are sending and receiving messages only from each other. As a result, the ethics behind this technology will be less of a concern and the technology can confidently be used on a larger scale. The ethical concerns inherent to WPT are clearly reduced by the introduction of mitigation and protection mechanism but will remain present. As with all technology, as new defensive measures are introduced new means to exploit these systems are developed. WPT development and implementation must continue to consider ethical implications of its use and work to secure existing and future ethical concerns.

To conclude, it is our group's belief that it is the ethical obligation of the standard to include security in the communication in order to avoid the attacks outlined in our research. If this standard is implemented in its current form into devices such as pacemakers as is outlined by some companies as the future of Qi charging capabilities, it has the capability of causing great harm to the users. The ethical liability then lies in the refusal to include mitigations to these attack vectors by the companies and/or the standard itself. Therefore, it is our concern that these ethical implications be addressed and that our research may prove useful in creating a more ethical environment.

Works Cited

“ACM Code of Ethics and Professional Conducts.” *Code of Ethics*, <https://www.acm.org/code-of-ethics>.

Grainger Engineering Office of Marketing and Communications. “Researchers Explore Wireless Charging of Pacemakers, Internal Medical Devices via Wearable Metasurface.” *Holonyak Micro & Nanotechnology Lab | UIUC*, https://mntl.illinois.edu/news/45807.