**Chapter 12: When All Things Are Hackable**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

CYBS 7359 – Digital Forensics

Spring 2020

Presented to Dr. Renita Murimi

1. Describe the incident about Texas Auto Center's remote vehicle immobilization technology. How did it backfire? What do you think were the problems with how this technology was used?

The incident regarding Texas Auto Center's remote vehicle immobilization technology began when suddenly, a few of the dealership’s customers’ cars just stopped running and wouldn’t restart. The incident backfired when the dealership faced several complaints from customers throughout Texas about their vehicles being bricked, completely un-drivable, and unable to start, the situation was also accompanied by police reports about the cars’ horns going off in the middle of the night. In my opinion, the problems with how this technology was used relays on Texas Auto Center. The dealership should have maintained proper access control to the system. When the dealership employees leave the company, their credentials should have been terminated. Additionally, the dealership should have properly monitored who is trying to access the system and confirming the authentication before any data alterations could occur.

2. What is the ratio of the address space available with IPv4 versus IPv6? What analogy does the author use?

The ratio of the address space available with IPv4 versus IPv6 is 4.3 billion connections (about 232) to 340,282,366,920,938,463,463,374,607,431,768,211,456 (2128) connections. The author uses a grain of sand analogy to explain the address space difference. That is, according to the author, if there are only 1019 grains of sand on all beaches of the world, IPv6 will allow each grain of sand to have a trillion IP addresses. The address is so enough that every single atom on our planet can have a unique address, still leaving enough addresses to do 100+ earths. The author also asserts that one can think of today’s Internet as the size of a golf ball and tomorrow’s as the size of the sun due to the growing IoT technology, which takes advantage of the huge address space.

3. The chapter describes ways in which RFID cards can be hacked. Describe one such way in detail. Where have these incidents occurred?

One of the ways hackers can hack RFID is by using tools that allow them to wirelessly capture a target’s credit card number, expiration date, and security tools. Using a card-magnetizing tool, the data is then encoded on a new card, which will allow them to conduct fraudulent purchases. These incidents have occurred in gas stations and shopping centers. That is, hackers have performed the attack by first downloading an RFID app onto their phone or by using a device. Then If a reader or RFID-app enabled smartphone is within range, the device or App could pick up the wireless signals transmitted when that card is being used to buy a product. The information was then input into a machine that can be purchased for $300-$400 to replicate the card (Zolfagharifard, 2015).

4. What is NFC? Where is it used? How can it be hacked? Describe incidents of NFC abuse.

Near-filed communication (NFC) is a popular IoT communication technology that is currently built into 20% of mobile phones, particularly in the latest iPhone 6 devices and Android models. The most common use of NFC is for mobile payment services such as Google Wallet.

NFC can be hacked with apps such as NFC proxy that is cable of copying the victim’s credit card data in real-time and replaying it later when the hacker wants to conduct fraudulent purchases. Hackers can also compromise the NFC chip in a nearby mobile phone and take over the device and make phone calls, send messages, and access files.

Hence, the incidents resulting from NFC abuse involve most public service payment systems and exhibit those resulting from RFID hacks.

5. The author talks about perfect enforcement. In your own words, what would perfect enforcement look like from your own work-life perspective? How far along the way are we in our knowing or unknowing pursuit of perfect enforcement?

In my opinion, perfect enforcement exhibits the character of fairness and accountability. That is, each employee must be given equal time to work from home, time for sick days, and employee benefits. This would take care of fairness. However, at the same time, the work we do should hold as accountable. Hence, using systems and new technology to track employees’ quality and timeliness would be critical. With that being said, I believe that we are getting closer to knowing the pursuit of perfect enforcement due to advancements in technology and the expansion of IoT devices that contain sensors to detect anything and keep as accountable for actions we take for granted or freely.

6. Describe juice jacking.

Juice Jacking refers to a phenomenon in which attackers rogue mobile phone power cords and successfully build a malware directly into compromised USB chargers so that they can bypass the victim’s device security safeguards and infect it. Once the phone is plugged to the charger, no pop-up alert is provided, and the malware isn’t visible on the list of running programs. However, the charger installs a backdoor on the device that allows the hackers to steal data such as banking information, capture passwords, read texts, track the movement of the victim, and make phone calls. Hackers usually compromise chargers at public charging station kiosks, airports, malls, and so on so that they can infect the greatest number of victims.

7. Research the butterfly effect. What does it describe? Describe a manifestation of the butterfly effect.

The butterfly effect is the idea that small things can have non-linear impacts on a complex system. The concept is explained with a butterfly flapping its wings and causing a typhoon. That is, even though a single butterfly flapping its wings can’t cause a typhoon, small events can still serve as catalysts that act on initial conditions (“The butterfly effect …”, n.d.). Hence, relying on this approach, the butterfly effect describes how everything in the world is connected, starting with small things that will end up forming complex designs. This phenomenon is a manifestation of the Internet of Things technology (IoT) and how digital devices are seamlessly connected to each other through networks.

References

The Butterfly Effect: Everything You Need to Know About This Powerful Mental Model. (n.d.). Retrieved from https://fs.blog/2017/08/the-butterfly-effect/

Zolfagharifard, E. (2015). Will you be a victim of digital pickpockets? Hacker reveals how easy it is to steal credit card numbers in seconds while you still have them in your hand. Daily Mail. Retrieved from https://www.dailymail.co.uk/sciencetech/article-2948212/Will-victim-digital-pickpockets-Hacker-reveals-easy-steal-credit-card-numbers-air-SECONDS.html