**Assignment 3: Sense Making of Computing Technologies**

**Niranjana Sathish Avilery**

Despite the rapid growth of the Internet of Things (IOT) applications and devices, security and privacy issues have become a major concern. According to current studies, security weak points have been detected in several IoT devices. Furthermore, these devices are not protected in many situations thanks to the lack of security mechanisms. [1] Critical infrastructure (Eg. transportation, city surveillance, public places) and industry both use IoT security cameras extensively. Globally, the market for video surveillance is projected to grow from US $45.5 billion in 2020 to US $74.6 billion by 2025, according to research firm Markets and Markets. Considering the prevalence and exponential growth of IoT cameras, understanding their security risks is important. [2]

Several people have sued a smart camera maker for "horrific" intrusions of privacy that revealed a security vulnerability in IoT devices in December 2020. It was claimed in the lawsuit that the security measures on the cameras were inadequate, allowing remote actors to take control of them. Further, the attackers allegedly harassed over 30 individuals in 15 households by using the cameras. According to the plaintiffs, the attackers demanded ransom, and even threatened them with murder in some cases.[3]

Figure 1 shows examples of vulnerabilities, features of the affected device, and threat-related information with respect to Smart-home security camera. As seen here, the CVEs targeted here tend to target smart living spaces, more specifically smart homes.

A group of hackers reportedly gained access to live feeds of 150,000 surveillance cameras inside hospitals, schools, companies, police departments via a breach in the security camera data collected by Silicon Valley startup Verkada Inc.[4] The attack showed the ease with which security feeds can be compromised and how common they are. Their attack method involved using a username and password to access ‘Super Admin’ account on the public internet. [5]

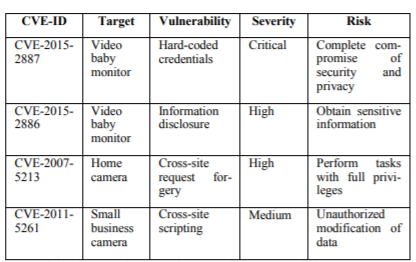
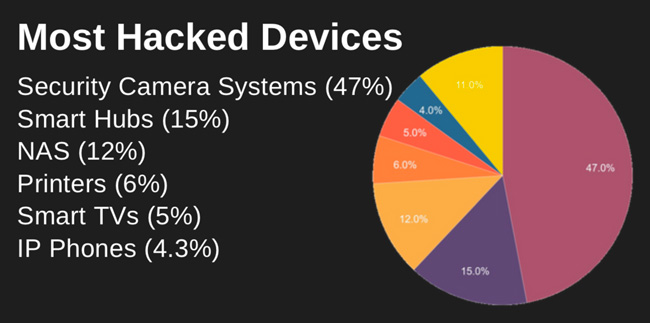
 

Figure 1 – Examples of security threats ranked according to their severity level [6]

Figure 2 – Most hacked devices according to a study by SAM Seamless Networks [7]

Figure 2 indicates a study where 47% of the most vulnerable devices are smart cameras, followed by smart hubs such as Googlehome and Amazon Alexa, with attacks coming mostly from China and the U.S.

As we can see in various instances and case studies, surveillance system threats are the most vulnerable and this issue needs to be addressed.

**REFERENCES**

[1] P. A. Abdalla and C. Varol, “Testing IOT security: The case study of an ip camera,” 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020.

[2] N. N. L. on July 15 and 2021, “New Report: Ransomware, Vulnerabilities and IoT Security Threats,” Security Boulevard, Jul. 15, 2021. https://securityboulevard.com/2021/07/new-report-ransomware-vulnerabilities-and-iot-security-threats/ (accessed Feb. 06, 2022).

[3] “When it Comes to Stopping IoT Security Camera Breaches, Focus on Procurement,” Security Intelligence. https://securityintelligence.com/articles/iot-security-camera-breaches-procurement/ (accessed Feb. 06, 2022).

‌[4] W. Turton, “Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals,” Bloomberg.com, Mar. 09, 2021.

[5] “IoT Security: Thieves Are Targeting Smart Cameras — Here’s How To Stop Them,” Security Intelligence. https://securityintelligence.com/articles/iot-security-smart-camera-thieves/ (accessed Feb. 06, 2022).

[6] J. Bugeja, D. Jonsson, and A. Jacobsson, “An Investigation of Vulnerabilities in Smart Connected Cameras,” 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Mar. 2018, doi: 10.1109/percomw.2018.8480184.

[7] “Smart home security devices most at risk in IoT-targeted cyber attacks,” Help Net Security, Jun. 13, 2019. https://www.helpnetsecurity.com/2019/06/13/iot-targeted-cyber-attacks/ (accessed Feb. 06, 2022).