Name: Teh Jia Xuan	Student ID: 32844700
Assignment 4 - CyberSecurity	

Article chosen: Here's how to remotely take over a Ferrari...account, that is

Write a short summary of the news item in your own words (max 200 words).

The article highlights vulnerabilities that Yuga Labs' Sam Curry found, one of them allowing hackers to track and take over up to 15 million vehicles (Hardcastle, 2023). The bug was found in a company specialising in GPS technology called Spireon. Curry executes remote code over Spireon through authorisation bypass and SQL injection (Hardcastle, 2023). The bug permitted tracking and commanding to all vehicles that subscribe to their service. Spireon implements remedial measures immediately and further strengthens its security to ensure its customer's safety (Hardcastle, 2023). Moreover, the researchers found vulnerabilities in Ferrari and BMW's systems where attackers can take control of customers' accounts (Hardcastle, 2023). Furthermore, attackers can access admin stuff like achieving sensitive data. But the car manufacturers didn't make any comment (Hardcastle, 2023). A vulnerability was also found in Mercedes-Benz's system, allowing hackers to access internal data by using "request specific tools for repair" as an excuse to create an account to sign in to GitHub. But Mercedes-Benz didn't see it as a problem(Hardcastle, 2023). Thus, the researcher created accounts to achieve all the sensitive data used by Mercedes-Benz employees and disguise themselves as employees. An access control vulnerability was also discovered on the Toyota Financial app(Hardcastle, 2023). However, all the manufacturers have fixed the vulnerabilities, and customers' data is unaffected (Hardcastle, 2023).

Identify which software, hardware or system is affected (max 50 words)

The vulnerabilities affected major car brands' systems, like accessing JavaScript that contained API keys which enabled attackers to control customer accounts (Hardcastle, 2023). Additionally, expose sensitive data like source code of applications through misconfigured single-sign-on(SSO) portal (Hardcastle, 2023). Moreover, attackers can track and command 15 million vehicles using SQL injection and authorisation bypass in telematic systems(Hardcastle, 2023).

Describe how the problem was discovered and how it was initially published.

The research expands on the earlier car hacking done by Yuga Labs' Sam Curry, which reveals the flaws of major vehicle brands and telematic companies where hackers can take control of their vehicles and accounts. He started his initial research by studying Hyundai's app traffic through Burp Suite. He found he could bypass JASON Web Token(JWT) and email existing checking of Hyundai's website by adding CRLF characters to the email during registration (Curry, 2022). He then creates an account by using victim's email to take over victim's actual account and get control of his car. Now the research done by Curry (2023), vulnerability in Spireon, he discovered weaknesses in authorisation bypass and SQL injection of Spireon and control vehicles that used their service.

Discuss how serious the issue/weakness/attack is, describe what is necessary to exploit the weakness, evaluate what the consequences might be if it is exploited, and what reactions you think are necessary/useful on (i) a technical level, (ii) in terms of human behaviour, and (iii) on a policy level (between 200 and 350 words).

The vulnerabilities found by Curry are serious ones, as they could allow hackers to take over their cars and accounts. The vulnerabilities were found in major car brands' systems and telematic companies. Vulnerabilities were found in Hyundai's system, which allows hackers to bypass JWT and email existing checking by adding CRLF characters at the end of victim's email (Curry, 2023). This enables hackers to create an account by using victim's email and taking over one's account. Alternately vulnerabilities were found in Spireon's system, it includes weaknesses in the outdated administration portals, which he discovered the system appeared to have vulnerability to SQL injection as input fields were sent to the database without being checked for malicious code (Curry, 2023). Upon further discovery, he discovered endpoint of "admin.spireon.com" could be accessed, but it triggered 403 forbidden error. It indicates that the endpoint is publicly accessible, which means he could perform authorisation bypass attack (Curry, 2023). After that, he could access full administrative portal by putting "%0d" prefix to Get/admin and Get/dashboard (Curry, 2023). The consequences of these vulnerabilities are that attackers could fully control their cars and accounts by achieving victims' email addresses. It can cause panic among the public by honking all the vehicles, disabling starters etc. Moreover, criminals could easily plan and carry out crimes and cause chaos when they can track police's location using Spireon's vulnerabilities to avoid arrest. Additionally, hackers can steal personal information from victims' accounts to perform attacks on them like fraudulent activities etc. However, these vulnerabilities can be solved by assigning unique salt for each user as it can prevent email checking bypasses (The Guardian, 2016). For example, a salt is randomly generated for each user, along with hashed password. Thus, their salt values are unique, even if the users have the same password and hence different hash passwords. Moreover, authorisation bypass can be prevented by updating the system regularly (Rapid7, n.d.). Such as keeping firewalls and software up to date to recognise recent patterns of cyberattacks and fixing known vulnerabilities to improve authorisation mechanisms so that they can provide stronger protection against unauthorised access. Additionally, these vulnerabilities can be prevented by developing a security policy, such as acceptable use guidelines (Paul, 2022). For instance, employees can only visit particular websites, restrict types of content allowed to be sent during working hours, restrict types of devices to connect to the organisation's network, databases containing sensitive data should not connect to outside network etc.

List of Reference

Curry, S. (2022, November 29). *We recently found a vulnerability affecting Hyundai and Genesis vehicles where we could remotely control the locks, engine, horn, headlights, and trunk of vehicles made after 2012* Retrieved from, https://twitter.com/samwcyo/status/1597695281881296897?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1597695281881296897%7Ctwgr%5E7ffcb9ffe2f6f234cdb9dbb3d019b76c5eec10df%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fsamcurry.net%2Fweb-hackers-vs-the-auto-industry%2F

Curry, S. (2023, January 11). *Web hackers vs. the auto industry: Critical vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and more*. Sam Curry | Web Application Security Researcher. Retrieved from, https://samcurry.net/web-hackers-vs-the-auto-industry/

Hardcastle, J. L. (2023, January 9). *Here's how to remotely takeover a Ferrari...account, that is*. The Register® - Biting the hand that feeds IT. Retrieved from, https://www.theregister.com/2023/01/07/car_hacking_ferrari_account/?td=keepreading

Kirvan, P. (2022, June 13). *What is acceptable use policy (AUP)? - definition from whatis.com*. WhatIs.com. Retrieved from, https://www.techtarget.com/whatis/definition/acceptable-use-policy-AUP#:~:text=An%20acceptable%20use%20policy%20(AUP)%20is%20a%20document%20stipulating%20constraints,being%20granted%20a%20network%20ID.

Rapid7. (n.d.) *What is patch management? Benefits & Best Practices*. Retrieved from, https://www.rapid7.com/fundamentals/patch-management/

The Guardian (2016, December 15). *Passwords and hacking: The jargon of hashing, salting and SHA-2 explained*. Retrieved from https://www.theguardian.com/technology/2016/dec/15/passwords-hacking-hashing-salting-sha-2