EN4720: Security in Cyber-Physical Systems
Exercise — Big Security Breaches and Exploring CVE

Name: Thalagala B. P.
Index No: 180631J

March 15, 2023

This is an individual exercise!
Due Date: 17 March 2023 by 11.59 PM

Big Security Breaches

It is important that you keep yourself up to date on previous and contemporary computer security breaches. Find real-world examples of breaches of Confidentiality, Integrity, Availability, Authentication, Authorization, and Non-repudiation using the Internet and fill the following table. Add a three-four sentence explanation for each example.

You can refer to books, web pages, research publications to gather the information. Feel free to copy-paste from the source, but make sure you add the citation. The first row is filled for you as an example.

The following sites may help you to get started:

- http://www.networkworld.com/topics/security.html
- http://www.zdnet.com.au/topic/security/

Exploring CVE

CVE, short for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws. Learn more about CVE here.

Search the CVE database at cve.mitre.org for vulnerabilities in one of the smartphone apps you use. Study a few of them carefully to get a sense of how beneficial this database can be for a security professional. Identify five flaws in your selected app and fill out the table below.

- Column 1: CVE ID of the vulnerability.
- Column 2: A brief description of the vulnerability in a way that a novice user can understand.
- Column 3: Which security goal (out of the CIA triad) is breached as a result of the vulnerability.
- Column 4: Add the title and URL for any known real-life incidents.

Table 1: Real-world examples of security breaches.

Security Goal	Example	Explanation
Confidentiality	Apache Struts vulnerability	An Apache Struts vulnerability allowed hackers to steal data on 143 million Equifax customers [8]. Struts is vulnerable to remote command injection attacks through incorrectly parsing an attacker's invalid Content-Type HTTP header. The Struts vulnerability allows these commands to be executed under the privileges of the Web server. This resulted in sensitive data leakage [2].
Confidentiality (*Keep data private or secret/ Control access*)	Marriott hotel chain's reservation system compromisation 2018	In late 2018, the Marriott hotel chain announced that one of its reservation systems had been compromised, with hundreds of millions of customer records, including credit card and passport numbers, being exfiltrated by the attackers[6].
Integrity (*Trusted/ No unauthorized modification*)	SolarWinds attack of 2020	SolarWinds offers an IT performance management and monitoring system called Orion. The hackers used a supply chain attack to insert malicious pieces of code into the Orion framework. It allowed the hackers to access system files and hide their tracks by blending into the Orion activity. More than 18,000 customers of SolarWinds were affected including the US departments of health, treasury, and state[1].
Availability (*Systems are up and running*)	GitHub Distributed Denial-of-Service (DDoS) attack 2018	February 28, 2018 GitHub.com was unavailable from 17:21 to 17:26 UTC and intermittently unavailable from 17:26 to 17:30 UTC due to a DDoS attack. The attack originated from over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints. It was an amplification attack using the Memcached-based approach that peaked at 1.35Tbps via 126.9 million packets per second[7].
Authentication (*Who are you?/ Are you who you claim to be?*)	2012 LinkedIn hack	The social networking website LinkedIn was hacked on June 5, 2012, and passwords for nearly 6.5 million user accounts were stolen by Russian cyber criminals. Owners of the hacked accounts were no longer able to access their accounts, and the website repeatedly encouraged its users to change their passwords after the incident[3].
Authorization (*What abilities and access should this user have?*)	Adobe Systems Data Breach 2013	October 2013, hackers stole login information and nearly 3 million credit card numbers from 38 million Adobe users[5].
Non-Repudiation (*To not allow someone to deny something*)	2016 Democratic National Committee (DNC) email leak	A collection of DNC emails stolen by one or more hackers, who are alleged to be Russian intelligence agency hackers. This collection included 19,252 emails and 8,034 attachments from the DNC, the governing body of the United States' Democratic Party[4].

Table 2: Vulnerabilities in a smartphone application.

Vulnerability	**Brief Description**	**Breach of security goal**	**Any known real-life case with URL**
CVE-2020-1908	Improper authorization of the Screen Lock feature in WhatsApp and WhatsApp Business for iOS prior to v2.20.100 could have permitted use of 'Siri' to interact with the WhatsApp application even after the phone was locked. An attacker who gains access to Siri may be able to read and send messages, access contacts, and perform other actions within the WhatsApp application without having to unlock the phone.	Confidentiality	None reported
CVE-2021-24035	A lack of filename validation when unzipping archives prior to WhatsApp for Android v2.21.8.13 and WhatsApp Business for Android v2.21.8.13 could have allowed path traversal attacks that overwrite WhatsApp files. This can allow an attacker to access files and directories outside of the intended location by manipulating the path used to access them.	Integrity	None reported
CVE-2020-1901	Receiving a large text message containing URLs in WhatsApp for iOS prior to v2.20.91.4 could have caused the application to freeze while processing the message. This can result in a denial of service to the user when he is involved in some interaction with the App.	Availability	None reported
CVE-2019-3571	An input validation issue affected WhatsApp Desktop versions prior to 0.3.3793 which allows malicious clients to send files to users that would be displayed with a wrong extension. The attacker can send files that can either execute malicious code, access sensitive information or both. The user may believe that they are opening a safe file, but the actual contents could be malicious.	Integrity, Confidentiality	None reported
CVE-2022-36934	An integer overflow in WhatsApp could result in remote code execution in an established video call. The attacker could gain access to the system, potentially steal sensitive information or modify the system's behavior, leading to a loss of data or disruption of service.	Integrity, Confidentiality	None reported

References

[1] SolarWinds Attack & Details You Need To Know About It | Simplilearn.

[2] CVE-2017-5638: The Apache Struts vulnerability explained: Synopsys, Nov 2021.

[3] 2012 LinkedIn hack, November 2022. Page Version ID: 1122344573.

[4] 2016 Democratic National Committee email leak, February 2023. Page Version ID: 1141363117.

[5] Terena Bell. Adobe's CSO talks security, the 2013 breach, and how he sets priorities, April 2018.

[6] Josh Fruhlinger. Marriott data breach FAQ: How did it happen and what was the impact?, February 2020.

[7] Sam Kottler. February 28th DDoS Incident Report, March 2018.

[8] Jeff Luszcz. Apache struts 2: how technical and development gaps caused the equifax breach. *Network Security*, 2018(1):5–8, 2018.