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/

Furthermore, as security professionals, it is important that we stay updated. Below are some resources that you can use to stay updated.

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 [2]. 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 [1].
Confidentiality (*Keep data private or secret/ Control access*)		
Integrity (*Trusted/ No unauthorized modification*)		
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.
Authentication (*Who are you?/ Are you who you claim to be?*)		
Authorization (*What abilities and access should this user have?*)		
Non-Repudiation (*To not allow someone to deny something*)		

Table 2: Channels to stay informed.

Technology Partners	**Government**	**Security Organizations**	**Security News Sites**
Microsoft	US-CERT	SANS ISC	Dark Reading
Red Hat	NIST NVD		The Hacker News
Ubuntu	SLCERT		CSO Online

Table 3: Vulnerabilities in a smartphone application.

Vulnerability	**Brief Description**	**Breach of security goal**	**Any known real-life case with URL**

References

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

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