Southern New Hampshire University

CS-405 Secure Coding

Week 5-1 Case Study: Triple A and Defense in Depth

**Introduction**

1. **Name of case and link**

Aadhar database breach

<https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html>

1. **Date of case**

January 2018

1. **Why did this case make the news?**

This data breach has been a very huge case as it exposed 1.1 billion Indian citizens identity, personal data and financial data. Which is a very massive effect on data theft which also exposed people’s biometric data.

**Describe the breach**

1. **Type of security or data breach or combination**

First, the personal information or identity of the citizens has been exposed which is their name, address, phone number, etc.

Second, their bank information and account information linked with Aadhar card has been exposed which resulted in financial breach.

Third, fingerprints and photographs data of the people was also stolen.

1. **Why was this company a target?**

The Aadhar database is a very big database in India that contains personal information and identity of the citizens. The hackers targeted this database as it is a biggest database with huge data which they can use it to initiate big frauds and demand government for their needs.

**Identify the threat(s)**

1. **Immediate threat(s)**

It causes both identity theft and financial fraud

1. **Potential threat(s) if the vulnerability goes unresolved**

If the vulnerability goes unresolved then the attackers might use that data to threat the government to fulfill their needs and might release those data to public which creates panic and losses trust and they might use that data to perform financial fraud as well.

**What could a developer have done to prevent this breach?**

Implementing strong authentication and authorization might prevent this kind of breaches. Ensuring proper setting up security defense system and performing regular audits to it will prevent any kind of gaps or vulnerabilities that attackers might use to perform the breach.

**Which policy or policies will help prevent this type of attack?**

Data encryption policy will help preventing this type of attacks. Ensuring proper encryption to the use data is most important to prevent the cyber-attacks.

**Summarize the case by explaining the role of best practices, Triple A and defense in depth in preventing future attacks.**

1. **Authentication**

Ensuring proper authentication like using any authenticating tools might have reduced this attack to happen.

1. **Authorization**

Providing limited access to the authorized people will helps in ensuring proper security and limits the access to unauthorized persons which prevents from this attacks.

1. **Accounting**

Proper and frequent security audits and maintenance of the defense system will reduce the risk of cyber-attacks.

1. **Defense in depth**

Creating multiple layers of security will protect data from cyber-attacks. While creating those layers of security it should be very balancing, as enough layers are required to protect from attacks and too many layers will cause complexity. Having enough number of firewalls and security layers will prevent the attackers from hacking.