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

Chris Bridges

Southern New Hampshire University

CS 405: Secure Coding

Professor Mill

30 September 2025

**Introduction**

* 2019 Capital One Data Breach
* <https://web.mit.edu/smadnick/www/wp/2020-07.pdf>
* This breach made headlines due to the volume of information that was compromised, as well as the manner of the attack. Over 100 million people had their personal information and privacy exposed.

**Breach Description**

* A misconfigured web application firewall (WAF) enabled exfiltration of sensitive credit card application data (Khan et al, 2022). The attacker bypassed the web application firewall due to misconfiguration and exploited a server-side request forgery (SSRF) vulnerability in the web application behind the web application firewall. The attacker manipulated the original request, which allowed the server to process the malicious request, which was then executed by the application.
* Capital One was the target of the attack due to the large amount of financial assets controlled by the company and the large database of customers’ information.

**Threat Identification**

* Compromise of cloud identity using SSRF attack, database access, exfiltration of personal information, and potential risk of fraud and extortion (Neto et al, 2020).
* If unresolved, customers’ information could be exfiltrated again, resulting in customer identity theft, legal liability, and financial loss for customers and the company.

**Breach Prevention**

* Properly configuring WAF settings would minimize the risk of this type of attack. Utilize logging and detection tools to ensure that breaches are identified and secured before data theft becomes possible. Conduct third-party security audits to ensure that bad actors cannot infiltrate or manipulate data.

**Triple A and DiD Best Practices Explanation**

* **Authentication.** Enforce phishing-resistant multi-factor authentication for people with admin access or service accounts. Require multiple parties for sensitive actions.
* **Authorization.** Enforce role-based access control and resource-level permissions. Ensure the default is to deny access. Separate production and dev environments and accounts.
* **Accounting.** Ensure logs are kept with access and modification history. Use logs to detect anomalies or data transfers. Maintain logs and records for compliance and forensics.
* **Defense in Depth.** Don’t rely on a single level of protection. Combine multiple layers like properly configured firewalls, identity checks, MFA, encryption, backups, and employee training focused on phishing and security.

**References**

Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022, November 7). *A systematic analysis of the Capital One Data Breach: Critical Lessons Learned | ACM Transactions on privacy and security*. research-article. <https://dl.acm.org/doi/full/10.1145/3546068>

Neto, N., Madnick, S., Paula, A. de, & Borges, N. (2020, January). *A case study of the Capital One Data Breach*. A Case Study of the Capital One Data Breach. https://web.mit.edu/smadnick/www/wp/2020-07.pdf