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

Ryan DeBraal

CS-405-X6389 Secure Coding 21EW6

**Introduction**

**Name of case and link:**  
Hacks of OPM databases compromised 22.1 million people, federal authorities say  
<https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/>

**Additional resources:**

<https://fas.org/sgp/crs/natsec/R44111.pdf>  
<https://www.opm.gov/cybersecurity/cybersecurity-incidents/>

**Date of case**

Discovered in April 2015, divulged to the public in June 2015.

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

The human resources department of the US government was infiltrated exposing the personal data of over 22 million Americans.

**Describe the breach**

In June 2015, the U.S. Office of Personnel Management (OPM) revealed that a cyber intrusion had impacted its information technology systems and data, potentially compromising the personal information of about 21.5 million former and current federal employees.

On April 15, 2015, a security engineer named Brendan Saulsbury discovered suspicious outbound traffic: a beacon-like signal pinging to a site called ¬opm¬security.org. But the agency owned no such domain.

After digging deeper, Mr. Saulsbury discovered the source of the outbound traffic. A file called mcutil.dll, a file common to McAfee products, however OPM didn’t use McAfee products.

It was eventually discovered to be a variant of PlugX, a remote-access tool commonly deployed by Chinese hackers: <https://attack.mitre.org/software/S0013/>

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

Both. The DiD defenses were breached and the data being “protected” by these lines of defense were stolen.

**Why was this company a target?**

Theft of personally identifiable information (PII) may be used for identity theft and financially motivated cybercrime, such as credit card fraud. Many have speculated that the OPM data were taken for espionage rather than for criminal purposes.

**Identify the threat(s)**

**Immediate threat(s)**

Exposure of millions of federal employees’ personal information (social security numbers, bank accounts, addresses, etc.)

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

Potentially many millions more of stolen personally identifiable information (PII).

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

The compromised file, mcutil.dll, could have been discovered (either by name, MD5 checksum, etc.) if it had been “blacklisted” and found during routine network wide scanning effort.

The network could have been secured to not allow any non-approved files from accessing and sending data to URLs outside the intranet.

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

Better security surrounding what processes are allowed to make external internet-facing API calls. Better scanning efforts.

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

**Authentication**

The process of authentication is based on each user having a unique set of criteria for gaining access. Since this breach took place on an internal computer, this means that at some point the bad actor was able to “spoof” a user with valid credentials.

**Authorization**

The file in question should never had the amount of access it had been granted. Either the account’s access levels had been elevated as part of the intrusion effort, or more likely, the account was simply given too much access to begin with to alleviate the headaches of having very granular security roles.

**Accounting**

Accounting for the resources a file is using could have easily exposed this issue. There is no reasonable explanation for why an apparent McAfee file should be exporting data in what must have been gigabytes or even terabytes of information to account for the 22 million exfiltrated records.

**Defense in depth**

The failure of the OPM’s DiD strategy is a difficult problem to nail down. To be able to breach so many layers from the outside seems unlikely. What is more likely is that the hacker’s leveraged some form of social engineering such as phishing. Someone in the OPM offices opened an email or downloaded a file while contained the malicious code. Multiple redundant layers of security are pretty much useless when your own employee’s accidently open the door for the invaders.

