Section 2: Week 5: Propose Strategies and Tools for Cloud Security

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

July 5, 2020

North Central University

# Propose Strategies and Tools for Cloud Security

NCU Financial (NCU-F) has fallen the victim of targeted malware attacks, and these assaults have disrupted internal systems. For instance, infected workstations are flooding the intranet with bogus traffic slowing communications to a halt. Ransomware has also corrupted several mission-critical systems, such as databases and monitoring solutions, impacting the businesses’ ability to make informed decisions promptly. The organization needs a strategy for restoring the security posture and removing the invasion from its network.

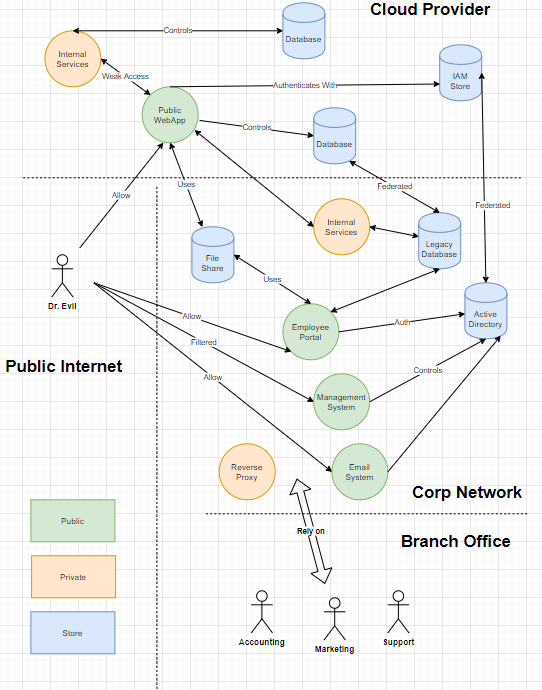
# Section I: Attacking Application Layer

Traditional cybersecurity solutions focus on hardening the network parameter with firewalls and vulnerability scanners. However, this approach is no longer sufficient as attackers center their efforts on the application layer (Astani & Ready, 2016). By design, anonymous users can interact with the organization through public interfaces, such as web services and email. When malicious actors exploit Structured Query Language Injections (SQLi) or embed ransomware into mail attachments—it bypasses these network barriers and allows unauthorized access to information. Further complicating matters, the boundary of the network is becoming more abstract due to the notion of “everything as a service” (Paller, Mahalik, Skoudis, & Ullrich, 2020).

## Poisoning Waterholes

NCU-F has three logical segments to their topology, namely branch offices, the corporate network, and cloud infrastructure (see Figure 1). Supporting business workloads across the company requires high-levels of connectivity between the segments. While possible to limit the exposure through process changes, reduces team velocity, and often encountering political pressure and resistance (Weston, Conklin, & Drobnis, 2018). For instance, a central file server is accessible from the cloud infrastructure via Virtual Private Networking (VPN) and the branch office employees. When the web application becomes compromised, then malware can poison the shared waterhole and burrow further into the network. Elevation paths can also exist across federated stores, such as identity and data management. Perhaps the attacker exploits a vulnerability in the WordPress Content Management System (CMS) and gains access to the associated Postgres database. Sufficient restrictions must exist, or these attacks can cascade through integration points, such as foreign table wrappers, that bridge into related connected systems.

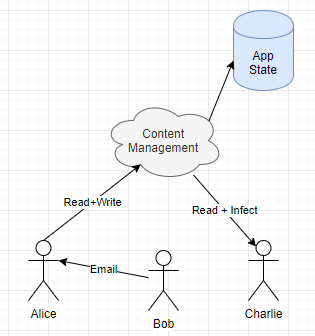
Figure 1: NCU-F Network Topology



## Invalid Encoding Scenarios

Vulnerabilities can exist in the web platform that does not require infrastructural system compromise. Invalid content-encoding can result in command injection at either the presentation (e.g., cross-site scripting) and transport layer (e.g., cross-site response forging). These situations enable the attacker to elevate outside their standard context and bypass security boundaries. For example, Bob sends a malicious link to Alice, which triggers malicious JavaScript code within her web-browsers (see Figure 2). Now the script can use her identity to manipulate the CMS and infect other system users. It can be challenging to prevent these scenarios, given the continuous stream of publically disclosed vulnerabilities in mainstream web platforms.

Figure 2: Cross Content Issues



## Exposed Internal AppState

While there are strategic advantages to manipulating web content and compromising infrastructural components, many attacks do not require either attack vector. Instead, the attacker can focus their efforts on weak controls such as missing authentication and authorization policies. For instance, the session identifier is a numeric counter, stored in a cookie. The user needs to authenticate into the system before getting a valid sequence number but can then fiddle with the value to arbitrarily join other sessions. Other permutations of vulnerabilities exist in query strings, allowing the user to enumerate through the database and find draft content. These drafts might have undisclosed information, like merge announcements or changes to corporate strategy. When the confidentiality of that information is lost, it enables third-parties an upper hand such as buying substantial quantities in that merger target and bidding up the price.

## Economics of Web Attacks

Malicious users seek espionage, sabotage, and subversion tactics against their targets (Kovacs, 2018).