Gabriel Tinsley
CS 331
2/23/2025

Case Study Analysis

Case Study: SolarWinds attack

- Incident Summary

In December 2020, the SolarWinds attack on SolarWinds Orion software was discovered. The attackers were believed to be part of a nation-state and put malicious code into a routine software update that was then sent to SolarWinds customers. The customers included government agencies and large companies and the attack was undetected for months allowing threat actors to steal sensitive data.

- How Integrity Was Violated

Once attackers were inside the network, they were able to manipulate data and credentials to move wherever they wanted. They avoided detection by changing logs and tampering with security protocols which all violated data integrity.

- How It Could Have Been Prevented

A way this could have been prevented was by continually doing integrity checks of users and whenever someone modified a file that should be detected. Also adding a limit to the amount of data manipulation a user can do so that would stop attackers from moving wherever they wanted.

- Which Integrity Model Would Have Helped?

The model that would have helped the most is Biba Integrity Model. This model enforces “No read-down” and “No write-up” so that would have prevented unauthorized modifications in SolarWinds’ software.

Sources:

Saheed Oladimeji, Sean Michael Kerner. “Solarwinds Hack Explained: Everything You Need to Know.” WhatIs, TechTarget, 3 Nov. 2023, www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.