Kyle Belanger, Owen Raftery, Thomas Murphy, Sasha Shikhanovich
12/10/2024
ECE 371 Honors Project Research

NTP Time Errors Lead to Security Threats

NTP is a crucial tool used across the eternity of the computer systems industry, and although it dates back to 1985, it remains the most used networking protocol for modern computing synchronization. It is necessary for computers across a network to be able to synchronize due to the fact that large inconsistencies in timing between devices in commercial applications could lead to operational issues and also open the door to cybersecurity risk. NTP clocks naturally are not perfect and will drift from each other in the measure of seconds to minutes if not properly synchronized after some time. When a company has hundreds of devices all on the same network this drift, if not accounted for, will cause all devices to believe the correct time is different. This means that log timestamps will not align with each other, and when passed to a system to check for unusual behavior, the times of events will appear wrong, and the system will struggle to point out if the system has been compromised. Attackers can use this to their advantage by covering their tracks during an attack by tampering with NTP timing to make them harder to identify [1]. By purposely causing delays to disrupt NTP protocol, attackers can overwhelm systems and trick them into resending data, creating false timestamps on logs, or losing logs as a whole. This allows them to create a side channel in the network that is more or less undetectable, making their attack patterns appear to have happened at a different time, or not at all in some cases. Attackers also have the ability to monitor NTP timing patterns when observing a network. Over time, patterns will show on how long it takes for the server to carry out certain calls, such as the time it takes to process an incorrect/correct password, and what encryption method the network is using. With this information, the attacker is able to gain insight on the network without having to breach it, all based on timing inconsistencies across NTP [2]. Overall, it is vital for network devices to remain in sync with each other to avoid unnecessary security risks, and protect sensitive information.

Sources:

[1] BeyondTrust, "The Implications of Network Time Protocol (NTP) for Cybersecurity," BeyondTrust Blog. [Online]. Available: https://www.beyondtrust.com/blog/entry/the-implications-of-network-time-protocol-ntp-for-cybersecurity. [Accessed: 13-Dec-2024].

[2] Z. Tan, "Document from Mobicom 2021: Timing and Communication Security," University of California, Riverside. [Online]. Available: https://cs.ucr.edu/~ztan/documents/mobicom21-pre.pdf. [Accessed: 13-Dec-2024].