Executive Summary: NTP-based Data Infiltration Channels

Rafael Ortiz <rortiz12@jhu.edu>
Ramon Benitez-Pagan <ramon.benitez@jhu.edu>
Stephen Scally <sscally@jhu.edu>   Cyrus Bulsara <cbulsar1@jhu.edu>

Many papers focus on creating covert channels for the purpose of data exfiltration. That is, they attempt to remove some information from a protected network. Less common appears to be the concept of data *infiltration*, where a covert channel is established to secretly move information *inside* a protected network. Many exfiltration oriented channels make assumptions about extant arbitrary infiltration channels being available for loading the tooling necessary to establish the outbound channel. We are proposing studying and implementing an NTP-based covert channel for infiltrating unauthorized information into a secure network.

Problem Statement

In typical enterprise threat scenarios, data infiltration is often achieved by way of phishing emails, TLS tunnels, or shell access. From there, exfiltration may be achieved by a number of covert channels. However, in certain locked-down networks, it may not be possible to send inbound email, establish a TLS tunnel, or directly access protected machines. On the other hand, administrators of these networks typically *do* want their machines clocks to be synchronized, since Bad Things^{TM} happen when clocks drift out of sync. This presents NTP as a potential channel whereby information from the Internet can slowly leak into the inside of a protected network. We will consider two scenarios: DMZ access and direct access.

DMZ Access

In DMZ access, devices in a secure network syncrhonize their clocks via an NTP server that is located in a controlled DMZ. That NTP server syncrhonizes its clock by connecting to one or more trusted NTP pools. Any information that can survive a stratum layer[*] may reach devices through the DMZ.

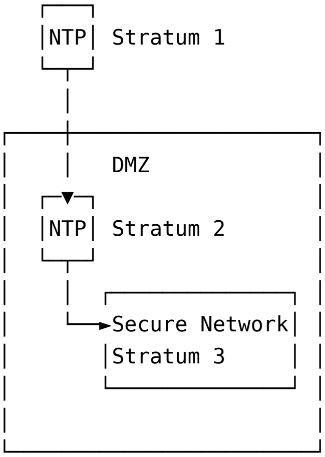

Figure 1. The DMZ Access NTP scenario, where an NTP server in a DMZ serves replies to clients in a secure inner network.

[*] In NTP, a stratum is a layer of devices that are the same distance from a reference clock. Reference clocks, considered a source of truth, are at stratum layer 0. Servers that rely on reference clocks are at stratum layer 1, and so on. In our DMZ scenario, if public pools are at stratum 1, then the DMZ NTP server is at stratum 2, and internal devices are at stratum 3.

Direct Access

In direct access, devices in a secure network synchronize their clocks directly via NTP to a trusted, publicly available, pool. Any information that the NTP server can pack into an NTP reply may reach devices inside this network.

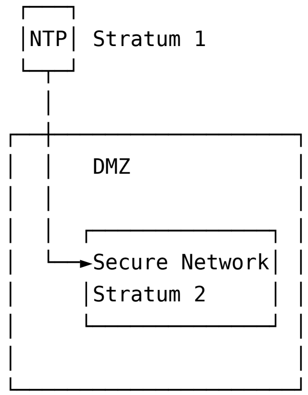

Figure 2. The Direct Access NTP scenario, where clients in a secure inner network are allowed direct access to NTP pool servers.

Project Summary

We are proposing the creation of an extended Berkeley Packet Filter (BPF) Traffic Control (TC) classifier (also known as a filter) that can be layered on top of existing NTP servers, or on routers between an NTP server and the target client, that can modify NTP server replies such that data may be infiltrated into secure networks. We will consider prior art on NTP covert channels and NTP as a covert storage cache and device a method for data infiltration in one or both of the two scenarios.

The chosen methodology for the Direct Access NTP scenario is the use of NTP extension fields. NTP allows for extension fields for proprietary add-ons to NTP, such as authentication, that implementators may use. Middleboxes are instructed by the RFC to not interfere or alter in any way the contents of these extension fields, as doing so may break NTP implementations which could lead to a denial of NTP service on the network the middlebox is protecting. Denial of NTP can be abused by attackers to do Very Bad Things, and should be avoided.

With the potential covert channel identified, we will fully define and document the channel. We will pay attention to factors such as: channel bandwidth, channel resiliance, channel covertness, and so on.

After defining the channel, we will implement and test the channel in a virtual environment. There will be two components to the channel, a TC filter and a receiver application that can decode received information. Ideally, we will build the receiver with nothing but tools available on the target machine, requiring no outside applications. However, for the purposes of this paper, we will consider the infiltration of data into a secure network as "good enough," and leave data reconstruction as a problem for the reader.

Project Breakdown

This is a rough outline of our project plan. At this stage, steps may be added or removed as necessary.

1. Study prior art on NTP storage channels and NTP covert caches
2. Identify potential NTP storage channels that satisfy the following criteria:
    - Do not noticeably interfere with normal NTP functionality
3. Design and document one or more covert channels that meet these criteria
4. Implement the channel as a BPF TC filter, with a receiver application
    - (optionally) Document a method to reconstitute data using nothing but OS native utilities
5. Demonstrate our implementation working in a virtual machine environment

Our final deliverables will be:

- A working sender and receiver application
- A report with the following sections:
    1. Abstract
    2. Introduction, covering background on NTP channels
    3. Related works in NTP covert channels
    4. Design of our channel
    5. Implementation of our channel
    6. Methods for discovering and defeating our channel
    7. Conclusions and Future Work
    8. Bibliography

- A video reviewing the above paper and demonstrating our implementation

Project Milestones

The milestones are presented in rough expected chronological order.

- (Milestone 1 - Cyrus) Potential NTP storage channels identified for selection (complete)
- (Milestone 2 - Stephen) Chosen NTP storage channel(s) identified, designed, and documented (in progress)
- (Milestone 3 - Rafael) BPF TC filter implemented (in progress)
- (Milestone 4 - Rafael) Receiver application implemented (in progress)
- (Milestone 5 - Stephen) Native receiver methodology documented
- (Milestone 6 - Cyrus) Techniques to defeat our covert channel documented
- (Milestone 7 - Cyrus) Report finalized
- (Milestone 8 - Stephen & Rafael) Video review and demonstration

Project Timeline

Milestone	Expected Completion Date
Preliminary Milestones	
1	12 July 2021
2	19 July 2021
Development Milestones	
3	02 August 2021
4	02 August 2021
5	09 August 2021
6	09 August 2021
Report Milestones	
7	16 August 2021
8	20 August 2021