white paper

The Traceability of Time Synchronization: Inside vs Outside the Network

spectracom

Internet Time Servers

- Time from outside the network results in variability from the internet
- Unknown time sources and unknown traceability
- User unable to audit the time source

GPS Time Server Appliances

- Time from inside the network is at least 1,000 times more accurate
- Direct connection to very accurate and traceable GPS time
- Full logging of synchronization

In today's modern networking infrastructures, great care is taken to ensure networks are reliable, highly available, and most of all, secure. Cybersecurity has emerged as a critical area in all facets of the internet. It's an area that companies spend millions on each year. Yet still, there are often overlooked areas which degrade security. One example of this is time.

As simple as it sounds, time plays a critical role in synchronizing core business and network systems. It supports authentication protocols as well as accurate log files critical for an audit trail necessary for any cyber forensics program. As such, synchronization is often a requirement for network security standards such as the Payment Card Industry's Data Security Standards. PCI DSS section 10.4 requires a traceable time source for synchronization of ecommerce systems.

This document briefly discusses the differences between a time source from within the network compared to outside the network with considerations for traceability for a network deployment of network time protocol (NTP).

NTP-over-the-Internet Increases Synchronization Variation

NTP is a mature network protocol for synchronizing a local system to a time server. NTP time servers are widely available on the internet. But you'll need to carefully consider if internet time servers are appropriate for your application. Even for internet time servers operated by national authorities, such as NIST or the US Naval Observatory that are based on extremely accurate atomic clocks, there are many factors that impact traceability. According to ntp.org, "If business, organization or human life depends on having correct time or can be harmed by it being wrong, you shouldn't 'just get it off the internet'." [http://www.pool.ntp.org/en/use.html, accessed Jan 15, 2016]

One problem with time synchronization is the variability of network conditions. Network load, variable paths, and firewall settings can impact time quality to the local system. To illustrate this effect we can use the time quality monitoring feature of Spectracom's VelaSync™ time server. It has a built-in GPS receiver as its reference that is accurate to tens of nanoseconds. NTP can be used to

compare it to another GPS time server on a local area network. The offset is around 15-20 microseconds (figure 1).

The VelaSync time server was then connected to some of the most popular internet time servers. The variation result, shown in figure 2, is as high as tens of milliseconds — 1,000 times worse than NTP across a local area network. If we assume all the time servers are accurate then difference is solely due to greater path delay and other dynamic conditions.

This variation is enough to question the traceability of time from the internet.

The Internet Obscures Time Traceability

Perhaps more important, for a security-critical network, you need to know the validity of the source used by the time server that distributes time to your network. Time from GPS signals is recognized as the most accurate, available and traceable time source. GPS-based time servers are easy and simple appliances to add to the local network. Even when different GPS time servers are deployed in different locations they will provide the same time regardless of geographies. What's more, GPS as a local time source can be monitored so its logs can be part of the audit trail.

Internet time servers may utilize GPS (or similarly accurate time sources) but you never know. To illustrate this point, we can use another feature of the VelaSync time server software, known as Time Map. The time map provides information available on the source of the time servers. See figure 3.

Of the seven internet time servers monitored over a 24 hour period, 20 different time sources were identified. Less than half of the sources could be identified as being directly from GPS. In one case, GPS time was distributed through 3 different time servers. The best practice of using NTP server pools is one reason why there are more sources than time servers. Server pools rotate among various internet time servers, each with their source of time, to reduce the chance of one bad or unavailable time server catastrophically affecting the synchronization. However, that is a problem for those requiring traceability. The source of time is not known or predetermined.

Conclusion

Indeterminate source identification, indeterminate accuracy variation, and the inability to log the resulting time synchronization calls to question the use of time from the internet. What's more, internet time servers are subject to being spoofed (bad NTP data sent from a faked IP address) and direct attacks including NTP poisoning, replay, and denial of service. So don't leave it to chance. When there is a business-critical need to trace time to an accurate source, the clear solution is GPS time server appliances deployed on the local network.

Spectracom offers several choices of high performance time servers to meet a variety of requirements and applications. Contact us to discuss which solution would be best for solving your requirements.

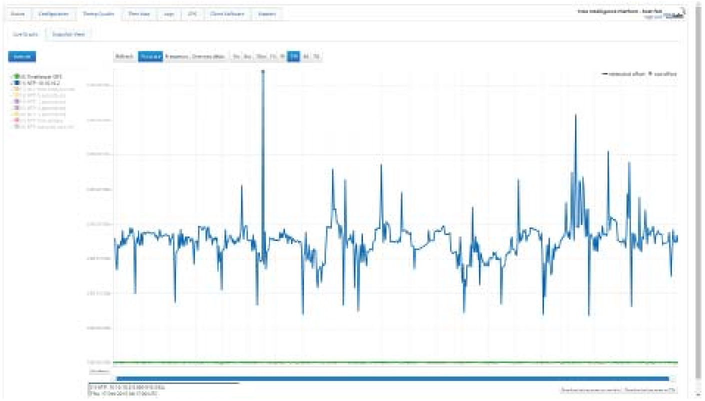

Figure 1: The comparison between two GPS time servers on the same LAN using NTP results in 15-20 microseconds offset.

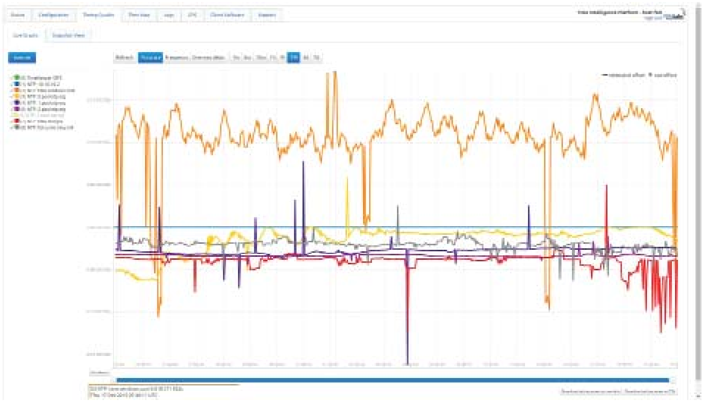

Figure 2: The comparison of internet time servers as measured by NTP on a local GPS time server. The scale is 1,000 times greater than figure 1.

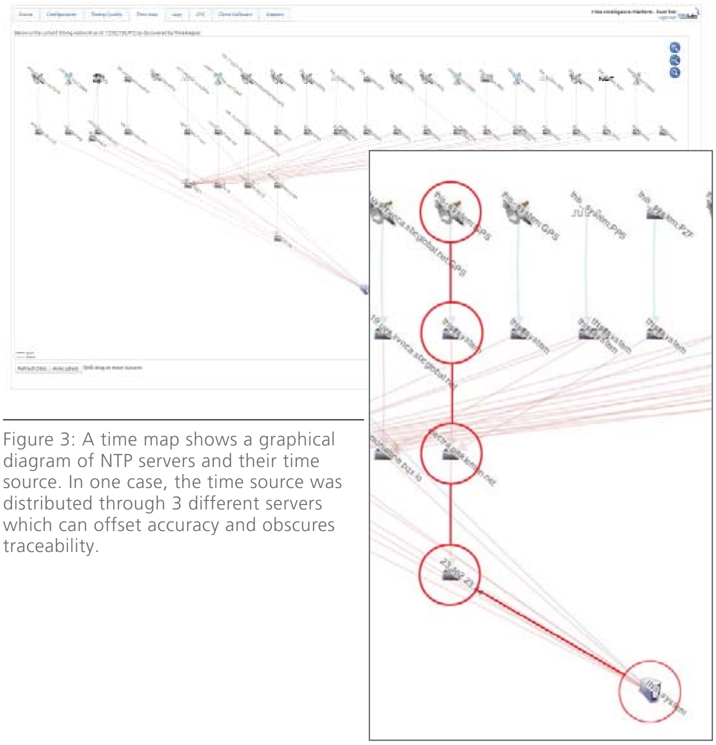

Figure 3: A time map shows a graphical diagram of NTP servers and their time source. In one case, the time source was distributed through 3 different servers which can offset accuracy and obscures traceability.