Tech Brief

The Traceability of Time Synchronization:

Why Internet Time Isn't Good Enough

By Jeremy Onyan
Director, Time Sensitive Networks

WHY INTERNET TIME IS BAD

- Time obtained from internet sources is highly variable
- Unknown time sources have no traceability
- Users are unable to correlate events across different locations
- There are security risks in having an open port to the outside for time synchronization

Time from GPS/GNSS-based time servers is far more accurate and secure, it is legally traceable and it significantly improves sync between locations

Executive Summary

In today's modern networking infrastructure, great care is taken to ensure that 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 that 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, which are necessary for any cyber forensics program. As such, synchronization is often a requirement for network security standards.

This document discusses the differences between a time source from within the network as compared to a time source from 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 that are based on extremely accurate atomic clocks, such as NIST or the US Naval Observatory, 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 path delays and firewall settings can impact time quality on the local system. To illustrate this effect, we can use the time quality monitoring feature of Orolia's SecureSync® 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).

We connected the SecureSync time server 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 the 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/GNSS signals is recognized as the most accurate, available and traceable time source. GPS/GNSS-based time servers are easy and simple appliances to add to the local network. Even when different GPS/GNSS time servers are deployed in different locations, they will provide the same time regardless of geography. What's more, GPS/GNSS as a local time source can be monitored, so its logs can become part of the audit trail.

Internet time servers may utilize GPS/GNSS (or similarly accurate time sources), but you never know. 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 coming directly from GPS/GNSS. In one case, GPS/GNSS time was distributed through three 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 own source of time, to reduce the chance of one bad or unavailable time server catastrophically affecting the synchronization. This is a problem if you require traceability. The source of time is not known, nor can it even be determined.

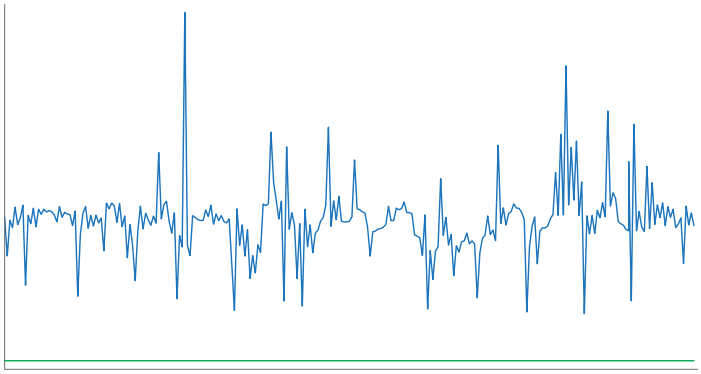

Figure 1: The comparison between two GPS time servers on the same LAN using NTP results in 15-20 microseconds offset.

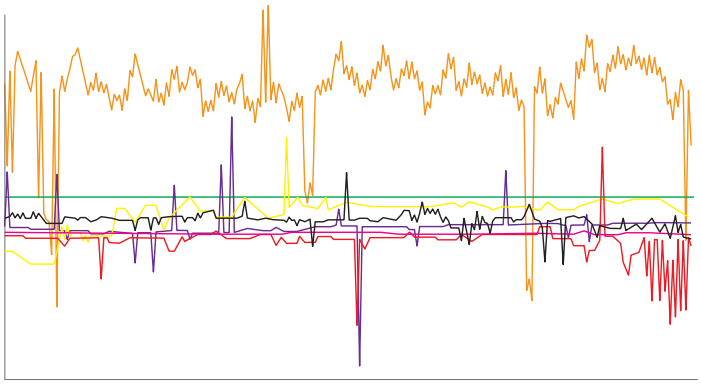

Figure 2: The comparison of internet time servers as measured by NTP on a local GPS time server. The scale is 1,000 times greater than figure 1.

Conclusion

Indeterminate source identification, indeterminate accuracy variation and the inability to log the resulting time synchronization calls into question the efficacy of getting time from the internet. Internet time servers are also subject to being spoofed (bad NTP data sent from a faked IP address) and to 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/GNSS-based time server appliances deployed on the local network.

Orolia 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 your requirements.

About the Author

Jeremy Onyan, Director of Time Sensitive Networks, holds a BS in Economics from the University at Buffalo. He has over 13 years of global sales and management experience. Onyan is recognized as an industry thought leader in timing for commercial applications.

About Orolia

Orolia is the world leader in Resilient Positioning, Navigation and Timing (PNT) solutions that improve the reliability, performance and safety of critical operations, even in GPS-denied environments. With locations in more than 100 countries, Orolia provides virtually failsafe GPS/GNSS and PNT solutions to support military and commercial applications worldwide.

Email: sales@orolia.com

Orolia USA, Inc.
1565 Jefferson Road Suite 460
Rochester, NY 14623 USA
Phone: +1 585 321 5800

France
Parc Technopolis, Bât. Sigma
3 Avenue du Canada
91974 Les Ulis, Cedex, France
Phone: +33 (0)1.64.53.39.80

Singapore
Plaza 8 @ Changi Business Park, Unit 03-08A
1 Changi Business Park Crescent
Singapore 486025
Phone: +65 8725.5543

www.orolia.com

28 March, 2019 - The Traceability of Time Synchronization (A)