spectracom

White Paper:

What Time is it? It's a Matter of Trust

Those in the business of measuring time are familiar with the saying, "If you have one clock, you know what time it is. If you have two, well…". Time synchronization is the ability for all clocks to have the same time. But what time is it? If your time synchronization deployment uses time from the internet, your organization may be at risk. Official time provided by a GPS-based network appliance is a time source that you can trust.

Introduction

The proliferation of electronic devices has resulted in three or four time-keeping devices within eyesight at any given time. But rarely do they agree. Which begs the question, "What time is it??" Since these electronic devices are really computers with network connectivity it should be easy to synchronize clocks. Mobile phones typically have the correct time since the telecommunications infrastructure has long been synchronized. Clocks in servers, workstations, routers, switches, and virtually any IP-enabled device can also be made to synchronize, so time-stamps, log files, database transactions, emails, security systems, and more, can be consistent and, hopefully accurate and correct.

If your organization is synchronizing its computer clocks, most likely your time is coming from an external time source, probably the internet. For many, the uncertainty of internet time is tolerable. But time-sensitive industries and applications require time that is trusted.

Can time from the internet be trusted when it really counts? An information security specialist for a large enterprise, found out as he was preparing for a legal deposition. His organization was involved in prosecuting a suspected intruder of their network assets. The organization had set up a system of computer clock synchronization using time from the internet. The security specialist was unable to verify or authenticate any of the time stamped evidence in his audit trails to be used against the intruder.

What is Time?

Time is unambiguous. Since the Treaty of the Meter of 1875, time has been defined and coordinated throughout the world. Official time is currently kept by extremely accurate atomic clocks at national metrology institutes. The result is Coordinated Universal Time (UTC) – the same time no matter where you are on the planet. (UTC replaced GMT as the worldwide time standard in 1972 as the Cesium atom replaced the solar day as the official time-keeping reference.)

Clocks in everyday use deviate from UTC and keep different times because they tradeoff accuracy for cost. It is simply impractical to build atomic clocks set to UTC into devices. Typically, consumer-grade clocks used in electronic devices lose one to ten seconds a day. That means time-stamps will be off an hour over a year assuming the clock was set correctly in the first place.

Being a few minutes or a few hours off from official time is a risk for applications such as IT security, and many others when seconds count. Instead of building more cost and complexity into computers, clock accuracy can be achieved through time synchronization. By synchronizing clocks to a trusted source of time, you do not need to worry about clock drift or manually re-setting time.

Network Time Protocol – Half the Answer

The Internet Engineering Task Force realized the need for a time synchronization standard for TCP/IP network devices many years ago. Network Time Protocol (NTP) was formalized in RFC 1305. Simple Network Time Protocol, SNTP, formalized in RFC 2030, uses a less complex client implementation. Client software for network time protocol is widely available for a variety of operating systems and is typically pre-installed in servers, workstations, firewalls and routers. Configuring an NTP or SNTP client is straightforward once you know who to synchronize to.

Why not internet time?

Sources of time are available on the internet. The main benefit is that they are free. But when factoring in the risks of internet time, it can come with a cost. There are six risk factors to using the internet as your source of time.

Internet connectivity – When your computer asks for the time will your internet service provider be able to connect you? In today's world if the internet is down your organization has bigger problems than time, but depending on synchronization schedules, one or two missed connections is enough for clocks to drift enough to effect applications.

Accuracy – The last study of internet time servers by MIT uncovered some surprising results. Of 957 stratum-1 time servers, the most accurate available for network use, "only 28% appeared to actually be useful". 638 were found to be based on free-running clocks and were not synchronized to an authority such as a national metrology institute. 391 were off by more than 10 seconds; one was off by 6 ½ years.

Availability – The MIT study concluded that time servers set-up by national authorities are the most popular and are "quite busy". If you use a government time server as your source of time, will it answer? Internet time servers can also be brought down by denial of service attacks. Sometimes these attacks come from a seemingly benign source. In 2003, a University of Wisconsin time server was out of commission for months after a programming bug in a consumer-grade router flooded it with requests. To help balance the load on internet time servers, there are terms that come with internet time servers. Rules of Engagement specify the requirements of internet time users. One rule is for smaller organizations to use lower accuracy time servers to help remove the burden on government servers. Are you prepared to live with these terms?

Firewall policy – Firewalling is the key to protecting the health and integrity of networks. IT security policies require blocking ports to eliminate risks. The use of internet time requires an open port that can be potentially exploited by hackers. For that reason, the US Department of Commerce recommends a firewall policy that blocks the internet time port in special publication NIST-800-41, *Guidelines on Firewalls and Firewall Policy*.

Authentication – Time packets received from a "trusted" source of time can easily be faked by a hacker. "Spoofing" data is a threat to the integrity of time from the internet. The US government through its national metrology institute (NIST), offers a statement on the authentication of time from its public time servers (http://tf.nist.gov/time/authentication.htm). Since no simple method exists to address the issues of authenticating and certifying time from internet time sources, they recommend alternative strategies.

Audit trails – When using the internet for time, no auditable records are available to prove the accuracy of time-sensitive data for compliance programs such as Sarbanes-Oxley, HIPAA and many others, or for legal disputes.

The GPS Time Server

The Global Positioning System (GPS) offers an alternative to internet time. GPS signals broadcast official time that is legally traceable anywhere on earth with outstanding accuracy. A device known as a GPS time server operates from within the network to ensure that time is available, accurate, and authentic. It supports security policies by eliminating open ports on the firewall.

Modern GPS time servers, such as the NetClock® from Spectracom, are secure and manageable network appliances. They provide audit trails for anything from tracking user configuration to satellite tracking logs. To prove the accuracy of time, simply compare the unit's logs with the operational status of each satellite as published by NIST (http://tf.nist.gov/service/gpstrace.htm). The result is a simple integrated timing solution that can be trusted.

Fig1. A GPS-based network appliance offers an exceptional return on investment

Conclusion

The use of a time source in a network synchronization deployment is a matter of trust. On one end of the trust spectrum, internet time servers offer an easy solution, but comes with risks relating to availability, accuracy, security, authentication, and auditing. Alternatively, a network appliance GPS time server offers secure, reliable, authentic, and manageable time from within the network. They are extremely simple to implement and easy to operate, but the real impact is unfailingly exact time deployed throughout your enterprise. The result is an outstanding return on a minimal investment to protect your organization.

	GPS	NetClock	Internet Time	Configured Server
Security	Government-backed	Built-in security	Open firewall	Configurable
Reliability	24 sats, 3-4 clocks per	12 sats, back-up options	Unknown, at risk	No back-up
Traceable / Auditable	Published data	Extensive logging	Unknown	Limited logging
Manageable	One-time antenna set-up	Network appliance	One-time set-up	Configurable

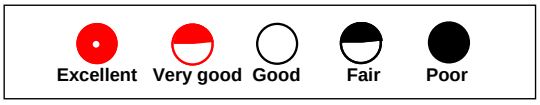

Fig2. The combination of a GPS time source and a NetClock® network appliance offers much higher value to a time synchronization deployment

USA | 1565 Jefferson Road, Suite 460 | Rochester, NY 14623 | +1.585.321.5800 | sales@spectracomcorp.com
FRANCE | 3 Avenue du Canada | 91974 Les Ulis, Cedex | +33 (0)1 64 53 39 80 | sales@spectracom.fr
UK | 6A Beechwood | Chineham Park | Basingstoke, Hants, RG24 8WA | +44 (0)1256 303630 | info@spectracom.co.uk

September 5, 2014 - WP01-101 (C)