spectracom

Time Synchronization for E-Commerce: PCI DSS Compliance

In a short period of time e-commerce has changed how we buy and sell all types of good and service, all around the world. It's estimated that in 2013, global e-commerce sales grew to over 1.3 trillion USD, with over 1 billion online shoppers. As these numbers continue to grow, so does the threat from hackers and cyber criminals who are constantly looking for ways to exploit systems to gain access to customer data. To help combat this threat, and ensure systems are protected against attacks, the major credit card vendors have established the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS certification is required for companies with credit card transaction volumes that exceed 50k per month for AMEX or 1M per month for Visa/MC/Discover. These companies must perform an annual audit which is required to confirm compliance. And for companies who don't meet these minimum transactions for which compliance is mandatory, in the event of a security breach, if they are not already PCI DSS certified then they must undergo a very costly and time consuming audit.

One aspect of PCI DSS compliance which is often overlooked, or poorly implemented, is time. Accurate time is essential for synchronizing critical systems and providing the ability to correlate events and logs with a high degree of certainty. Without accurate time, it becomes almost impossible to piece together the sequence of events of a breach, which is crucial for forensic analysis. This is especially true in distributed systems where datacenters and systems are becoming more and more disparate. However, time is also essential to security functions as well.

Time is used in various authentication protocols to help prevent replay attacks, where an attacker reuses an authentication token to maintain access to a system. SSL, for example, uses timestamps for certificate validation. Inaccurate time can cause the users to be unable to access a system since the server's certificate can appear to be expired or not yet useable. However, disabling the certificate check leaves servers vulnerable and could allow someone who has gained access to stay in the system indefinitely. This is also true in two-factor authentication such as Google Authenticator, RSA SecurID, and others.

In fact, time is such an important aspect to PCI DSS compliance that it is addressed as part of Requirement #10, *Track and Monitor All Access to Network Resources and Cardholder Data*.

> **10.4 Using time-synchronization technology**, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.
>
> 10.4.1 Critical systems have the correct and consistent time.
>
> 10.4.2 Time data is protected.
>
> 10.4.3 Time settings are received from industry-accepted time sources.
>
> https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf

While network time protocol (NTP) is a good example of time synchronization technology, requirements for correct and consistent time, time data protection, and industry-accepted time sources defines a PCI DSS-compliant deployment. Using free or public time sources is not good enough. These sources tend to be inaccurate, unreliable, and worst of all, impossible to prove. A better approach is to leverage a GPS-based NTP time server from within the cardholder data environment[1].

A Spectracom enterprise-class GPS NTP time server at each physical e-commerce data-handling facility ensures that you are in compliance with section 10.4 of the PCI DSS. Time derived from one of these sources is accurate, reliable, and legally traceable. And now, with the addition of the powerful new timing signal, STL, the ability to deploy timing has never been easier or more secure. STL is a timing reference which can be used to accurately synchronize network clocks using an easy to deploy indoor antenna. The STL signal is also encrypted making it highly secure. Contact us to learn how a GPS-based timing system ensures compliance to PCI DSS requirement 10.4 that is easy, inexpensive, and virtually maintenance-free.

[1]According to the Scope of PCI DSS Requirements, "The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. 'System components' include network devices, servers, computing devices, and applications. Examples of system components include Network Time Protocol (NTP)."

June 28, 2017 - PCI DSS (B)