Securing the Time in YOUR NETWORK

Ravi Shankar Rai
MD,
Savitri Telecom Services

The *Digital India* movement put India on the world map for the sheer magnitude and complexity of the initiative. It helped millions of Indians get access to the government services and helped bring transparency in the system. But such a huge initiative has its own set of challenges – primarily securing the infrastructure.

To put this to perspective, India had more than 6 million instances of web attacks in 2Q17. And this number is predicted to have increased by 17 percent in 3Q17 as per the domain name and internet security company Verisign. It was also found that most of the companies that came under some form of cyber-attack were targeted multiple times.

The most common form of attacks identified were denial of service (DoS) and DDoS (distributed denial of service) attacks. And though the simplest form of these attacks can be dealt with by rebooting the server, it still provides an opportunity of window for the perpetrator to exploit the vulnerabilities in the network.

One of the examples of the DDoS attacks includes the massive Botnet Attack which at its peak was sending 620Gbps of data to the target. The attackers used IP cameras and other unsecured online devices to connect to the internet, pummeling the site with requests in an attempt to bring it down.

There is a specific type of DDoS attack called NTP amplification, in which the attacker exploits publicly-accessible Network Time Protocol (NTP) servers to overwhelm the target with User Datagram Protocol (UDP) traffic. NTP is one of the oldest and widely used network protocols and is used by machines to synchronize their clocks.

Most networks get free time from the internet. *Pool.ntp.org* lists the free public servers which can be used to get free time. These servers are accessed by tens of millions of systems around the world but since these are primarily public servers, there is typically no monitoring of the health of these servers. Moreover, getting time from these servers requires a port to be open in the firewall leaving the entire network vulnerable to attacks.

Now, as we move toward the third platform of computing, primarily driven by millions of apps connecting billions of users and devices via datacenters distributed across the globe, the importance of timing and synchronization across these devices becomes more and more critical. Devices on the edge of the network (like IP cameras) are getting smart and can process a lot of information and only save the information that is important. Some of the industries like financial institutions and cards payments have already mandated time delay requirement across the networks to validate a transaction.

That raises the question, how do we ensure secure, accurate, and reliable timing across all these devices. The answer is a Stratum 1 Network Time Server like Microsemi's SyncServer S600 which sits inside the network firewall and gets the time directly from GPS satellites. The Microsemi SyncServer S600 is a purpose built, security hardened Network Time Server that delivers exact hardware-based NTP time stamps. The unparalleled accuracy and security is rounded out with outstanding ease-of use features for reliable network time services ready to meet user network and business operation needs today and in the future.

So, the real question then is, are you willing to risk your network for *Free Time* – what is the price that any organization is willing to pay for this *Free Time*. ●