The Global Leader in Resilient PNT

Tech Brief
Resiliency in PNT: Cybersecurity

John Fischer
Vice President of Advanced Research & Development, Orolia

Executive Summary

Cybersecurity is the watchword of the day, but what does it mean for Positioning, Navigation and Timing (PNT)? For many, the ability to hack or spoof a GPS/GNSS signal is a cybersecurity issue. At Orolia, we agree, which is why we have a wide array of products to augment, toughen and protect against GNSS vulnerabilities.

However, the other aspect is network connectivity. Any device that is on a network – which includes many PNT devices – must address cybersecurity.

This Orolia Tech Brief explores the basic steps for maintaining security using a network-connected time server and looks at different ways to achieve resiliency in PNT. As an example, we will start with our SecureSync® Time Server product line to demonstrate how to maintain security with this network-connected device.

The second part of this Tech Brief then gives some examples of how PNT information can enhance security.

Who Should Read This Tech Brief?

- Critical Infrastructure and Defense IT Security Providers
- CIOs
- Network Architects
- Network Engineers
- Program Managers
- System Integrators
- System Engineers

Part 1: Securing the Network

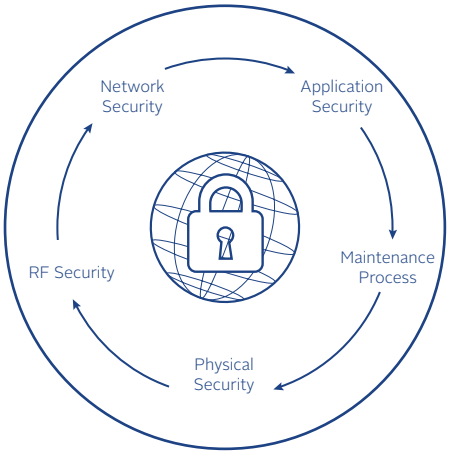
At Orolia, we begin by taking a layered approach to ensure that a time server provides all the required security features. In general, even though a time server is a server on the network, it doesn't face the same major concerns that most other types of servers have. A time server contains very little information that must be protected from hackers: there is no credit card information, personal privacy files, secret information, etc. In fact, the time it is serving out can be freely available to all.

That is not to say that there are no security issues.
The primary security issues for a time server are:

- It must not compromise the security of the rest of the network
- It must provide authenticated time information dependably

In our layered approach to security, we consider these five areas:

1. Physical Security
2. RF GNSS Security
3. Network Security
4. Application Security
5. Maintenance Process



Physical Security

Rather obviously, the easiest way to combat a Denial of Service (DoS) attack is to simply disconnect the equipment's power by turning it off or pressing a few buttons to disable operation. So, the first step in cybersecurity is always Physical Security – protecting the equipment from unauthorized or accidental manipulation. The basics include locking the doors of the server room and controlling access to it.

It is important to take Physical Security a step further by using equipment designed to be robust and protected from inadvertent defeat. For example, Orolia's SecureSync time servers offer fully independent, redundant power inputs (A and B side) so that customers can secure the power entry to ensure that a single power failure will not deny operation. Power input can be AC or DC from a battery backup system. In addition, SecureSync includes the ability to lock the front panel access controls, so that even personnel who have physical access to the rack cannot change settings unless authorized.

In the news recently were concerns about servers manufactured overseas having hidden "spyware" in them. This is becoming a growing concern, through either inadvertent or malicious means. Orolia's SecureSync time servers are manufactured in the USA through ISO 9001:2015 certified processes that guarantee that stringent manufacturing and quality controls are in place. Both the hardware and software components installed in our servers are strictly controlled and any updates are scrutinized before implementation.

SecureSync time servers are also approved by the Defense Information Systems Agency (DISA) for use in US Department of Defense networks. They are the first and only DoDIN approved product listed for timing and synchronization devices.

RF GNSS Security

Many industries consider jamming or spoofing of GNSS signals to be a cybersecurity issue. Orolia has taken extensive measures to protect, augment, and toughen GNSS signals using anti-jam antennas, interference and spoofing detection software (BroadShield), interference and spoofing mitigation technology (ThreatBlocker), atomic clock holdover oscillators, and other signals of opportunity such as STL, to supplement GNSS when it is unavailable.

Network Security

As a network device, Orolia's SecureSync time server provides the following security features:

- Access control lists (ACL) to limit network access to authorized users only.
- The ability to disable services and ports. This configuration is controlled at the Admin level to ensure that only those services and ports necessary for operation are enabled.
- User data is not stored on a time server – because time servers output precise time, vs. serving a file storage function (other than activity logs), there is no user data to be compromised.
- Iptables: Using these tables, customers can create their own set of security rules with source and destination IP addresses and/or port numbers. By using iptables, customers can add such alternative layers of security rules to prevent unauthorized and unwanted access to the system.

Resilient PNT Application Security

At the Application Layer, there are several other SecureSync time server security features:

- AAA – Authentication, Authorization and Accounting – Orolia's products adhere to AAA security practices. The following protocols are supported:
  - LDAP.
  - RADIUS authentication.
  - TACACS+ (Cisco).
- Multi-level authorization.
- Configurable, complex passwords that expire periodically and cannot be reused.
- HTTPS – No-clear text is the standard default setting, using signed certificates (SHA256 default) with configurable cipher usage and TLS v1.1 and v1.2.
- NTP – Symmetric keys and autokey. Orolia also serves on the standards setting committees for the creation of more robust protocols. The Internet Engineering Task Force (IETF) is organizing the creation of a new standard: Network Time Security (NTS) in which Orolia is involved in the formation.
- SSL, SSH, SCP, SFTP with public/private key support.
- Compliance with NIST standards for Personally Identifiable Information and Digital Identity Guidelines.

Maintenance Process

Cybersecurity is an evolving issue. New threats arise daily as bad actors find new ways to hack into systems. As new technologies and features are introduced, so are new vulnerabilities.

At Orolia, we constantly scan our networking products against CVEs (Common Vulnerabilities and Exposures), correcting weaknesses. We also scan our source code using the latest tools to detect weak coding practices that could open the code to attack. Our software engineers receive periodic training to ensure that best practices for security are followed in our code creation. Routine software updates are released that constantly toughen the products to attack. We make emergency releases in cases where a particularly pernicious vulnerability is discovered.

It is often said that Security is a Process, not a Product, and we believe in this philosophy. Only with constant vigilance and making security part of the maintenance process can true network security be assured.

Part 2: Using PNT to Improve Cybersecurity

Now that we've looked at how a network connected PNT device can support cybersecurity, let's look at how precision PNT features can improve cybersecurity. Consider these examples:

1. Passwords

Most secure systems require that passwords be changed periodically, such as every 90 or 180 days. The longer a password or key stays static, the longer a hacker has time to break it. Thus, the more often you change passwords, the more secure you will be. Imagine the increased security if you changed them every day, or even every second. Even if a hacker knew some of the passwords or keys, they would have to know when you were changing them and the sequence of use.

So now, besides having a shared secret between the user and the server, there is another dimension – that of time. Precise synchronization between the user and server offers the ability to reduce the static time interval for the use of a given key, thus enhancing security. For automated systems where a human is not involved, this interval can be reduced to milliseconds.

Precision time synchronization becomes an enabler to a whole new level of security.

2. Data speed

A second example is based on the concept that data can never travel faster than the speed of light.

(This statement may be undone when data communication via quantum entanglement becomes a reality, but until then, this is a practical limitation.)

Imagine that a user remotely logs into a classified server that is located in Virginia, claiming to be on the East Coast of the USA. A legitimate user within 1000 km of the server will have a roundtrip network delay time that is significantly less than that of a user halfway around the world. It is physically impossible for a distant user to fake a short network delay.

Of course, network congestion can increase delays, but nothing can reduce it beyond the physical limit imposed by the speed of light. Therefore, a server that can precisely measure roundtrip delay to its users can provide added security.

For secure applications, it is not unreasonable to require a high bandwidth connection, especially for critical systems, which eliminates the ambiguity in response time caused by congestion. Moreover, the variable packet delay possible in any network can be measured and compensated for.

Man-in-the-middle attacks and replay attacks add delay to response time, so placing limits on acceptable response delays, both minimum and maximum, based on known geographic parameters can improve security.

3. Geolocation authentication

Today, we typically have three types of authentication – ways to prove you are who you claim to be:

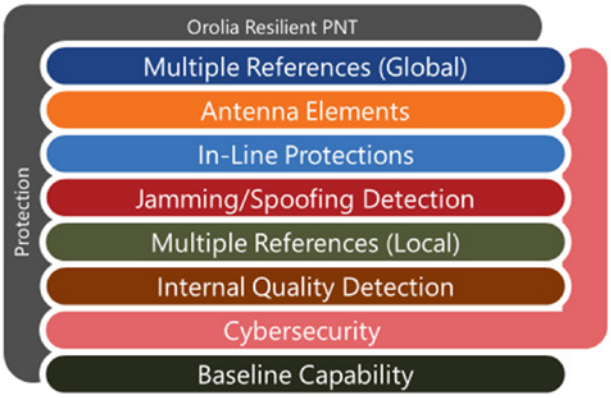
- Something you know – a shared secret between the server and the user, such as a password
- Something you have – a physical key, such as a wireless fob
- Something you are – a fingerprint, retinal scan or facial recognition

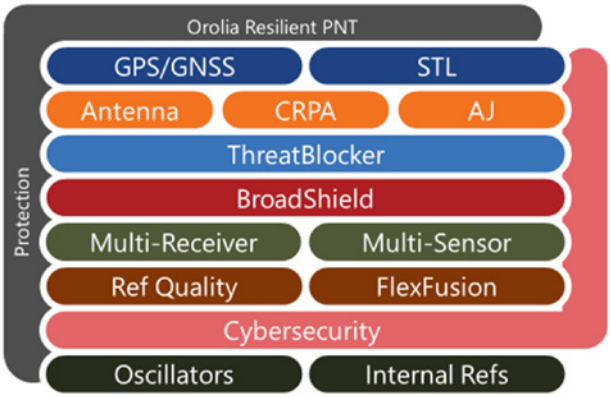
Now let's imagine a fourth factor – your location. Suppose you could provide irrefutable evidence that you are in a given location at a given time. The new STL signal – Satellite Time and Location – provides just such a service. It transmits an encrypted token from low-earth orbiting satellites that can be received only within a focused beam area on earth. Reception of just one packet locates you to within a few hundred kilometers, but since the satellites are fast moving, successive receptions over a few minutes locates you more accurately, down to within 100 meters.

Reception of these encrypted packets requires a paid subscription to decode, but it ensures they are secure. And this method is not susceptible to a replay attack because the packets are time-stamped to the microsecond level, referenced to universal coordinated time.

Now that we have an irrefutable way to prove location, how could we use it? Consider this example: The only way I could log into a specific server is by being physically on the premises, or within the gates of another secure facility somewhere in the world. Now, STL becomes another very powerful protection measure. It allows you to completely bypass the case where a bad actor can access your server from an unauthenticated location.

Solution Capabilities





Conclusion

As rapidly as network cybersecurity continues to evolve, so too do the malicious intents of bad actors. Jamming and spoofing are on the rise, making it critically important to protect your network against those types of attacks. Odds are that you have been jammed without even knowing it. And that is just one type of security: GNSS security. You also need to consider network security, because almost every device is on the network in this age of the Internet of Things (IoT). This includes the domains of physical security, network security, application security, and maintenance processes. It quickly becomes apparent how critical the need for a secure time server becomes.

Precision PNT features can improve cybersecurity, and network architects would be well served by adapting some of the technologies that are advancing the state of PNT today. Password security, data speed, and geolocation authentication are emerging as key technologies to help protect the security of your network. Augmentation signals such as STL can also play a significant part in providing backup in the event of a GNSS attack, as well as providing geolocation authentication.

About the Author

John Fischer has worked with global navigation satellite systems (GNSS), wireless, positioning navigation and timing (PNT) and specialized systems for more than 15 years. Prior to joining Orolia, he specialized in wireless telecom as a founding member of two startups: Aria Wireless in 1990 and Clearwire Technologies in 1997. At Clearwire, he served as chief technology officer, creating wireless broadband equipment for Internet connectivity. Early in his career, John worked as a systems engineer in radar, EW and command and control systems. He graduated with master's and bachelor's degrees in electrical engineering and computing engineering from the State University of New York at Buffalo.

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

France
Parc Technopolis, Bât. Gamma
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
Changi Business Park
Singapore 486025
Phone: +65 8725.5543

www.orolia.com
sales@orolia.com

22 February, 2019 - Resiliency in PNT: Cybersecurity (A)
Specifications subject to change or improvement without notice.