Booz | Allen | Hamilton

UNDERSTANDING AND MITIGATING THE IMPACT OF SYNCHRONIZATION DISRUPTIONS

WORKSHOP FOR SYNCHRONIZATION AND TIMING SYSTEMS

KEVIN COGGINS
VICE PRESIDENT FOR RESILIENT PNT

JUNE 21, 2018

PNT AS A CRITICAL ENABLER

- PNT is a critical enabler to most DoD weapons systems – from simple radios, to intelligence systems, to cruise missiles.
- These different weapons systems operate as a system of systems – few are effective in isolation.
- In the Department of Defense, there are hundreds of systems that are synchronized via GPS and USNO time.
- With these systems working together, synchronized to the same PNT reference frame, we can achieve tremendous advantage over our adversaries.
- In the recent strike on Syria, countless systems were involved in enabling a synchronized strike from numerous directions to evade air defenses and converge on the targets simultaneously.

PNT has been a critical enabler of modern warfare since the wide-scale adoption of GPS.

PNT AS A CRITICAL ENABLER

- PNT information enables the infrastructure that drives our modern society.
- The stability of our modern society depends on PNT information.

- Continued technological advancement requires more accurate and reliable PNT

Government and Commercial Infrastructure is Highly Dependent upon PNT Information

PNT AS A CRITICAL VULNERABILITY

- Clausewitz, a German military strategist, stressed the need to identify the enemy’s “center of gravity”, and trace it back to a single source – as this was the means to ensure defeat of the adversary.
- The ”center of gravity” of our PNT capability is GPS.
- DoD Adoption of GPS has been:
  - Ubiquitous across most systems
  - Without provision for timely updates
  - Without an architecture that facilitates ease of upgrade
  - Blind to the details of the signal and the system
  - Without resilience

A typical GPS receiver is a special-purpose processor with a one-way (unprotected) data link into the host system

IMPLICATIONS FOR CIVIL USERS

1. **Adoption of GPS in Civil Users is similar to DoD in most cases**
   - Ubiquitous – GPS is universally employed
   - Blind trust – GPS is inherently trusted
   - Static – GPS systems are usually never patched
   - Without resilience – GPS-only solution – single point of failure
   - Without situational awareness – no knowledge of threats in real-time
   - Without system understanding – limited knowledge of how the system consumes, processes and propagates PNT data
2. **Threat Techniques and Systems are Readily Available**
   - Techniques are published and widely known
   - Inexpensive and effective threat systems are available
3. **Questions for U.S. Civil Users are the Same**
   - What do our systems really need?
   - How to architect our systems and affordably enable PNT resilience?
   - How to prioritize actions and allocate limited resources?
   - How to update older systems?
   - How to get organizations and people to do what is necessary?

Hostile Control of Ships via False GPS Signals: Demonstration and Detection

UNDERSTANDING RISK

Risk = *Function* (Likelihood, Consequence)

- ***Likelihood*** Is The Probability That An Event Might Occur
  - If ***Intentional Stimulus*** – You Have To Consider ***Intent***, ***Capability*** And ***Opportunity***.
  - If ***Unintentional***, You Should Consider Quality Of System Design, Performance Data, And What Phenomena Might Stimulate An Unintentional Disruption
  - **What Can You Do About Likelihood?**

- ***Consequence*** Is The Impact If The Event Occurs
  - "***Consequence***" Is Analogous To "***Impact***", And Can Range From ***Acceptable Impacts*** To ***Unacceptable Impacts***.
  - This Can Range From ***Customer Dissatisfaction*** To ***Business Failure***
  - **What Can You Do About Consequence?**

SAMPLE RISK STATEMENTS

BEFORE

GIVEN my system design which has a **single source of time**,
IF that single source fails and cannot be recovered in a relevant timely manner,
THEN my system will **fail and impact clients and revenue**.

AFTER

GIVEN my system design with **two independent timing sources**,
IF a single source fails and cannot be recovered in a relevant timely manner,
THEN my system will **continue to operate using the second source of time**.

SAMPLE RISK STATEMENTS

BEFORE

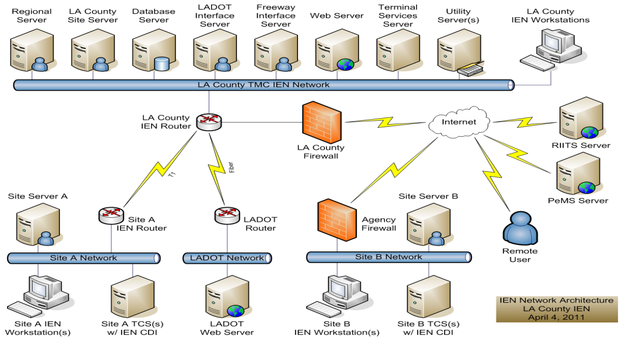
GIVEN my system design that **inherently trusts the GPS received signal**,
IF my system consumes a false GPS signal and the resulting solution is propagated throughout my network,
THEN **my system and dependent systems could fail resulting in financial impact**.

AFTER

GIVEN my system design has a ***GPS firewall***,
IF my system consumes a false GPS signal,
THEN my system will **continue to operate using the protections of the GPS firewall**.

PROACTIVE STEPS

Understand your System



DHS Best Practices

U.S. DEPARTMENT OF HOMELAND SECURITY

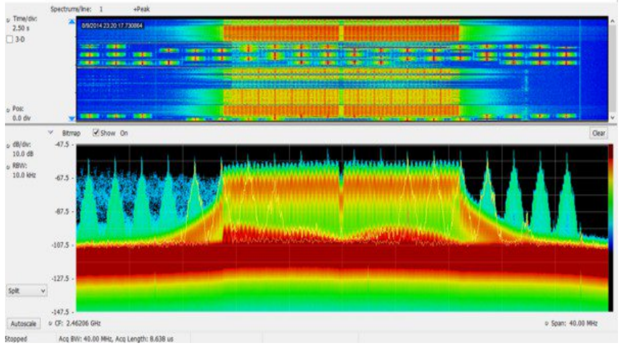
Homeland Security

Conduct Pen Testing

Add Resiliency

Deploy a GPS Firewall

Monitor



Spectrums/line: 1 +Peak
Time/div: 2.50 s
□ 3-D
8/9/2014 23:20 17.730864
Pos: 0.0 div
Bitmap ☑ Show On
Clear
dB/div: 10.0 dB
RBW: 10.0 kHz
Split
Autoscale
CF: 2.46206 GHz
Span: 40.00 MHz
Stopped
Acq BW: 40.00 MHz, Acq Length: 8.638 us

THANK YOU!

Kevin Coggins

Vice President for Resilient PNT

Coggins_kevin@bah.com