Timing Security: Mitigating Threats in a Changing Landscape Webinar

Panelists:

Barry Dropping, Senior Director, Product Line Management, Microsemi
Kevin Coggins, VP for Positioning, Navigation and Timing, Booz Allen Hamilton
James Platt, Director, Position, Navigation and Timing Office, DHS

Moderator:

Marc Weiss, Consultant, Spirent

May 22, 2018

Advancing ICT Industry Transformation

Introduction to ATIS Webinar on Timing Security

Marc Weiss
Consultant
Spirent

This webinar is presented in cooperation with WSTS.

Timing security is a complex topic.

While this webinar may serve as a good introduction or update to timing security, interested attendees can hear more in-depth information on this and many other topics at the upcoming WSTS event.

To view the complete agenda, visit www.atis.org/wsts

Outline

- Introduction, Marc Weiss, Consultant for Spirent
- Needs for Timing in Telecom, Electric Power and Finance

  Barry Dropping, Microsemi
- Reasons for Increasing Timing Security

  Kevin Coggins, Booz Allen Hamilton
- Options for Mitigating Timing Issues

  James Platt, Department of Homeland Security
- Conclusions
- Questions

Barry Dropping
Senior Director
Product Management
Microsemi

Use of GPS for Timing in Critical Infrastructure/Key Resource Sectors in U.S.


Chemical


Commercial Facilities


Communications


Critical Manufacturing


Dams


Defense Industrial Base


Emergency Services


Energy

Of the 16 Critical Infrastructure / Key Resource sectors in the U.S., 15 use GPS for **timing**.

GPS **timing** is deemed **essential** for 13 of the sectors.

[Source: U.S. DHS]

Financial Services 

Food and Agriculture 

Government Facilities 

Healthcare 

Information Technology 

Nuclear Systems 

Transportation Systems 

Water Systems 

Sample of GPS Based Timing Requirements

Industry	Synchronization Requirement	Accuracy Needed
Communications (Fixed and Wireless)	All communications systems require Primary Reference Clock (PRC) traceability. Advanced wireless systems require precise Time and Phase Alignment.	Frequency 1 x 10-11 Time: 100ns source 1.5us application
Financial	MiFID II Financial Trading Requirements for high speed electronic trading.	Time: 100us to UTC
Power Grid	Synchrophasors must be time traceable to the microsecond level to phase align the power grid.	Time: 1us
Emergency Services – E911	911 calls placed on cellular phones in North America commonly use triangulation techniques based on accurate timing to locate the caller.	Time: 100ns

The Impact of Poor Synchronization in LTE Wireless Networks

Macro LTE	Function Enabled	Impact of Poor Synchronization
FDD	Frame alignment	Dropped calls, Interference Packet loss, Inefficiency
TDD	Time slot alignment	
LTE-A		
eMBMS	Distribution of high quality video	Video hanging, pixilation, voice/video mismatch
MBSFN	Separation downlink/uplink transmission	Packet collision, degradation in overall link and connection quality
MIMO	Coordination of signals to/from multiple antenna	Poor signal quality at edge of cells, LBS accuracy, service degradation
COMP	Coordination of signals to/from multiple eNB	Spectral inefficiency & general degradation of services
eICIC	Interference coordination	Interference , echo, packet loss, application hang

Kevin Coggins
Vice President for PNT
Booz Allen Hamilton

Innovation center, Washington, D.C.

PNT Threats and Implications for Critical Infrastructure

TIMING SECURITY: MITIGATING THREATS IN A CHANGING LANDSCAPE

Kevin Coggins
Vice President for Resilient PNT

MAY 22, 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.
- Continued technological advancement requires PNT.



- The stability of our modern society depends on PNT information.




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 CRITICAL INFRASTRUCTURE

1. **Adoption of GPS in Critical Infrastructure 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. Critical Infrastructure 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

JAHSHAN BHATTI and TODD E. HUMPHREYS
The University of Texas at Austin, Austin Texas

Received August 2015; Revised August 2016

ABSTRACT: *An attacker's ability to control a maritime surface vessel by broadcasting counterfeit civil Global Positioning System (GPS) signals is analyzed and demonstrated. The aim of this work is to explore civil maritime transportation's vulnerability to deceptive GPS signals and to develop a detection technique that is compatible with sensors commonly available on modern ships. It is shown that despite access to a variety of high-quality navigation and surveillance sensors, modern maritime navigation depends crucially on satellite navigation and that a deception attack can be disguised as the effects of slowly-changing ocean currents. An innovations-based detection framework that optimally chooses the measurement sampling interval to minimize the probability of a ship exceeding its alert limits without detection is developed and analyzed. A field experiment confirms the vulnerability analysis by demonstrating hostile control of a 65-m yacht in the Mediterranean Sea.* Copyright © 2017 Institute of Navigation.

INTRODUCTION

Surface vessels, from fishing boats to container ships to deep-water oil rigs, depend crucially on Global Positioning System (GPS) signals for navigation, station keeping, and surveillance [1–4]. GPS, its ground and satellite-based augmentation systems, and other Global Navigation Satellite Systems (GNSS) are used as a primary maritime position-fixing system. They are an important maritime navigation aid even for vessels actively piloted by human operators, except in familiar littoral waters such as port entry and within natural or man-made channels where conventional optical navigation is used. Moreover, as surface craft become more autonomous, the trend is toward increased reliance on GNSS: current autopilot systems, dynamic-positioning systems, and fully unmanned surface vehicles are designed under the assumption that GNSS signals are usually available and trustworthy [2, 3, 5, 6]. Even autonomous underwater vehicles typically depend indirectly, or periodically, on GNSS [7].

Given the fragility of GNSS signals under conditions of signal blockage or jamming, and given that the signals do not penetrate underwater, there is interest in developing GNSS-independent maritime navigation and control systems [2, 8]. Terrain-relative navigation has been successfully employed in autonomous submersibles [8], and could serve as a backup to GNSS for surface vessels. This technique has historically required high-resolution (e.g., m-level) underwater terrain maps, which are available for only a tiny fraction of the seafloor, but recent results indicate that coarser (e.g., 20-m-resolution) ship-based bathymetry maps may be adequate for 10-meter-level positioning, provided sufficient terrain variability [9]. Nonetheless, for the present, terrain-relative navigation does not even appear to be an active research topic for civil surface maritime transportation. What is more, the only widespread radionavigation backup to GNSS, Loran-C, was abandoned by the U.S. Coast Guard in 2010 [10], and there are no official U.S. plans for a successor, despite continued lobbying for deployment of its upgrade, eLoran, which is available in other parts of the world [11]. Consequently, one can expect most maritime navigation systems to rely primarily on GNSS for position-fixing for years to come.

By standard practice marine craft are equipped with redundant GNSS units so that one serves as backup if the other experiences a fault. And for extremely critical applications, an entirely GNSS-free positioning system may be available, such as the acoustic positioning system required as a backup to GNSS on dynamically-positioned deepwater drilling vessels [3]. But these fail-safe systems are designed to handle obvious faults or GNSS outages caused by signal blockage or ionospheric effects. They are likely to fail when confronted with a sophisticated and deliberate attacker: outlaws are different from outliers; fraud is different from faults.

EXPLOITATIONS AND MITIGATIONS

Attributes	Definition	Sample Exploitations	Sample Mitigations
Access	Ability to ensure a sufficient level of access to PNT information	Jamming Spoofing System Attack	Improved Receivers Anti-Jam Antenna System Diversity
Integrity	Ability to ensure a sufficient level of trust in PNT information	Spoofing System Attack	Improved Receivers Situational Awareness System Diversity
Affordability	Ability to afford the procurement, operations and maintenance of a capability (enabled by PNT)	Any of the above, to a point that drives the system to require an upgrade	Open-architecture System Diversity

Effective mitigation requires an understanding of the client system and how it consumes PNT information.

THANK YOU!

Kevin Coggins

Vice President for Resilient PNT

Coggins_kevin@bah.com

Jim Platt
Director
PNT Office
Department of Homeland Security

The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Department of Homeland Security Assessing Secure and Resilient Time

Timing Security: Mitigating Threats in a Changing Landscape Webinar

May 22, 2018

Homeland Security

Outline

- DHS Role in Critical Infrastructure
- Timing in Critical Infrastructure
- Managing Risk
  - Holistic view of risk management
  - National Infrastructure Protection Plan (NIPP)
  - National Mitigation Framework
- Notional PNT architecture (FRP)
- Way ahead

DHS is the Federal Coordinator for U.S. Critical Infrastructure

- Leads the national effort to mitigate risks to, strengthen the security of, and enhance, the all-hazard resilience of critical infrastructure.
- Partners across the critical infrastructure domain, leads related preparedness activities, and serves as an information-sharing conduit between the private sector and public entities.

Security: *Reducing the risk to physical and cyber critical infrastructure caused by natural and manmade threats.*

Resilience: *The ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions.*

Homeland Security

IP is the Federal Coordinator for U.S. Critical Infrastructure

Critical infrastructure: the systems, assets, and networks that maintain our way of life. It is diverse and complex, includes varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both physical and cyber space, and governance constructs that involve multi-level authorities, responsibilities, and regulations.

Courtesy of DHS

Critical Infrastructure Defined: "Assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."

IP is the Federal Coordinator for U.S. Critical Infrastructure

Critical infrastructure: the systems, assets, and networks that maintain our way of life. It is diverse and complex, includes varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both physical and cyber space, and governance constructs that involve multi-level authorities, responsibilities, and regulations.

Time/UTC

Do you need UTC? If yes, how do you get it? How do you operate without it?

Strategies for Managing PNT Risk

Courtesy of DHS

- Employing an integrated approach to address diverse and evolving risks
- Understanding vulnerabilities to manage GPS risks
- Educating Partners and Changing Perspectives (*e.g.*, GPS as a computer, not a radio)
- Exploring new technologies
- Keeping National Policies Relevant

Strengthening Critical Infrastructure Security and Resilience Requires Engagement with a Broad/Diverse Community of Partners

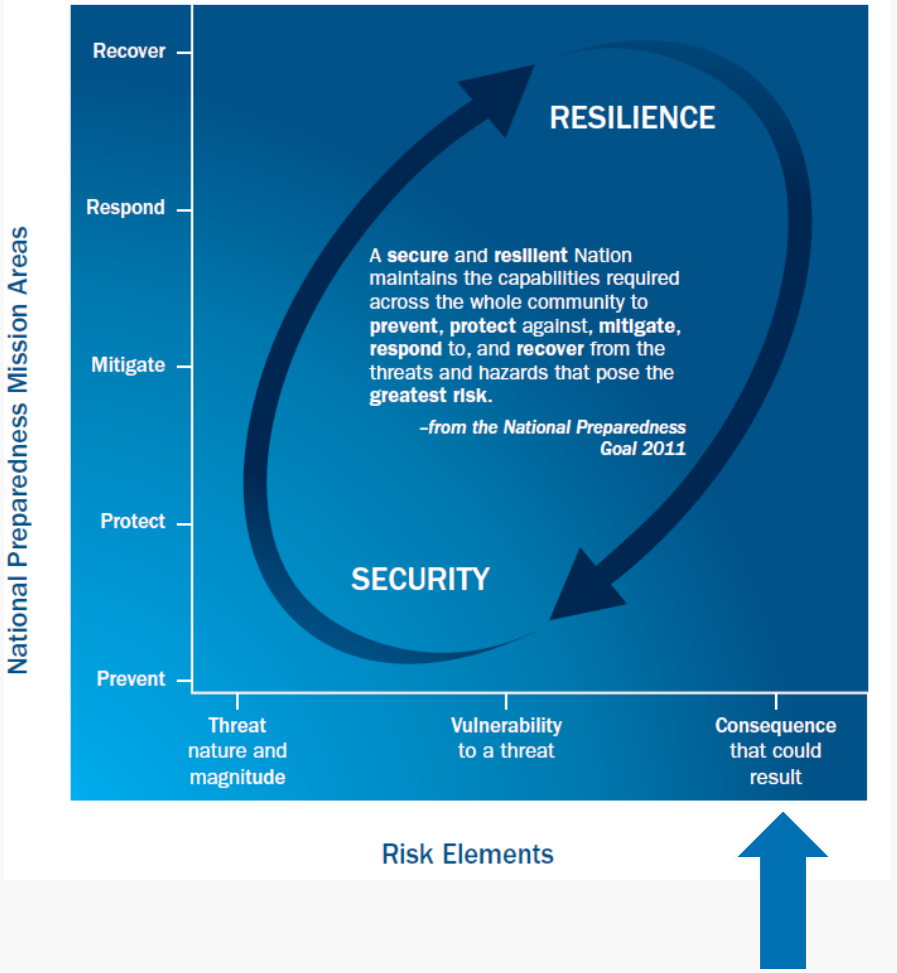
- Engaging in collaborative processes
- Applying individual expertise
- Bringing resources to bear
- Building the collective effort
- Enhancing overall effectiveness (not just timing)

Homeland Security

National Infrastructure Protection Plan Mitigating Consequences

- Information sharing
- Restore Critical Infrastructure, especially lifeline sectors
- Ensure that redundant processes are implemented for key functions, reducing the potential consequences
- Remove key operational functions from the Internet-connected business network
- Repair or replace damaged infrastructure with cost-effective designs that are more secure and resilient
- Utilize and ensure the reliability of emergency communications capabilities.

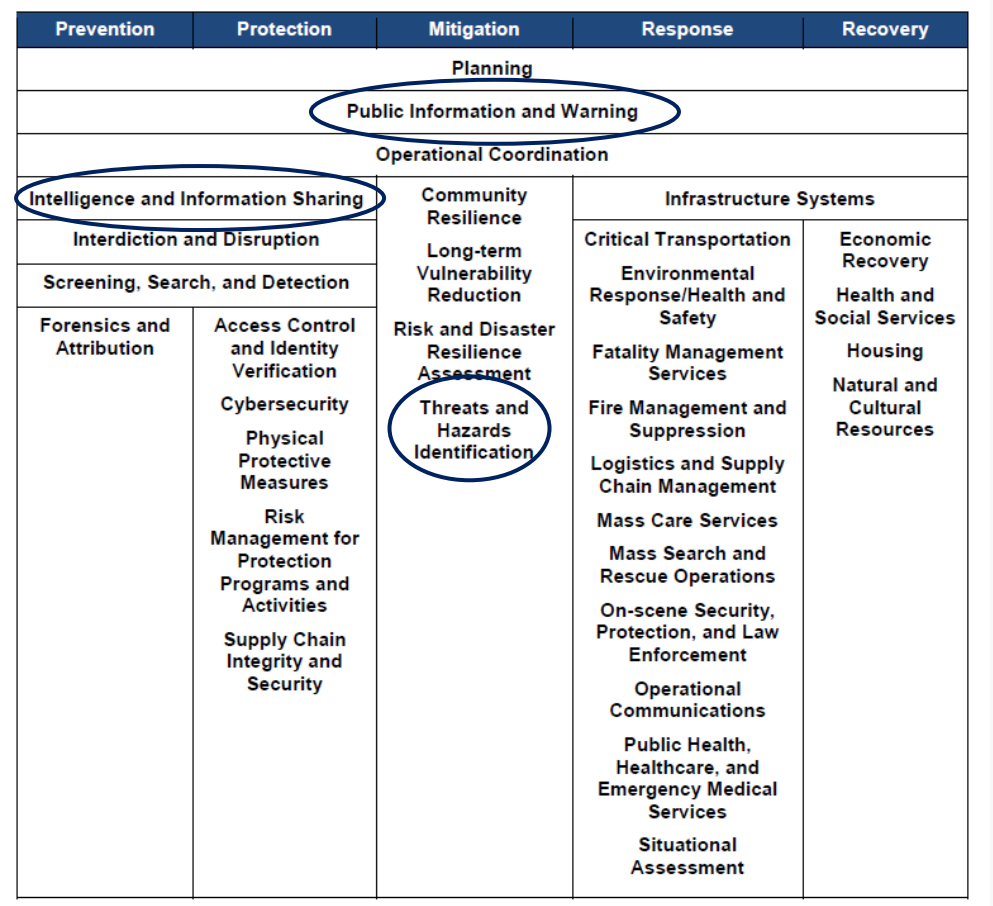
Figure 4 – Critical Infrastructure Risk in the Context of National Preparedness



The National Mitigation Framework

PNT Mitigation

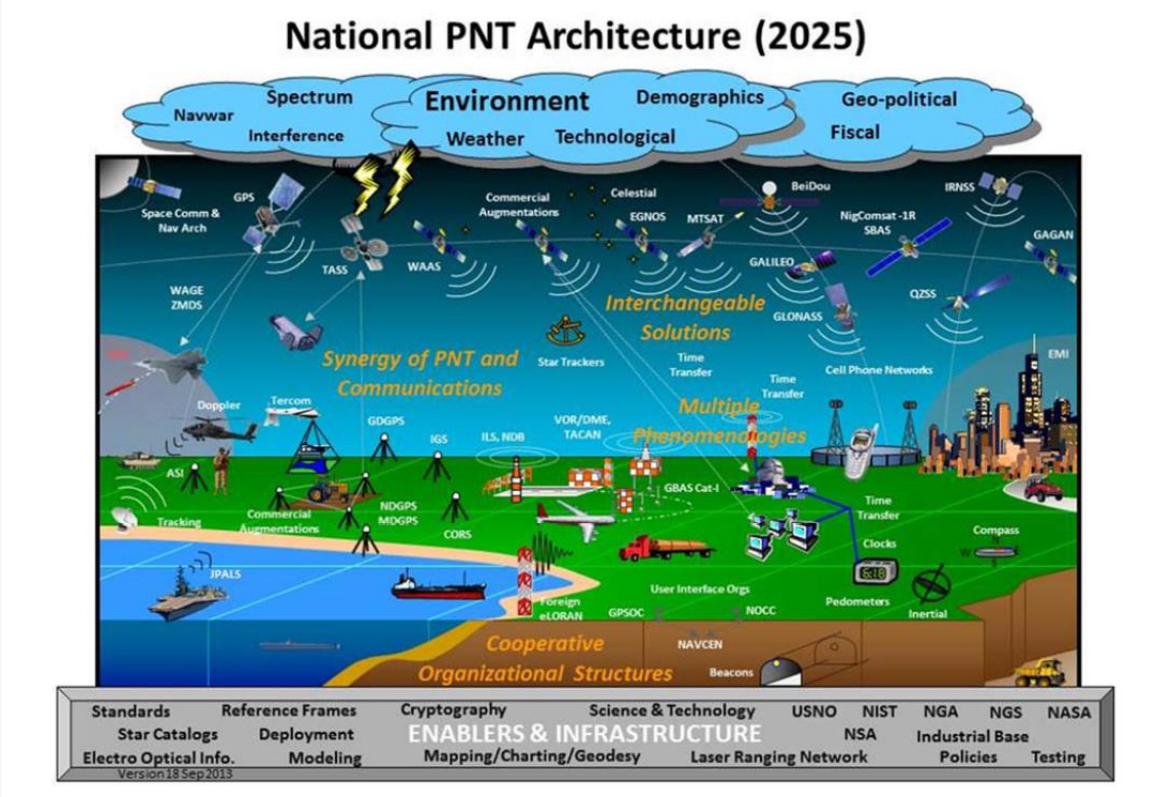
- Focus has been on Prevention and Protection
- Mitigation Efforts less energetic – more difficult
- How do we respond and recover?
- Do we understand where we fit in community efforts?
- When should we start thinking about mitigation (Hint: Design Phase)



Federal Radionavigation Plan

PNT Architecture

- Multiple Phenomenologies
- Not centrally funded
- Industry filling gaps
- Assessing alternative federal systems



Do you have a strategy to identify timing needs and select the appropriate timing sources?

Looking Forward

- Validation of Critical Infrastructure PNT requirements
- Analysis of PNT systems to fulfill NSPD-39 requirements
- Competent PNT framework
- Fiscal Year 18 PNT Demonstration
- Normalization of PNT in risk management decisions
- Secure and Resilient Infrastructure

Homeland Security

For more information, visit:
www.dhs.gov/critical-infrastructure

James Platt
James.Platt@hq.dhs.gov
Mike Striffolino
Michael.Striffolino@hq.dhs.gov

Conclusions

- Needs for Timing in Telecom, Electric Power and Finance

  Barry Dropping, Microsemi
- Reasons for Increasing Timing Security

  Kevin Coggins, Booz Allen Hamilton
- Options for Mitigating Timing Issues

  James Platt, Department of Homeland Security

Questions and Discussion


WORKSHOP ON
SYNCHRONIZATION
AND TIMING SYSTEMS
JUNE 18-21, 2018
SAN JOSE, CA
TIME MATTERS ...
TODAY AND TOMORROW
atis
www.atis.org/wsts


NIST
Assured Access to Accurate Time Workshop
A Comprehensive View of Timing Solutions and Interoperability Issues
www.atis.org/assured-access
11:59
11:59
June 22, 2018 | San Jose, CA

Thank you for attending the
Timing Security: Mitigating Threats in a Changing Landscape Webinar

All registered attendees will receive a follow up email containing links to a recording and the slides from this presentation.

Learn more about GPS vulnerabilities and synchronization issues at WSTS 2018
www.atis.org/wsts