Module 7: GPS and AIS: Operation, Jamming, Spoofing, and Manipulation
Objectives of this Module

• To provide an understanding of the operation of GPS and AIS systems

• To understand the jamming, spoofing, and manipulation vulnerabilities of GPS and AIS

• To describe recent incidents of GPS and AIS spoofing in the maritime domain, and current threats

• To understand the vulnerability and implications of Critical Infrastructure OT to a disruption of GPS, especially the GPS timing information
Global Network Satellite System (GNSS)

There are six GNSS in the world, one of which is GPS. Although they use different numbers of satellites, orbits, and different frequencies, some are compatible and can be shared by the receiver for better accuracy and reliability (except if they are encrypted).

- The GNSS systems are:
  - GPS (United States)
  - GLONASS (Russia)
  - Galileo (Europe)
  - BeiDou (China)
  - QZSS (Japan)
  - NavIC (India)

- GPS uses 24 satellites and 6 orbits (4 per orbit) arranged so that 8 satellites are visible from most points on earth. GLONASS uses 24 in three orbits (8 per orbit) arranged for better resolution in the northern hemisphere.
Satellite Orbits and Applications

• There are many types of satellite orbits, and each have different applications

• Satellite orbits are characterized by their altitude and the plane in which they revolve around the earth

• Some characterizations are
  – GEO - Geostationary Earth Orbit: Telecomm, 22,000mi
  – MEO - Mid Earth Orbit: GPS, Inclined plane, 13,000 mi
  – LEO - Low Earth Orbit: Earth observation and spy, 100 – 1000 mi
Global Positioning System (GPS)

- 6 Orbital planes
- 8 Satellites visible
- 4 necessary for accurate three-dimensional positioning
GPS Satellite Signal Basics

• GPS satellites transmit radio signals at 1-2 Ghz, to receivers; these signals contain highly **accurate timing information**
  - It is used to calculate receiver position by measuring the travel time of signals between the satellite and receiver, by comparing the satellite transmitted time to local receiver time
  - GPS timing is also used in critical infrastructure such as the electrical grid.
    - Hence GPS is vital to the operation of Critical Infrastructure

• The GPS satellite transmission also includes a **Pseudo Random Code (PRC)** which identifies which of the satellites the transmission is coming from.

• GPS satellites periodically transmit their orbital data known as the **ephemeris**
  - Used by receivers to calculate the accurate position of satellites
GPS receivers **select strongest signals** and reject others, including **multipoint interference** due reflections from buildings, water surface, waves, as well as signals from other GPS satellites.

**Spoofing Note:** If a Man-in-the-Middle can:
- capture the received signal on their receiver,
- then alter the time stamp or ephemeris (or just delay and replay it)
- and transmit the result to the victim receiver, the victim’s receiver will calculate an incorrect position.

Reflections result in multiple signals reaching the receiver from the same satellite. Called multipoint interference.
GPS Satellite Signal Basics (3)

- GPS satellites, contain **atomic clocks** that keep, and transmit, very precise time
- GPS receivers contain much less expensive clocks because
  - There are on the order of 30 satellite transmitters
  - But millions of receivers
  - The inexpensive clocks go into the millions of GPS receivers (cell phones, cars, boats, watches...)
- **Spoofing Note:** It’s impractical (or practically impossible), to fix all the receivers to mitigate against spoofing
Pseudo Random Numbers (PRN)

- All the GPS satellites transmit signals over the same frequencies
- Each Satellite is assigned a unique code which identifies it, called a PRN
- These PRNs are used by the receiver to capture the signal and lock onto it

Spoofing Note:
- Military GPS PRNs are much longer than civilian apps, may be encrypted, and are much harder to spoof
- To spoof the GPS receiver, the spoofer must break the lock and substitute their own signal for the receiver to lock onto.
The receiver measures the time delay of its received signal from each satellite.

The receiver calculates its distance from multiple satellites.

Usually, four signals are used, of eight possible
The Automatic Identification System (AIS)

Applications:
• Traffic Management and Collision Avoidance
• Complements radio, radar, CCTV, etc.
• Provides information about ship and cargo to authorities
• Can keep track of whether vessels are where they should be
• AIS receives position data from GPS
• AIS transmits the above info by terrestrial radio when close to shore, or by AIS satellite when at sea.
Spoofing Note:

• AIS receives vessel position information from GPS. If GPS information is spoofed, the AIS reports vessel position incorrectly.

• By falsifying their own GPS in their AIS transmissions, a ship can avoid detection and engage in illegal activities:
  – Illegal fishing
  – Stealing Ukraine grain
  – Violating oil/trade embargoes
Case Study: Intentional AIS Falsification


A Cyprus-flagged ship, Reliable, loading oil at a port in Venezuela. Venezuelan oil is under embargo by the US.

Reliable, top, at a refinery in Venezuela. Planet Labs
Case Study: Intentional AIS Falsification

While the *Reliable* was spotted at Punto Fijo (yellow arrow), its AIS transmissions showed it adrift off the coast of Santa Lucia (red arrow) hundreds of km away.
Case Study: Intentional AIS Falsification/Manipulation

Current Status

• AIS Falsification/manipulation is a growing problem, exacerbated by international tensions and embargoes, such as Russia, Iran, Venezuela
• Systems for spoofing AIS are growing in availability
• Detection requires analysis of unusual AIS transmissions, or no transmissions
• Long term solution is to make AIS software more resilient
GPS Jamming and Spoofing

While AIS manipulation may be done to evade detection of illegal activities, GPS jamming and spoofing may be done to attack a ship or deter an Unmanned Aerial Vehicle attack

- A GPS signal at the receiver is weak, (like a 25-Watt lightbulb 15,000 km away)
- Jamming is overloading a receiver with an unwanted signal locally generated
- Can render a GPS receiver dysfunctional
- **Spoofing Note:**
  - May be a prelude to Spoofing by breaking PRN signal lock, and then substituting a Spoofing signal
  - Spoofing is more subtle than jamming and relies on the generation of a counterfeit signal with just the right strength to “lift” a navigation receiver from the legitimate signal.
Case Study: Russian Federation Spoofing

In June 2017, the captain of the merchant vessel Atria provided direct evidence of GNSS spoofing activities off the coast of Gelendzhik, Russia, when the vessel’s on-board navigation systems indicated that the vessel was located in the middle of the Gelendzhik Airport, about 20km away.

Ref: C45ADS, “Above Us Only Stars”
Case Study: Russian Federation Spoofing, 2017

GNSS Spoofing Detected Through AIS Data
June 22, 2017

Spoofed Position at Airport

Ship Path Jumps Between Ship’s True Location and Civilian Airport

True Position at Sea

C45ADS, “Above Us Only Stars”
AIS Path History for Vessels Affected by Spoofed GNSS Signals
June 22, 2017

Spoofed Vessel Location (Gelendzhik Airport)

Actual Vessel Location
Russian Federation Spoofing (cont.)

Possible Motivation

• Between Feb 2016 and 2018, 1,311 commercial vessels affected

• AIS reported positions at the local airports

• This might have been motivated by the prevention of drones in denied airspace, forcing them to land or backtrack

• Often events coincide with high value targets in vicinity (e.g., Putin)
Kerch Port Spoofed 200 km to Crimea
Day that Putin visited Kerch project Sept 15, 2016

Spoofed Vessel AIS Path to Simferopol Airport

President Putin in Kerch to Oversee Construction of Kerch Bridge
Positioning, Navigation, and Timing (PNT) System

The MTS depends heavily on the three dimensions of PNT, which are derived primarily from GPS. This is true for other CI, as will be shown

• The dependence of CI on GPS with its vulnerabilities has been a concern for a while.

• A key attribute of GPS is its use of global satellite constellations, but satellite signals are vulnerable to spoofing and jamming

• The recent Russian threats, including threats on ICS/SCADA, have greatly heightened these concerns. Many CI depend on accurate timing and synchronization, largely derived from GPS. Some slides from DHS follow:
Civilian GPS Applications

Civilian GPS penetration growing / dependencies not well understood

GPS Supporting Power Grid Systems

GPS Supporting Banking Operations

GPS Supporting Transportation Systems

GPS Supporting Communications Systems
GPS Support to Maritime Operations

- Management of maritime port facilities
- GPS technology, coupled with geographic information system (GIS) software, is key to automated container operation
- Navigation to optimum fishing operations, and compliance with regulations
- Underwater surveying, buoy placement, and navigation hazard location and mapping
- Search and Rescue
Countermeasures and Mitigations

Under study

• Use several receivers (difficult to spoof simultaneously, especially if separated)
• Look for direction of received signal (could it be coming from something other than a satellite?)
• Alarm for unexpected loss of GPS (signal loss might be a prelude to an attack)
• Possibly use eLORAN beacons (terrestrial) to complement GPS
• Use GNSS receiver that employ GPS, GLONASS, Galileo, Bei Dou in case GPS satellites are damaged
Module 7 Summary

In this module:

• The basics of GPS and AIS operations were presented, with an eye toward how they could be jammed, spoofed, or manipulated

• The growing concern of criminal manipulation of AIS was discussed, with examples

• The differences between GPS jamming and spoofing were explained, as well as how jamming could be used to initiate a spoofing attack

• Examples and a Case Study were presented as to how spoofing attacks may have been done by the Russian Federation

• The widespread use of GPS in most CI requires urgent understanding and mitigation of GPS threats!

• See also GPS/GNSS Security, Backup and GPS Timing Alternatives – RNTF, https://rntfnd.org/
This material is based upon work supported by the U.S. Department of Homeland Security under Cooperative Agreement No. 2014-ST-061-ML0001.

MSC@stevens.edu
www.stevens.edu/MSC