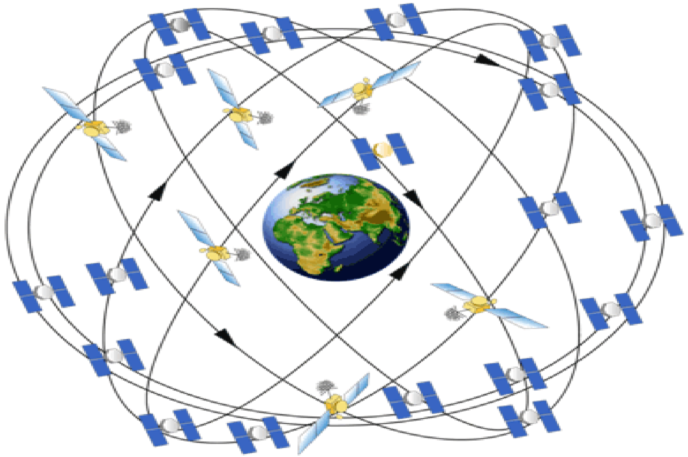
GPS Network Timing Integrity



Malcolm J Airst,
Senior Principal Engineer
MITRE Corporation,
619-318-3837
mairst@mitre.org

C3I INTEGRATION AND INTEROPERABILITY CAPSTONE PROGRAM

The Problem

- Modern communications networks depend on GPS-derived time and frequency reference signals
- Our reliance on GPS and its global nature also make it a target for denial/interference by adversaries and even hobbyists
- Advanced spoofing—re-creating valid signals but adding a time delay—is a greater threat than jamming
  - When jammed we can take simple counter-measures; advanced spoofing is invisible to the user
- Industry/academia have demonstrated a low-cost (<$2k) spoofer using commercially available parts
  - Mitigations exist but customer demand is lacking
  - Detailed techniques, components and software required to construct a GPS Spoofer are now widely available via the public domain (a recent Google search returned almost 500,000 hits)
- Effects of jammed and spoofed signals can be significant
  - Can disable radios, provide incorrect time stamp to stock trades, etc
  - Create positioning errors resulting in the user erroneously believing he is somewhere where he is not

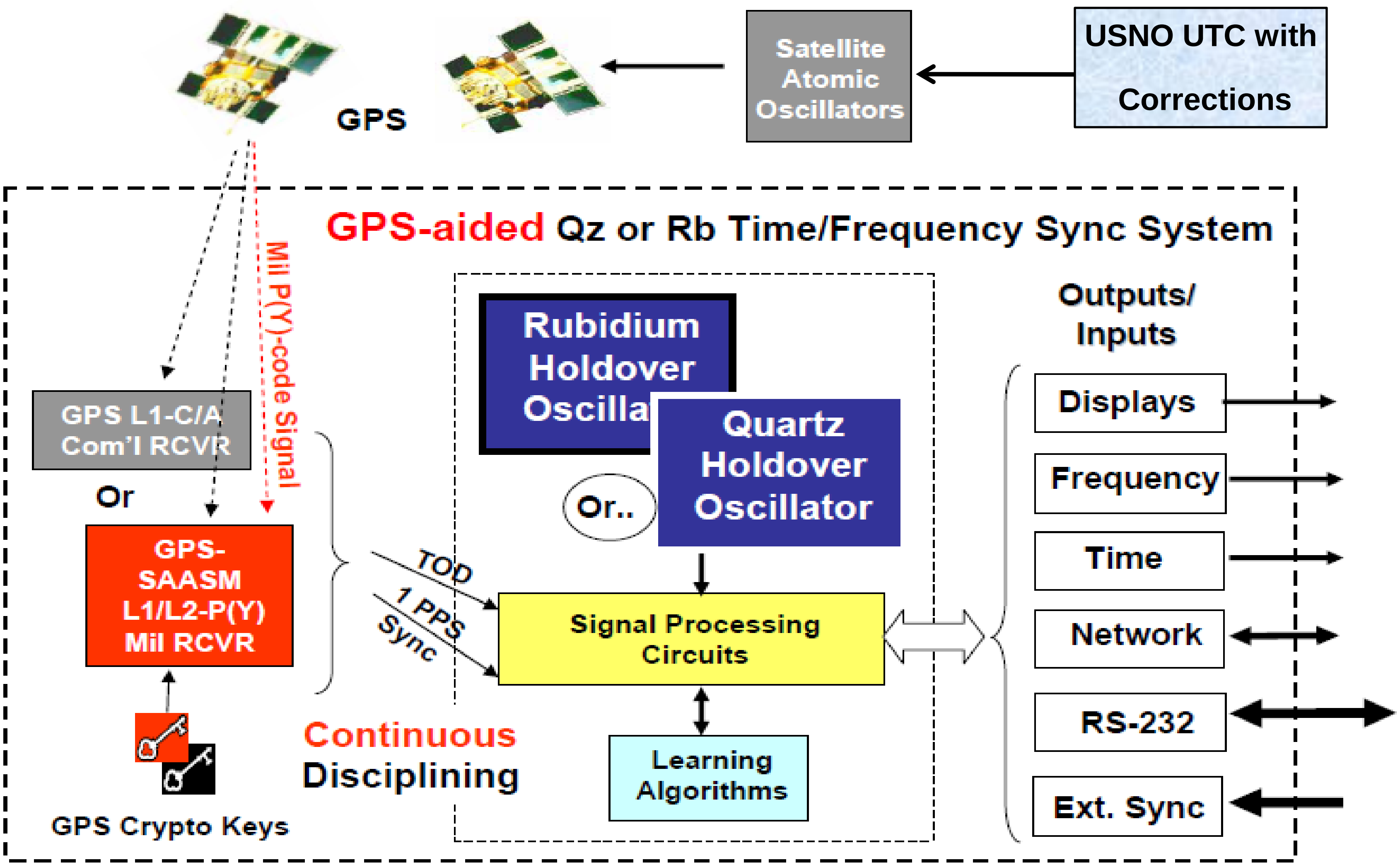
MITRE

GPS a Victim of Its Own Success

- **Ubiquity of GPS makes it the primary source of PNT/F information to all users**
  - **Provides a free service to all GPS users**
    - **For positioning/navigation information**
    - **For precision time, frequency and phase information**
- **The reliance on GPS, its global nature, and the information advantage we derive from PNT/F makes GPS an ideal target for attack – many users unaware of threats**
  - **Adversary threats**
    - **Ground, air, and space based**
    - **EW, advanced and persistent cyber bad guys**
  - **Insider vulnerabilities**
    - **Networked receivers present cyber attack challenge**
- **Threat has expanded from nation-state to informed hobbyist**

We have an Asymmetric Vulnerability as a result of our dependence

GPS Time/Frequency Server Operation



MITRE

Typical Point-of-Presence Time and Frequency Signals

1 pps (pulse/second) to frequency hopping radios

1.544 MHz for telephony (to PBX)

NTP and Device Management (Ethernet)

• NTP for C4ISR track and event time tagging, common time distribution

1, 5 or 10 MHz Reference
(to SONET/DWDM Equipment)

Symmetricom Xli GPS-Disciplined Rubidium Shown

GPS System Vulnerabilities*

- **Unintentional Interference**
  - Radio Frequency Interference (RFI)
  - GPS Testing
  - Ionospheric; Solar Max
  - Spectrum Congestion
- **Intentional Interference**
  - Jamming
  - Spoofing – Counterfeit Signals
  - System Damage
- **Human Factors**
  - User Equipment & GPS SV Design Errors
  - Over-Reliance
  - Lack of Knowledge/Training

1 Watt Jammer

* Courtesy of Dr. M. Weiss, NIST

Factors Impacting GPS Vulnerability*

- Very Low Signal Power
- Single Civil Frequency
  - Known Signal Structure
- Spectrum Competition
- Worldwide Military Applications Drive a GPS Disruption Industry
  - Jamming Techniques are Well Known
  - Devices Available, or Can be Built Easily

* Courtesy of Dr. M. Weiss, NIST

Disruption Mechanisms – Jamming*

- **Jamming Power Required at GPS Antenna**
  - On order of a Picowatt (10^{-12} watt)
- **Many Jammer Models Exist**
  - Watt to MWatt Output – Worldwide Militaries
  - Lower Power (<100 watts); "Hams" Can Make
- **Jamming Signal Types**
  - Narrowband
  - Broadband
  - Spread Spectrum - PRN Modulation

Russian Jammer

* Courtesy of Dr. M. Weiss, NIST

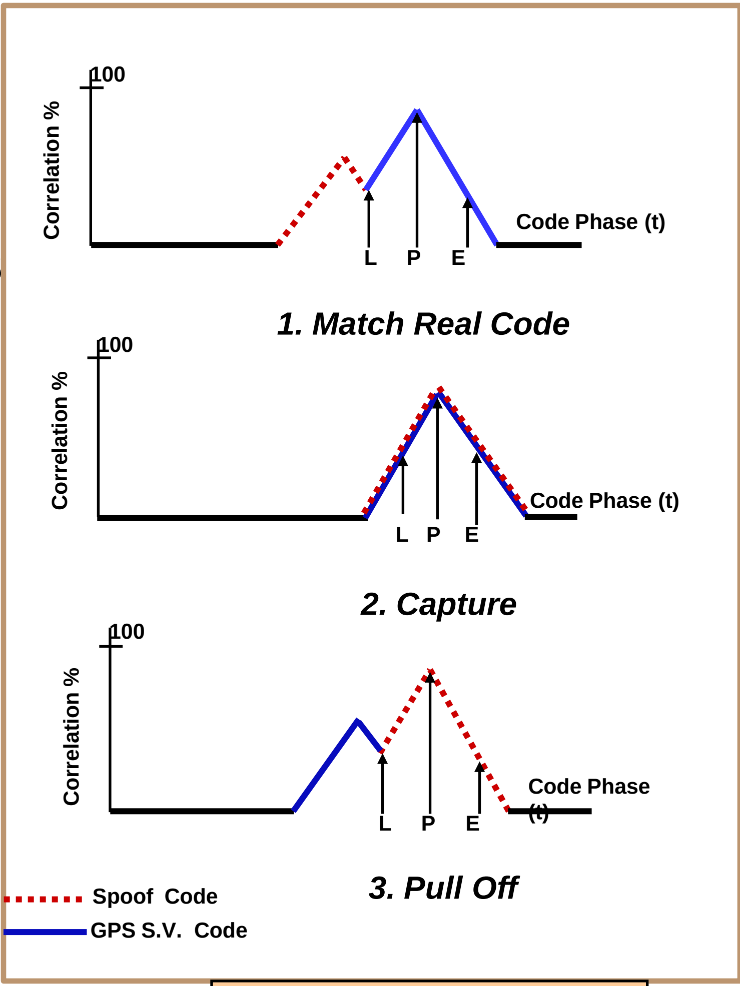
Intentional Jamming*

- **North Korean jammers exist, based on technology from the Iraq war 2003**
- **There are credible reports that China created jammers in 2007**
- **Domestic US jammers have been sold in order to disable potential vehicle tracking**
- **Techniques are available for a receiver to detect if it's being jammed**

* Courtesy of Dr. M. Weiss, NIST

Disruption Mechanisms - Spoofing/Meaconing*

- **Spoof – Counterfeit GPS Signal**
  - C/A Code Short and Well Known
  - Widely Available Signal Generators
- **Meaconing – Delay & Rebroadcast**
- **Possible Effects**
  - Long Range Jamming
  - Injection of Misleading PVT Information
- **No "Off-the-Shelf" Mitigation**



Successful Spoof

* Courtesy of Dr. M. Weiss, NIST

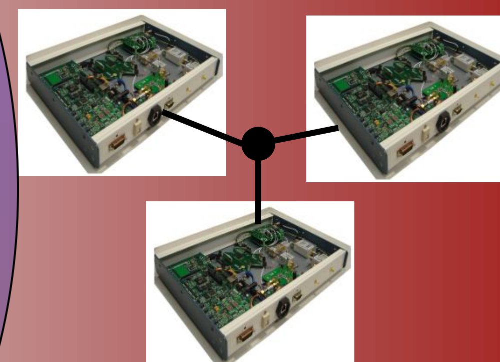
Examples of GPS Simulators

CAST 5000

Pendulum GSG-55

MITRE

Civil GPS Spoofing Threat Continuum*

Simplistic	*Intermediate*	*Sophisticated*
		
Commercial signal simulator	Portable software radio	Coordinated attack by multiple phase-locked spoofers

* Courtesy of Coherent Navigation, Inc

Untraditional Target: Financial Sector*

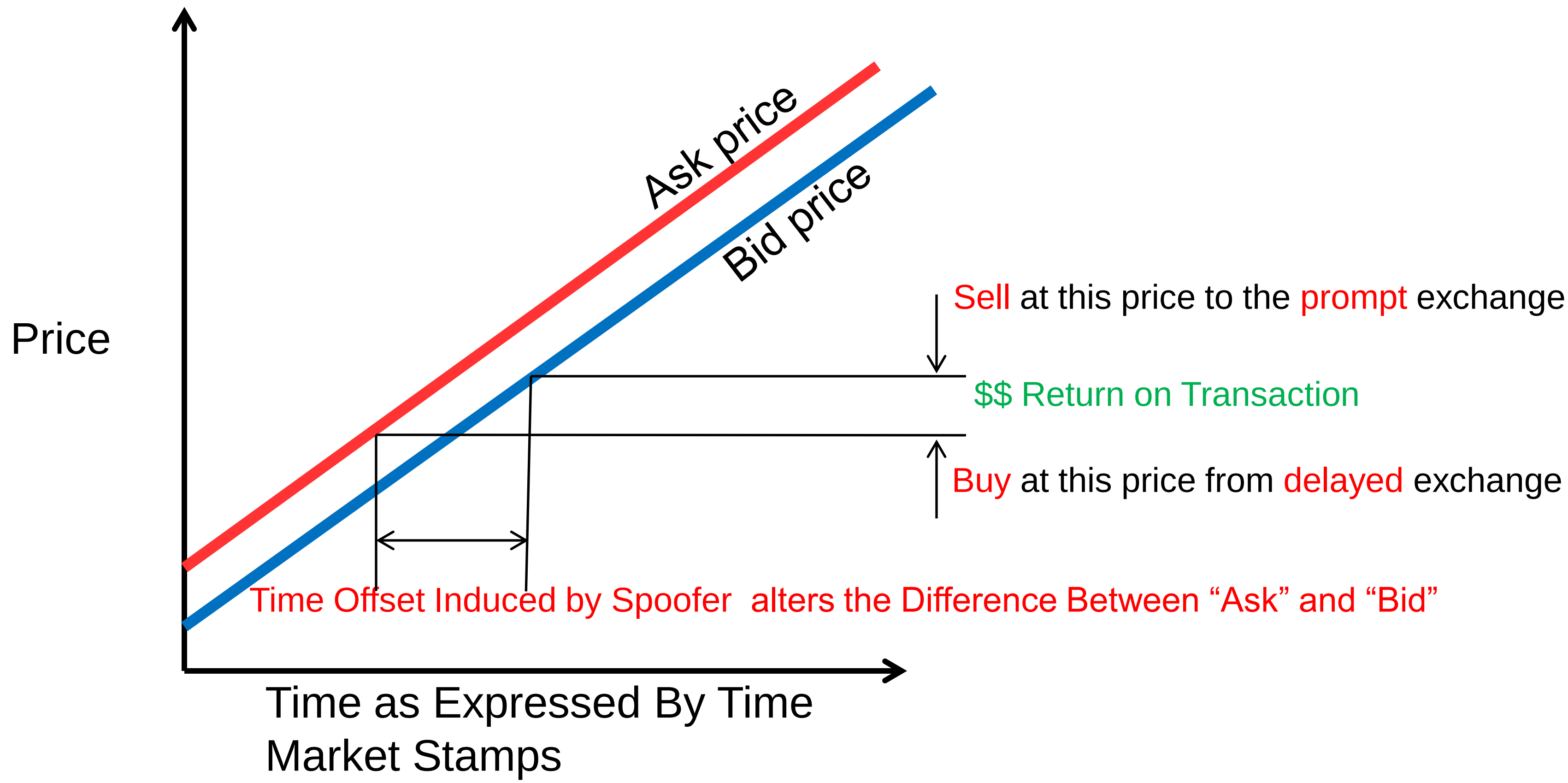
- The New York Stock Exchange and the Nasdaq have large data centers that hold the exchanges' matching engines -- the modern-day equivalent of the historic trading floor -- in racks of interconnected servers.
- DHS (Department of Homeland Security) considers these data centers part of the national critical infrastructure
  - Private security personnel, tall fences, and the best network security money can buy protect the integrity of the thousands of high-stakes trades executed every second within these data centers.
- The NTP (Network Time Protocol) port that the network firewalls is unprotected
- An unassuming set of antennas on the data center's roof carry unsecured civil GPS signals directly into the core of the matching engine network
- Slaved to a once-per-second synchronization pulse from a GPS-locked timing card, the individual servers in the network apply time stamps to the trades they execute
- Far less accurately, many trading houses are obtaining time from Sprint or Verizon cellular networks, which then obtain time from civil GPS
- A decade ago, a tenth of a second was an acceptable time stamp resolution
- High frequency traders now demand nanoseconds (billions of a second)

* Courtesy of Dr. Todd Humphries, University of Texas at Austin

GPS Spoofing Wall Street*

C3I INTEGRATION AND INTEROPERABILITY
CAPSTONE PROGRAM

- A GPS Time attack could possibly manipulate trading



* Courtesy of Dr. Todd Humphries, University of Texas at Austin

Selected Protocol Interface Tolerances

Interface Type	Time Tolerance	Frequency Tolerance	Notes
Serial	n/a	*0.01 %*	12.8 Hz at 128 kbps
SONET	4.6 µsec/sec	4.6 Hz per MHz	46 Hz on 10 MHz frequency reference, 715 Hz for OC-3
IP	n/a	n/a	Asynchronous
Ethernet	25 µsec	50 ppm	5 kHz for 1 GbE
NTP	n/a	n/a	Application specific, inaccuracy increases proportional to distance from the server
CDMA	+/- 3 µsec	n/a	With respect to UTC

SONET Timing Specification Limits

- **Maximum SONET time or frequency variation is 4.6 ppm (parts per million), or <u>46 Hz on the 10 MHz frequency reference</u> feed from the GPS receiver to the SONET add/drop multiplexer (ADM) and associated equipment**
- **4.6 ppm translates to 4.6 Hz per MHz or 4.6 µsec/sec of time offset**

OC-X	Maximum Frequency Offset*
3 (155.52 MHz)	715 Hz
12 (622.08 MHz)	2.861 kHz
48 (2.488 GHz)	11.446 kHz
192 (9.953 GHz)	45.760 kHz

NTP Derived via GPS

- **GPS receivers (Symmetricom or FEI-Zeifer) are deployed at sites to provide "time-of-day" or *Network Time Protocol* (NTP) services where required/requested**
  - **NTP is an Internet Protocol (IETF RFC-1305) used to synchronize the clocks of computers (and often routers as well to some type of time reference)**
- **Typical NTP accuracy (derived from USNO or NIST) is within 10-20 msec of UTC (CONUS)/ 100+ MSEC (OCONUS over fiber due to propagation delays)**
- **If greater accuracy is desired, then a local GPS receiver is required to provide a local NTP source**
- **NTP accuracy requirements are determined by the way NTP is used**
- **NTP is very inaccurate (typically + 2 seconds of UTC) when obtained via the Internet**

GPS Spoofing Detection / Mitigation

- **Civilian GPS signals are without authentication or encryption, making detection and mitigation more difficult**
- **Most mitigations involve integrity checking via multiple clocks, user-supplied position, and RF signal anomalies**
- **Recommend vendors add integrity checking to time/frequency servers**
- **Receivers should detect signal anomalies such as**

- **Wrong time (compared to reference clock)**
- **Suspiciously low noise**
- **Excessive signal strength**
- **Artificial spacing of signals**
- **Limited short term jitter or variation in signal strength**
- **All satellites have the same signal strength**
- **High level sanity checks (e.g., no large position discontinuities)**

Potential Augmentations to GPS

Time	Today	Near Term	Far Term
National	GPS	GPS/IEEE- 1588	LF/Multiple GNSS/IEEE-1588
Deployable	GPS/Atomic Clocks	GPS/Atomic Clocks/ Multi-sensor integration/3G-4G Cellular	LF/GNSS/ Multi-sensor integration/ Signals of opportunity
Worldwide	GPS	GPS/IEEE- 1588/DTV	LF/IEEE-1588/Multi GNSS

Recommended Mitigations

- Immediate migration to NTPv4, to add authentication and other enhancements to mitigate NTP cyber threat
- Critical timing subsystems, especially those used in major communications nodes should detect and mitigate GPS jamming and spoofing via multiple means
  - Integrity checking via multiple atomic clocks and multi-sensor fusion
  - Detect and mitigate rate of clock walk-off via advanced disciplining algorithms
  - Employ user-provided position information as additional integrity check
- Employ available Chip Scale Atomic Clock (CSAC) for mobile or SWAP (Size, Weight and Power)-constrained applications
  - Use CSAC as additional integrity check
- Disseminate precision time and frequency from critical nodes to other platforms via IEEE 1588v2