#RSAC

RSA Conference2018

San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: HTA-W12

WHAT TIME IS IT? HOW MANIPULATING "NOW" CAN CRASH OUR WORLD

Michael Calabro

Senior Lead Engineer
Booz Allen Hamilton
Calabro_Michael@bah.com

Why do we need Synchronization?

- Event ordering
- Fairness in Race Conditions
- Security
- Event Forensics

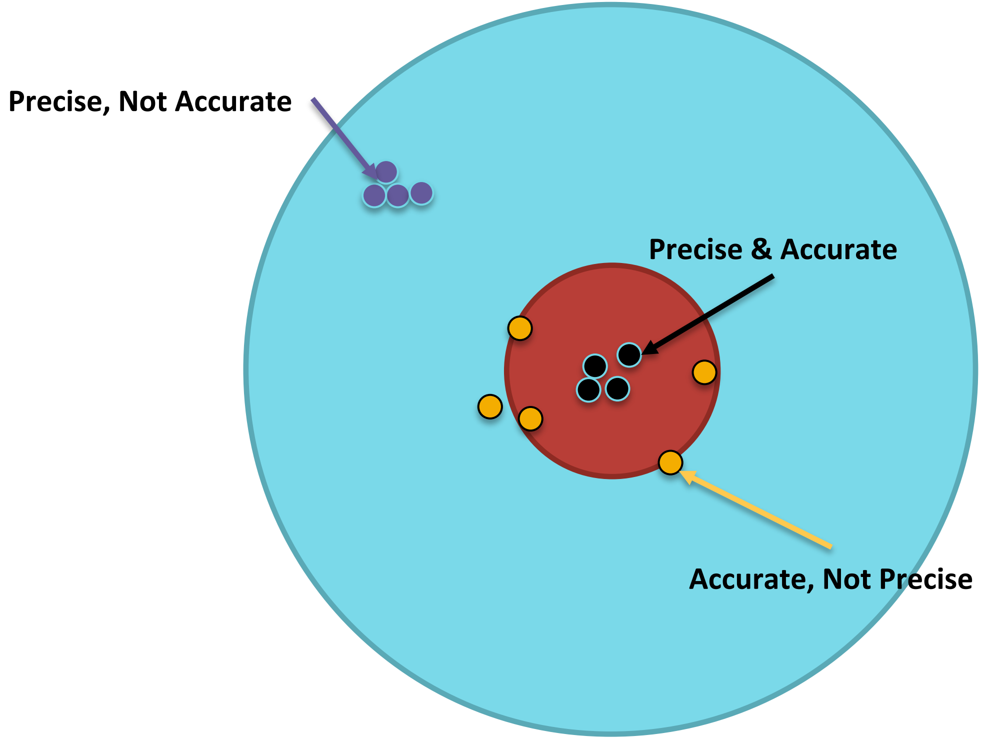
Time is Made Up

- Physicists noted that some materials generate very stable reference signals at predictable periods (cesium, rubidium)
- If you count these periods …
- The SI definition of a **second** is the time that elapses during 9,192,631,770 cycles of the radiation produced by the transition between two levels of the cesium 133 atom.

Time Scales are Agreed Upon and "Local"

UTC (USNO) UTC (NIST) Mike Time

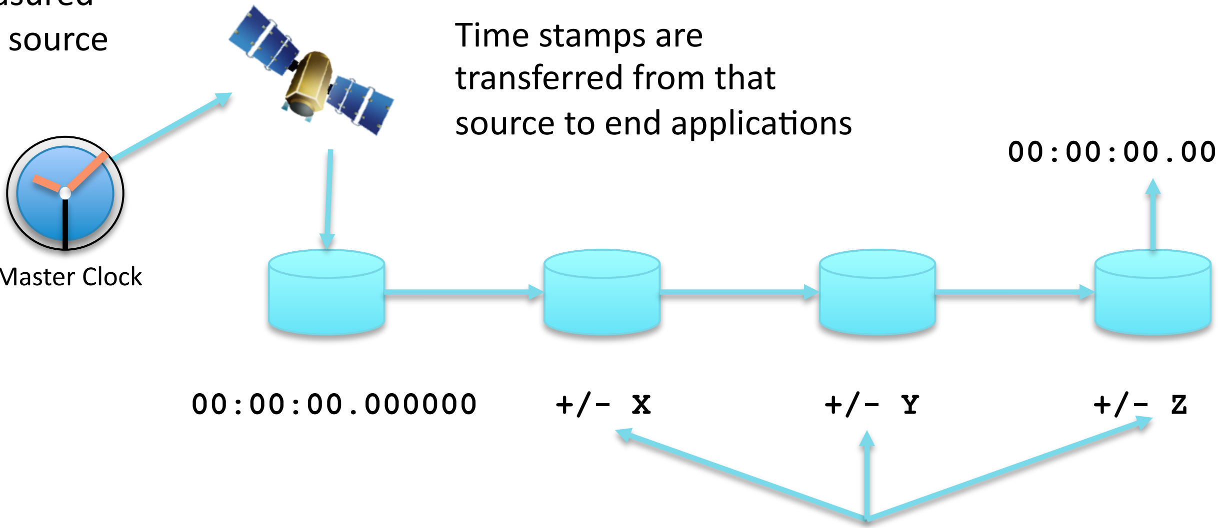
Time Accuracy and Precision are Distinct



The Path of Time Transfer

Time is measured at a source

Time stamps are transferred from that source to end applications



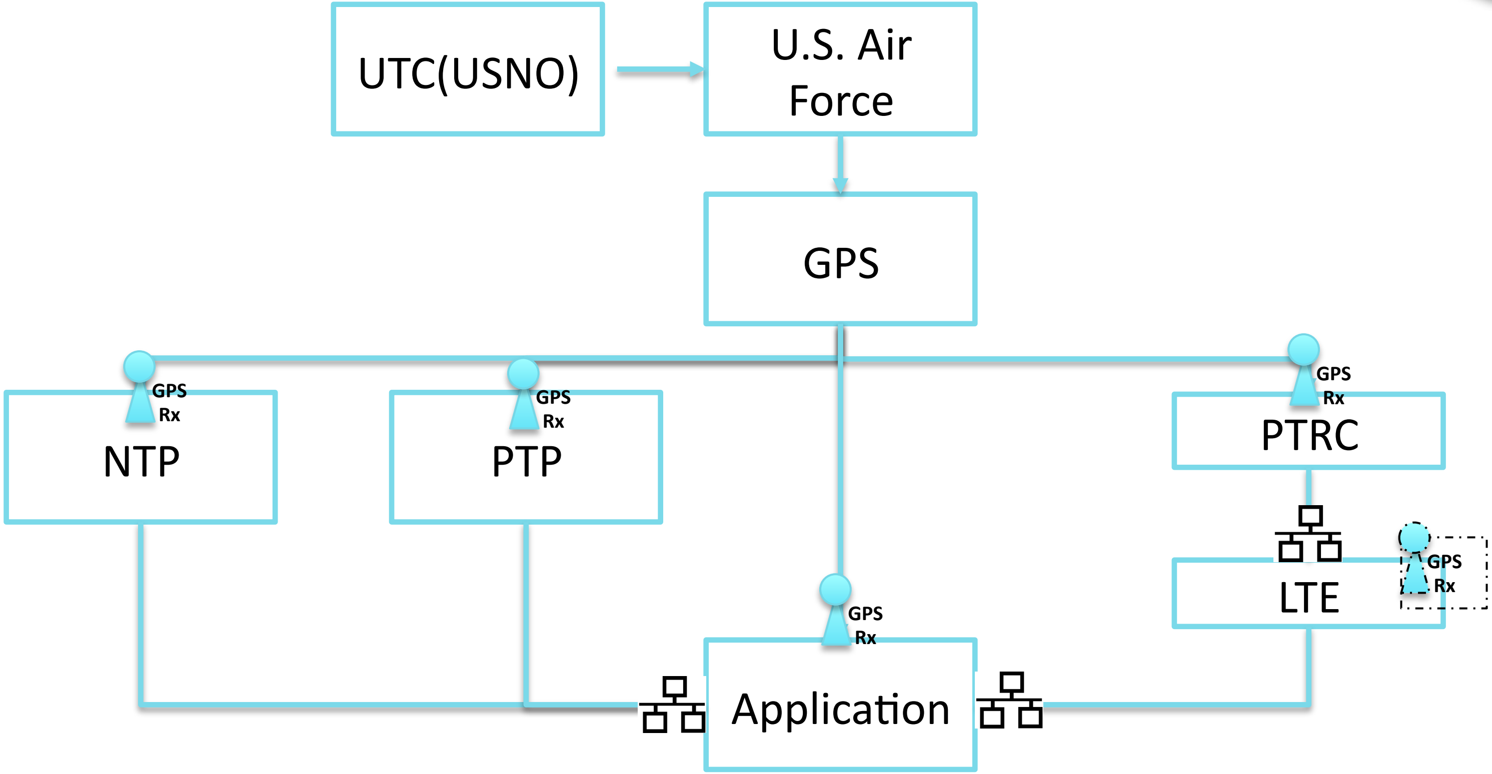
Master Clock

00:00:00.000???

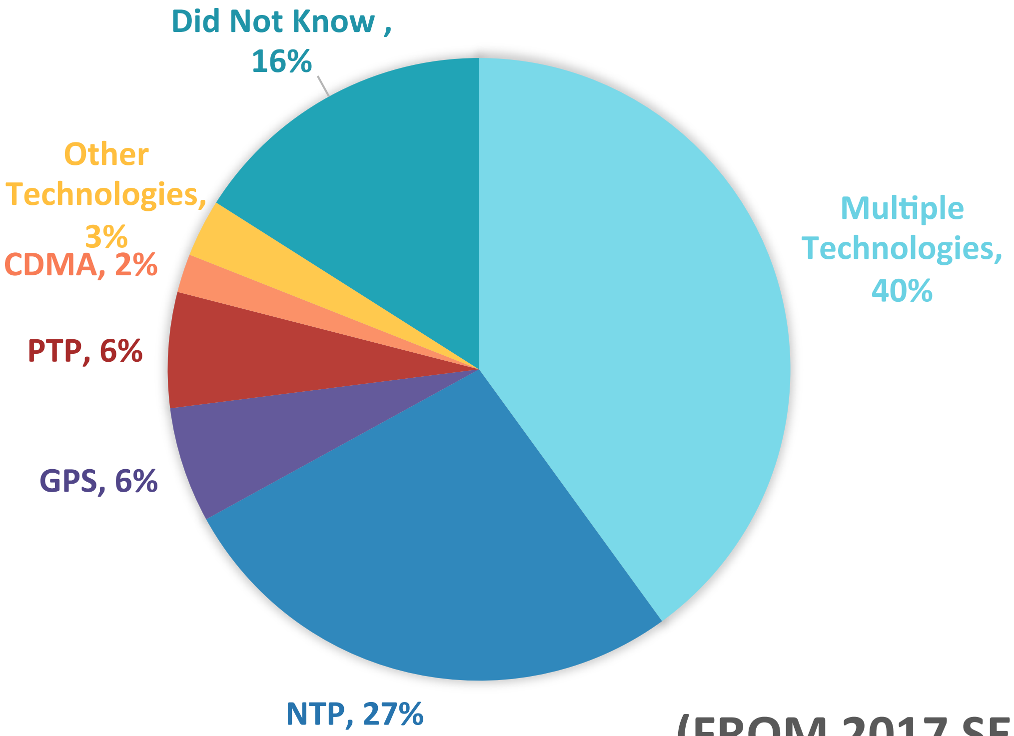
00:00:00.000000 +/- X +/- Y +/- Z

Delays are known or bounded

Time Transfer and Time Sources are Different



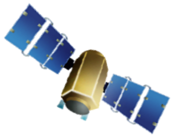
Financial Business Clock Time Sources



(FROM 2017 SEC CLOCK SURVEY)

How Time is Transferred via GPS

- Precise code phase alignment can give < 10 nanoseconds of precision
- Distance (m) / Speed of Light (m/s) = Delay (Rule of Thumb: 1 ft / ns)



Path Delay

01001101101010110101011110101

01001101101010110101011110101

RX

SV Transmits known PN Sequence

GPS receiver generates local copy and aligns it to transmitted sequence

Precision of alignment determines precision of time delay calculation

GPS is Vulnerable to Manipulation

Data Attacks

Broadcast by GPS

$$t_{UTC} = W\left[\text{Modulo }(86400 + \Delta t_{LSF} - \Delta t_{LS})\right], \text{ (seconds)};$$

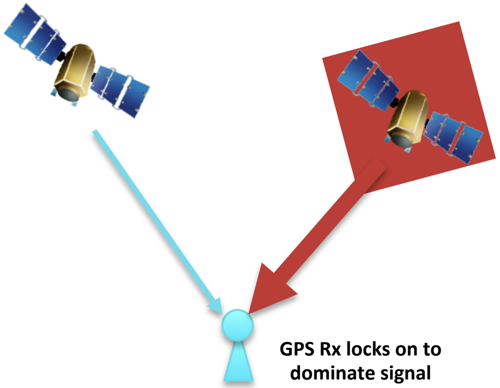
where

$$W = (t_E - \Delta t_{UTC} - 43200)\left[\text{Modulo } 86400\right] + 43200, \text{ (seconds)};$$

Algorithms from GPS SPS Specification

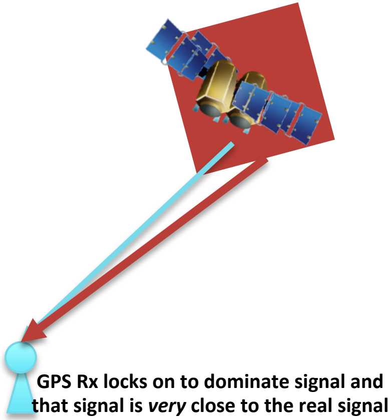
Receivers and their applications do math based on broadcast parameters. Divide by zeros? Overflows? Time might go backwards.

Repeaters or Unsynchronized Spoofers



Time will jump around.

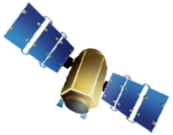
Code Phase Synchronous Spoofers



Time may advance more or less quickly … but at a high level, may appear accurate.

How GPS Time can be Subtly Spoofed

#RSAC



Path Delay

0100110110101011010101110101

SV Transmits PN Sequence

Spoofer

Near Matched Delay

0100110110101011010101110101

0100110110101011010101110101

RX

Rx Generates local copy and aligns it to transmitted sequence

Precision of alignment determines precision of time delay calculation

Review So Far

- Time is "made up"
- Time is Measured directly or Transferred
- GPS is a common source of time across all applications
- Timing and Synchronization requirements exist at a variety of levels across applications
- So… What happens when Synch breaks down?

Telecommunications Networks Have the Strictest Commercial Timing Requirements

Application/ Technology	Accuracy	Specification
WCDMA MBSFN	12.8 µs	[b-3GPP TS 25.346] sections 7.1A and 7.1B.2.1
LTE-TDD (wide-area)	10 µs	[b-3GPP TS 36.133]) section 7.4.2
LTE-TDD to CDMA	10 µs	[b-TS 3GPP TS 36.133] section 7.5.2.1
CDMA2000	3 µs	[b-3GPP2 C.S0002] section 1.3; [b-3GPP2 C.S0010] section 4.2.1.1
WCDMA-TDD	2.5 µs	[b-3GPP TS 25.402] sections 6.1.2 and 6.1.2.1
WiMAX (downlink)	1.428 µs	[b-IEEE 802.16] table 6-160, section 8.4.13.4
WiMAX (base station)	1 µs	[b-WMF T23-001], section 4.2.2
Primary Reference Time Clock	100 ns	[ITU-T G.8272] (Primary Reference Time Clock)
Enhanced PRTC	30 ns	[ITU-T G.8272.1] (Enhanced Primary Reference Time Clock)

Power Grid Uses of Time

Grid application	Timing requirements (minimum reporting resolution and accuracy relative to UTC)
Advanced time-of-use meters	15, 30, and 60 minute intervals are commonly specified (ANSI C12.1)
Non-TOU meters	Ongoing, with monthly reads or estimates
SCADA	Every 4-6 seconds reporting rate
Sequence of events recorder	50 µs to 2 ms
Digital fault recorder	50 µs to 1 ms
Protective relays	1 ms or better
Synchrophasor/phasor measurement unit (30 - 120 samples/second)	Better than 1 µs 30 to 120 Hz
Traveling wave fault location	100 ns
Micro-PMUs (sample at 512 samples/cycle)	Better than 1 µs
Communications protocols	
Substation local area network communication protocols (IEC 61850 GOOSE)	100 µs to 1 ms synchronization
Substation LANs (IEC 61850 Sample Values)	1 µs

From NASPI-2017-TR-001

EU Finance Requirements in Effect Jan. 2018

Level of accuracy for operators of trading venues

Gateway-to-gateway latency time of the trading system	Maximum divergence from UTC	Granularity of the timestamp
> 1 millisecond	1 millisecond	1 millisecond or better
≤ 1 millisecond	100 microseconds	1 microsecond or better

Level of accuracy for members or participants of a trading venue

Type of trading activity	Description	Maximum divergence from UTC	Granularity of the time-stamp
Activity using high frequency algorithmic trading technique	High frequency algorithmic trading technique.	100 microseconds	1 microsecond or better
Activity on voice trading systems	Voice trading systems as defined in Article 5(5) of Commission Delegated Regulation (EU) 2017/583 (1)	1 second	1 second or better
Activity on request for quote systems where the response requires human intervention or where the system does not allow algorithmic trading	Request for quotes systems as defined in Article 5(4) of Delegated Regulation (EU) 2017/583	1 second	1 second or better
Activity of concluding negotiated transactions	Negotiated transaction as set out in Article 4(1)(b) of Regulation (EU) No 600/2014.	1 second	1 second or better
Any other trading activity	All other trading activity not covered by this table.	1 millisecond	1 millisecond or better

From COMMISSION DELEGATED REGULATION (EU) 2017/574

Some Scenarios – Financial Front Running

T = 0.000
T = 0.001
    Buyer buys 1000000 shares of ABC
    Seller sells 100000 shares of ABC
T = 0.002

T = 0.00000
T = 0.00010
    Seller sells 100000 shares of ABC
T = 0.00035
    Buyer buys 1000000 shares of ABC
T = 0.00200

Which ordering of events would you prefer? What if you could change your time stamp?

January 25th, 2016 – The Worldwide "Spoof"

A Unique Set of Error Conditions

- On January 25th, 2016, during the retirement of the last IIA satellite, an error occurring in the GPS system causing many receivers that used the UTC correction broadcast by the satellites to be ~13.7 microseconds deviant from truth
- Global effect
- Not all satellites broadcast erroneous data
- Affected receivers needed to obtain their UTC offset from a bad satellite – i.e. not all receivers with a common skyview would have been affected

Suspect a GPS Problem? Call the Coast Guard

1) * Your Name: (Our Privacy Policy)		
2) * Email Address:		
3) * Telephone number: [i.e. - (703) 313-5900]		
4) Preferred method and time to be contacted if additional information is necessary:	Click Here For Choices ▾ Click Here For Choices ▾	
5) *What was the start time and date of the GPS disruption?	Date: 04/05/2018 Time: Zone: Select Time Zone ▾	
6) * Is the GPS disruption ongoing?	Select ▾	
7) * Where did the disruption occur? (LAT/LONG; Nearest City or landmark)	**Lat** **Long** **City/Landmarks**	
8) GPS user equipment make and model (receiver manufacturer and model, antenna type, etc...)?		
9) GPS installation type (aviation, marine, surveying, agriculture, transportation, timing)?	Click Here For Choices ▾	Other:
10) What was the elevation of the GPS antenna?	Click Here For Choices ▾	Above Ground Level Above Sea Level
11) What GPS frequency are you using?		
12) How many satellites were being tracked at the time of the disruption?	0 ▾	
13) Which satellites were being tracked at the time of the disruption?		
14) What was the GPS receiver being used for at the time of occurrence?		
15) Summary (Please provide any additional information, unusual screen display indicating a problem and/or operator intervention that may have helped)?	Remaining Characters 3000	

Effects (caused by an ~12 hour event)

- Of ~80 NIST clocks monitoring event, only 11% were unaffected
- Some high performance precision timing receivers took 1+ day to resynchronize to their previous levels of stability
- Many precision timing receivers entered into holdover (starting a count down hours to out-of-spec performance)
- At least one telecommunications backhaul provider reported that it was necessary to manually reset affected precision timing receivers
- Some clocks located in telecom systems started to free run with no atomic discipline or back up
- Many organizations that should have been affected did not report any impact (did they even know how close they came to major issues?)

It is Really Hard to Get Away from GPS…

Timing Source	GPS Dependent	Scale	Availability	Comments
GNSS	Yes	< 100 ns	Global	Not appropriate for all environments; may be denied
GSM NTIZ	Yes	~1s	Regional	
CDMA2000 Sync	Yes	1 ms	Regional	
LTE R11+ SIB 16	Yes	10 ms		Not widely deployed. 10 ms may not be sufficiently precise.
Iridium Time (Satelles)	Yes	< 500 ns	Global	Paid Service; May have higher availability than GNSS
eLoran	Yes	< 100 ns	Europe, Asia, Middle East	Not available in the US

Upcoming 5G and IoT Sync Requirements

- Edge of network sync in in TDD LTE is ~ 1 microsecond; 5G proposes to aggressively push this down – thereby increasing dependency on synch
- Synchronization requirements between cloud processes and events will become stricter
- IoT will need ways to synch local devices

Organizations that are working on this

- ATIS Synchronization Committee
- Resilient Navigation & Timing Foundation
- Network Time Foundation
- North American Synchrophasor Initiative (NASPI)
- National Space-Based PNT Advisory Board and PNT Executive Committee

Conclusions

- GPS remains the most convenient source of time transfer and is the only technology capable of meeting upcoming synchronization requirements efficiently
- 2017 and 2018 are seeing many new synchronization applications being deployed across telecom, finance, transportation, and
- Sync needs to be done securely and deliberately
- Secure Synchronizations Solutions exist today; advocacy is needed at a national level for an alternative system to GPS

Selected References

- NIST Report on January 2016 Outage
  - https://tf.nist.gov/general/pdf/2886.pdf
- SEC Clock Survey
  - https://www.sec.gov/divisions/marketreg/consolidated-audit-trail-clock-synchronization-assessment-051517.pdf
- NASPI
  - https://www.naspi.org/sites/default/files/reference_documents/tstf_electric_power_system_report_pnnl_26331_march_2017_0.pdf

Apply What You Have Learned Today

- Next week you should:
  - Identify synchronization dependent applications within your organization
- In the first three months following this presentation you should:
  - Understand where these sync-dependent applications get their time from and their corresponding tolerances for failure
- Within six months you should:
  - Understand how to attribute system failures to synchronization outages
  - “Protect, Toughen, and Augment” your Timing Sources and Sync Methods

Michael Calabro
Calabro_Michael@bah.com