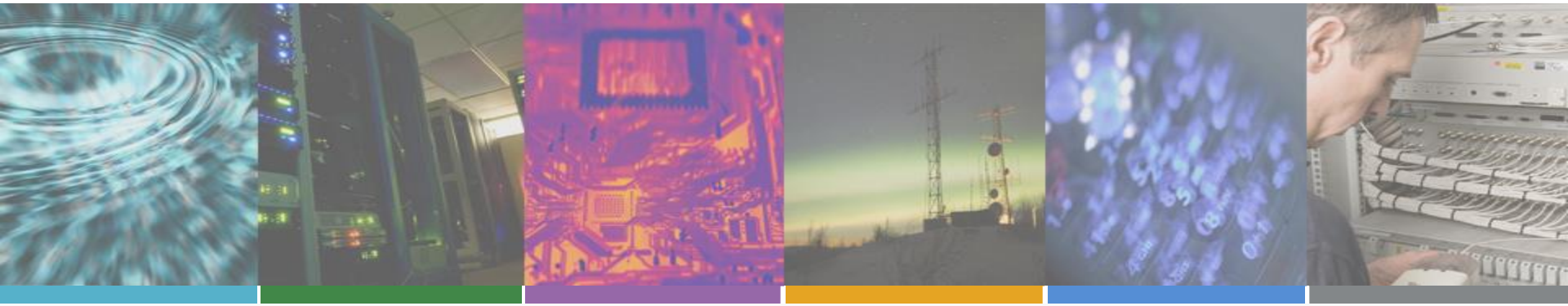
GPS Spoofing Susceptibility Testing



GNSS Vulnerability – Countering the Threat 13th Feb 2013

NPL, Teddington, London

Prof. Charles Curry B.Eng, C.Eng, FIET
Managing Director, Chronos Technology Ltd

With acknowledgements to Brent Ledvina et al, Coherent Navigation, Inc

Presentation Contents

- Background
- Spoofing & Meaconing Defined
- Spoofing Testing
- Conclusions

Presentation Contents

- Background
- Spoofing & Meaconing Defined
- Spoofing Testing
- Conclusions

Background

- Jamming is now better understood
  - GAARDIAN, SENTINEL
- Spoofing and Meaconing
  - Military and Academia
- Bring these GPS Vulnerabilities into perspective
- Assess the threat
- Start to embark on Susceptibility Testing

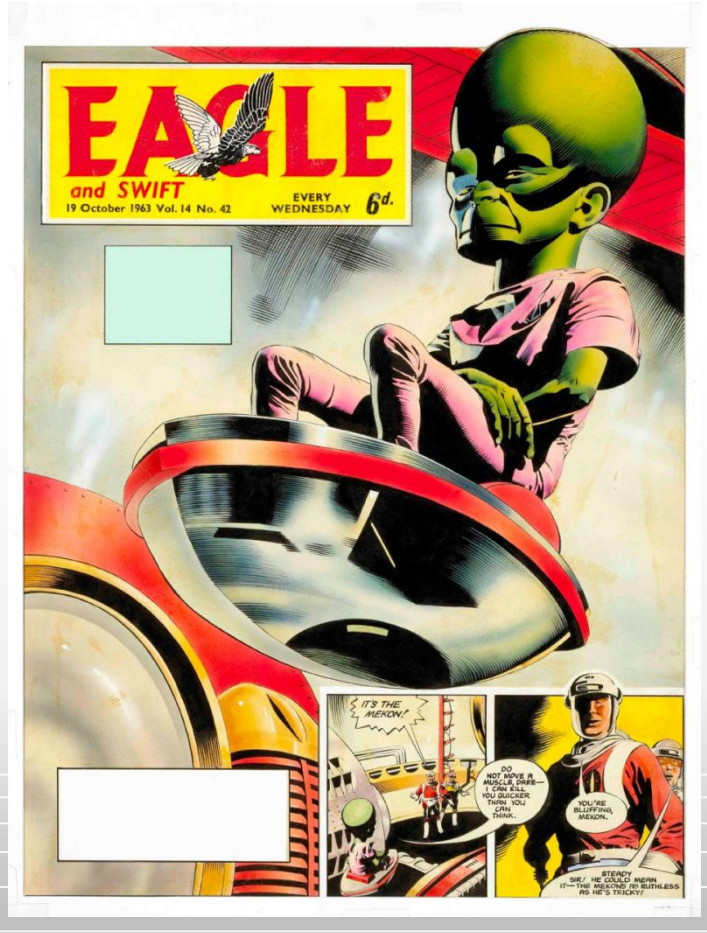
Presentation Contents

- Background
- Spoofing & Meaconing Defined
- Spoofing Testing
- Conclusions

Alternative Definitions!

- Spoof

- Meaconing (Mekon)



Meaconing

- Local re-broadcast of GPS Signals
- Giving false time and/or position
- Current examples (non-military)
  - Faulty Antennas
  - Bad Re-Radiator deployments

Spoofing

- Masquerading as a genuine GPS signal
- Taking over the input to a GPS Receiver
- Steering the GPS Rx off position and/or time
- Without triggering alarms!
- Currently evolving out of Academia
- Emerging threat
- It’s Invisible (unless you have detection)!

Presentation Contents

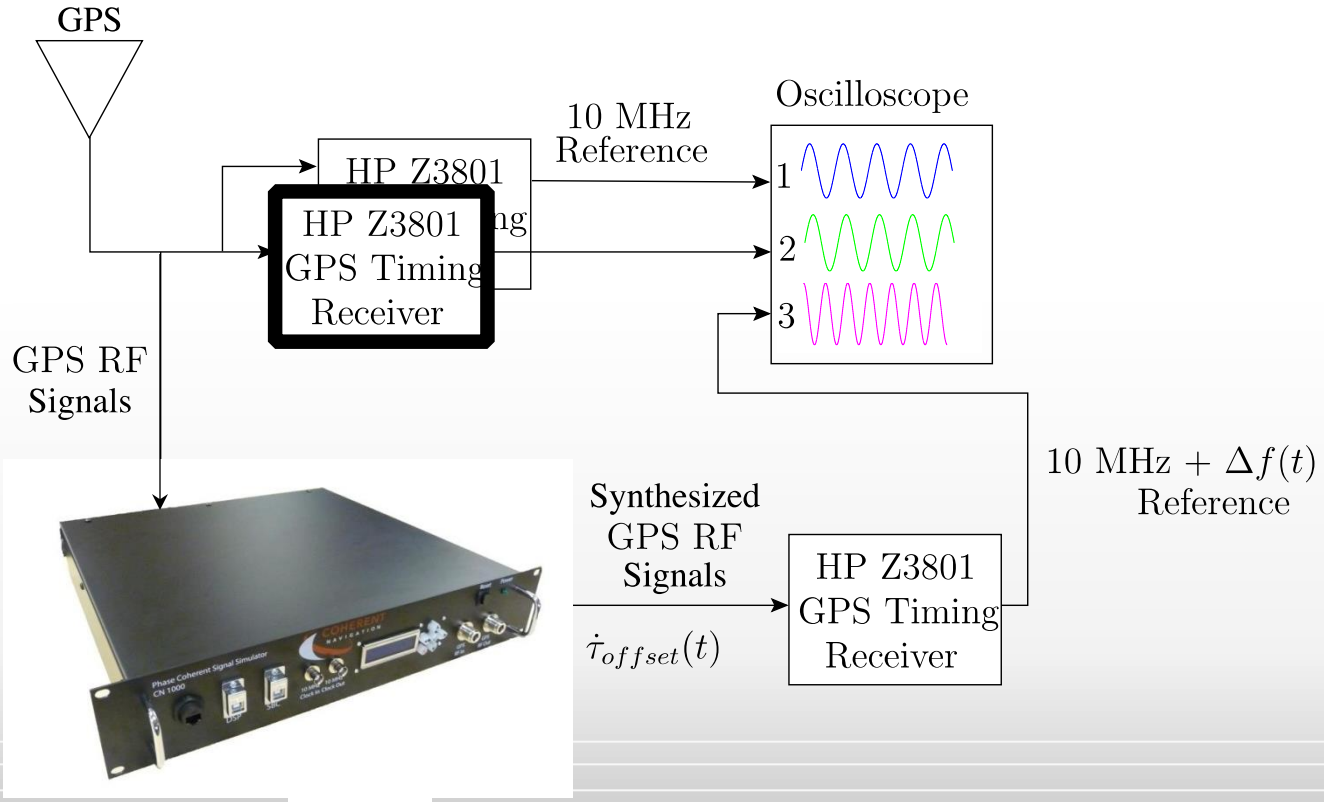
- Background
- Spoofing & Meaconing Defined
- Spoofing Testing
- Conclusions

Spoofing Testing

- Todd's Ted Talk
  - http://www.ted.com/talks/todd_humphreys_how_to_fool_a_gps.html
- Coherent Navigation, Inc – Spoofer Demonstrator
  - PCSS CN1000 on Chronos Booth
- Why Spoofing Testing?
  - Assess vulnerability of application
  - Assess defences to an attack
  - Assess mitigation options

GPS Time Spoofing Experiment

- HP Z3081A GPS Time and Frequency Reference Receiver
  - Contains ovenized crystal oscillator, Motorola GPS receiver, and control logic circuitry



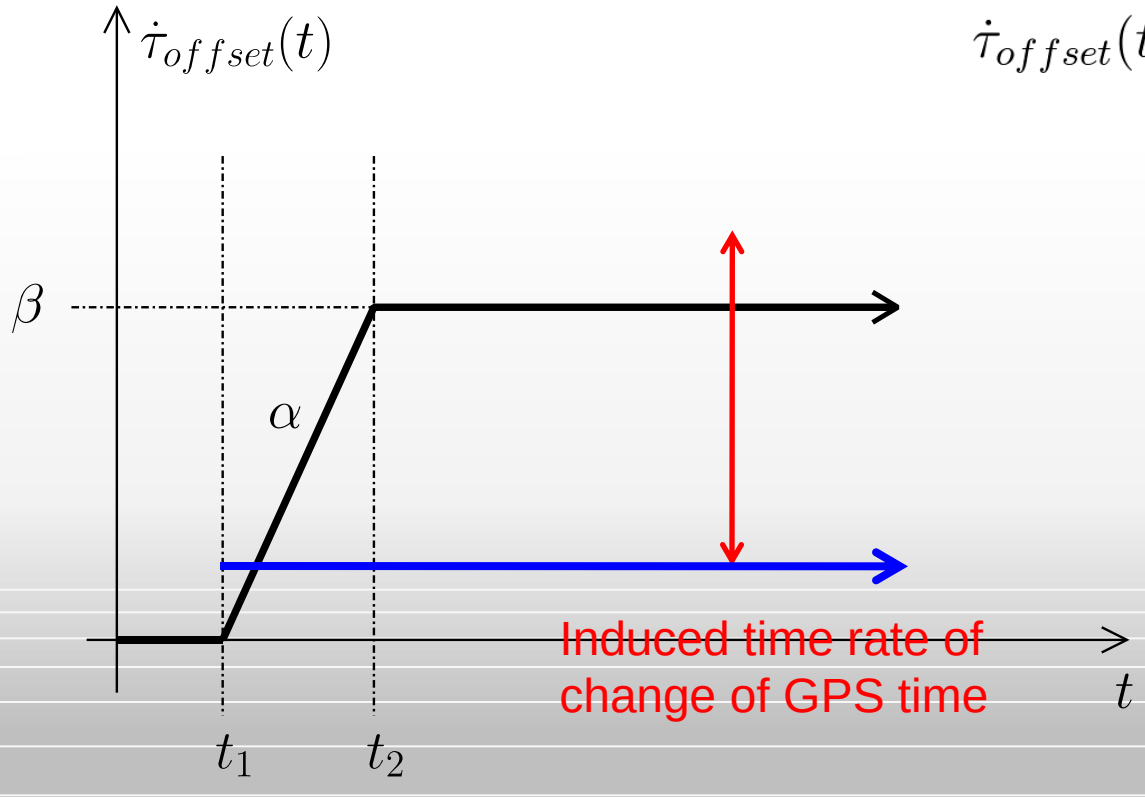
Coherent Navigation Phase-Coherent Signal Simulator (PCSS)

Slide Courtesy of Coherent Navigation

Spoofer Attack Methodology

- Spoofer induces erroneous time rate of change of GPS time,
- Must be careful not to trip alarms programmed into control loops within GPS timing receiver

$$\dot{\tau}_{offset}(t) = \begin{cases} 0 & t < t_1 \\ \alpha(t - t_1) & t_1 \le t < t_2 \\ \beta & t \ge t_2 \end{cases}$$



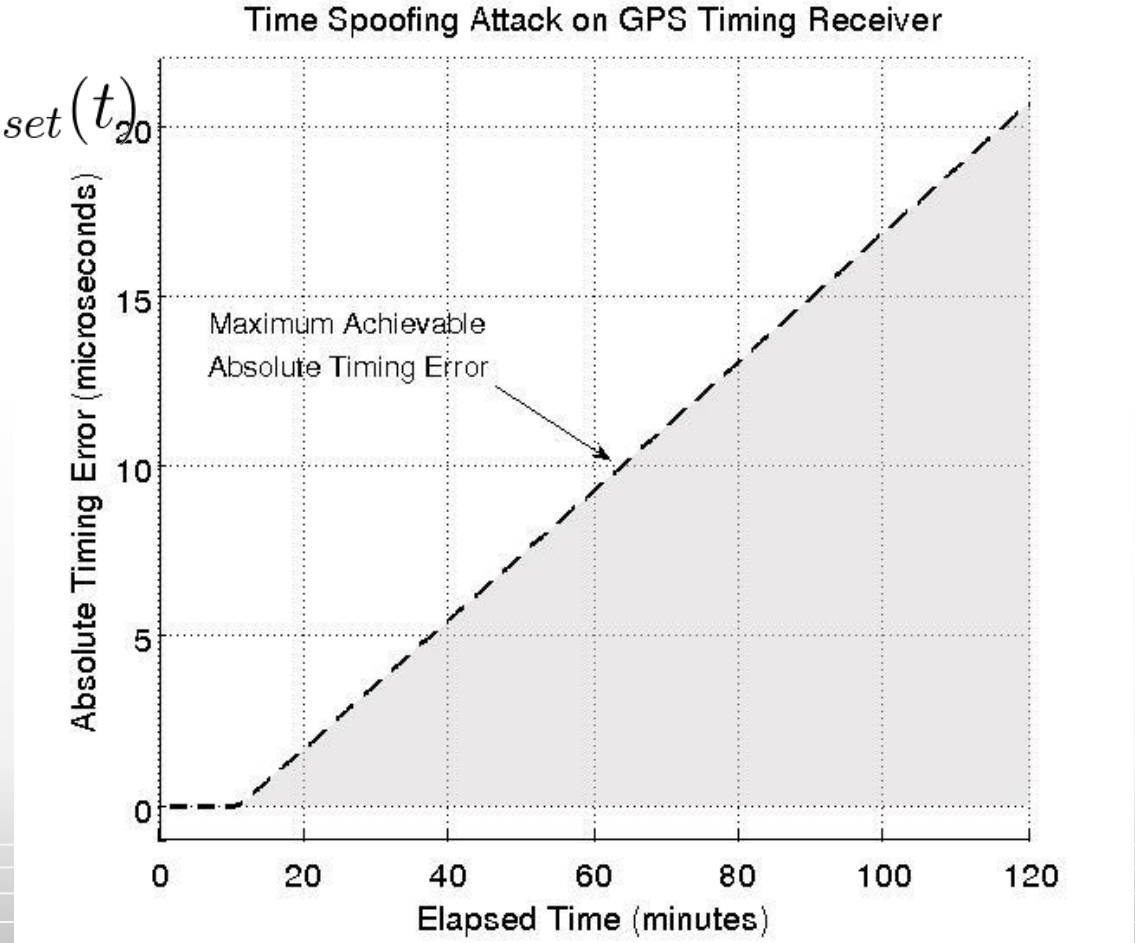
Estimates of GPS timing receiver internal control parameters $\{\alpha, \beta\}$

Slide Courtesy of Coherent Navigation

GPS Time Spoofing Attack

Slide Courtesy of Coherent Navigation

How Long to a 20 µsec offset?



Graph Courtesy of Coherent Navigation

Vulnerable Applications

- Financial Trading - HFT time stamping
- Mobile Base Stations using GPS (Not UK)
- Increased slips in a telecom network
- Erroneous relay protection switching in power networks
- Inability to monitor phase angle on SMART Grid
- Inability to analyse any time stamped data

Chronos Time Spoofing Trials

- Chronos - Spoofing Susceptibility trials
  - CTL Time labs
  - Later this week
- Various GPS Timing Receivers
  - TCXO, OCXO, Rb, CSAC
- Answering Questions…
  - How far can we change time?
- How quickly?
- Without alarms being triggered

Presentation Contents

- Background
- Spoofing & Meaconing Defined
- Spoofing Testing
- Conclusions

Conclusions

- Spoofing & Meaconing – Emerging Threats
- Meaconing here today
  - but few people realise this!
- Spoofing Susceptibility testing available now

Questions?

www.chronos.co.uk

www.gpsworld.biz

www.gaardian.co.uk

charles.curry@chronos.co.uk