# “Toughen” Team

10 June 2015

# “Toughen” Scope

- “Toughen” is the ability for satnav receivers to reject or operate through contaminated or invalid inputs, including:
  - In-band or out-of-band interference
  - Invalid signals transmitted by satellites
  - Invalid signals transmitted by unauthorized sources (spoofers)
  - Space weather (e.g., scintillation)

- Toughen applies to all satnav signals

# Technical Aspects of “Toughen”

- Tougher signals
  - Higher received power
  - Pilot components for robust tracking
  - Forward error control for lower data demodulation thresholds
  - Wider bandwidth spreading modulations for interference resistance
  - Digital signatures or other cryptography for authentication of the transmitted signal
- Tougher user equipment
  - Horizon-nulling or adaptive antijam antennas
  - Multifrequency, multisystem
  - High dynamic range front ends with good selectivity
  - Spoofing discrimination and signal authentication
  - Temporal/spectral interference excision
  - Received signal integrity monitoring and crosschecking
  - Robust acquisition and tracking techniques
  - Information Assurance for networked computing
- Supporting infrastructure
  - Provision of long lasting ephemeris and authentication
  - Independent monitoring and reporting of transmitted signal integrity
  - Information Assurance

# June 2014 Focus

- Aviation
  - MITRE presentation on FAA and RTCA activities
  - Multi-constellation MOPS planned for 2018 is next opportunity for toughening
- Consumer
  - Broadcom presentation
  - Ability to operate through GLONASS events using multiple satnav systems and long term ephemeris
- Critical infrastructure
  - DARPA presentation on PNT technology development
  - Emphasis on high quality clocks

# December 2014 Focus

- Speakers: financial transactions, agriculture, telecommunications & a leading receiver manufacturer.
- Pre-loaded questions for all:
  - What kind of toughness do you think is important for the applications you serve?
  - How do you measure the toughness of the product (conceptually, but also spec and test)?
  - What kind of feedback do you get from customers about the need for toughness?
  - Do you see a need to be tougher, and if so what approaches are you thinking about?
  - What negative aspects (performance, cost, reliability) are associated with making your product tougher?

# June 2015 Focus

- Navigation Message Authentication (NMA), as a subset of Digital Message Authentication
- Pre-loaded questions for all speakers:
  - What benefits would NMA add to GPS?
  - If a receiver is designed to use open and unauthenticated signals with best practices for security and robustness (please summarize what these best practices are in your opinion), what will be the remaining gaps in its ability to resist different types of attack?
  - How well does NMA do in closing these remaining gaps?
  - What limitations or gaps would still exist with NMA?
  - What characteristics (strength, latency, private key vs. public key, etc.) do you think that NMA should have if it is introduced to GPS?
  - If NMA were added to GPS, on what GPS signals do you think it should be added?
  - What negative unintended consequences could NMA introduce (e.g., denial of service vulnerability), and how can these negative unintended consequences be handled?
  - Are there positive unintended consequences that we should consider?
  - Are there any viable approaches for “out-of-band” NMA, and, if so, what are the pros and cons of inband NMA using satellite broadcast signals, and of out-of-band NMA?
  - Do you foresee any kind of market opportunity for third-party out-of-band NMA, and, if so, what do you see as the pros and cons of such an approach?

# June 2015 Take-Aways

- Two speakers:
  - Dr. Todd Walter on NMA for WAAS
  - Professor Todd Humphreys on NMA for GPS
- Key points
  - Receiver-based antispoof techniques can counter many common spoofing attacks; NMA closes gaps that would remain
    - It’s not clear whether the investment in NMA is warranted
    - Threat models and more study are needed
    - Users are not demanding NMA
  - NMA can only be added to modernized GPS signals, not legacy signals
    - If NMA is provided on GPS, users only care if it is on L1, hence the L1C signal
  - GPS uplink capacity limits drive long latency (9 minutes) for NMA, making it of very limited utility
  - For protecting WAAS signals, it might be better and sufficient to protect the WAAS uplink rather than add NMA
  - NMA can introduce increased vulnerability to denial of service attacks; no clear way how to address this
  - SBAS Q channel is available for NMA; requires changes to ground segment and satellite transponder
  - WAAS could provide NMA for GPS messages as well
    - Could explore higher data rate, higher power, more capable FEC to provide higher data rate and maintain low latency for aviation