Security in Wireless and Spectrum Sharing

Opportunities and Challenges

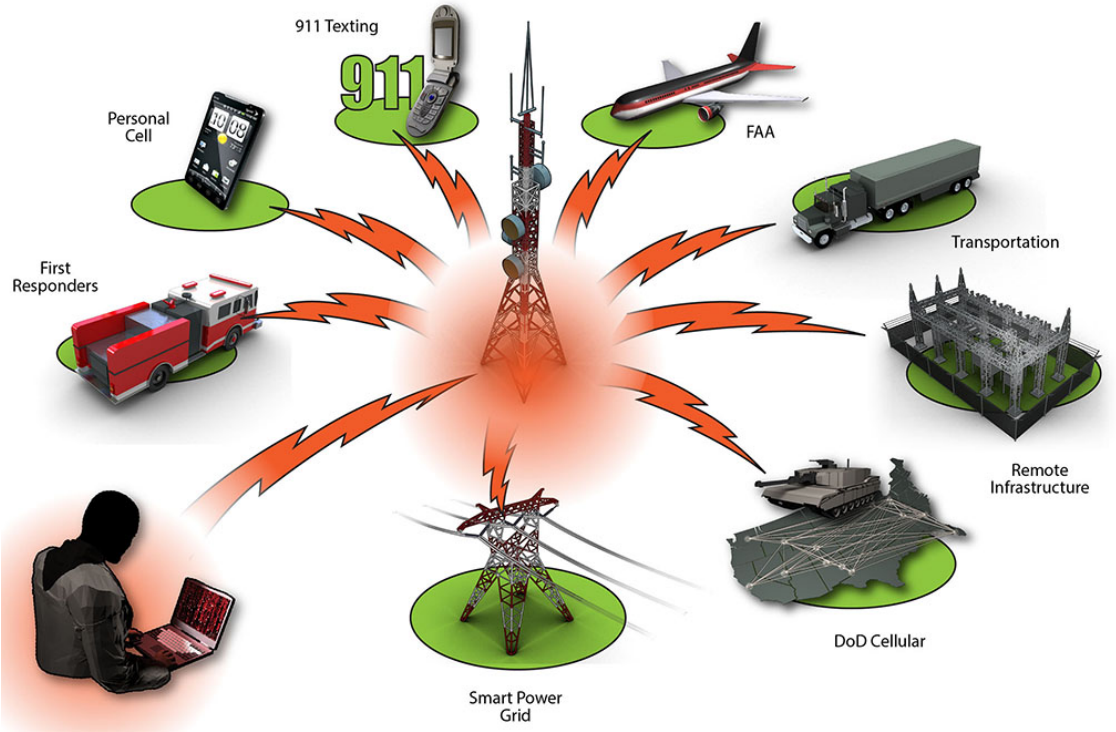
Daniel Devasirvatham
Director, WNUF
Idaho National Laboratory
Daniel.Devasirvatham@inl.gov
858-366-8994

Communications Impacts CI Sectors

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams & Bridges
- Defense Industrial Base
- Emergency Services
- Energy and Water
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials and Waste
- Transportation Systems
- Water and Wastewater Systems

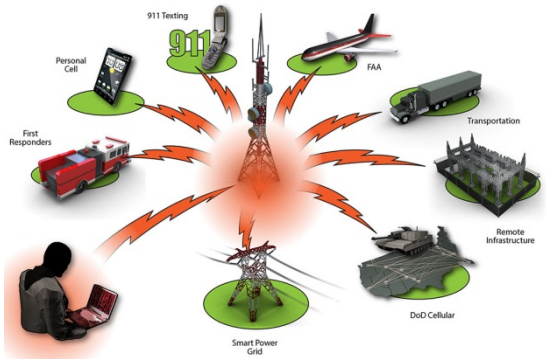
Potential Wireless Security Targets

- **Wireless is ubiquitous**
- **Wireless protocols often easier to compromise**
- **Many types of systems are hence vulnerable**



Wireless and Critical Infrastructure

- **Critical infrastructure control is going digital**
  - SCADA, M2M, Smart Grid, Water storage and delivery
  - Communications is key to benefit (Generation<->Load, etc.)
- **Network connected for updates/maintenance**
- **Latent Communications in well guarded systems**
  - Sometimes enabled with a software change
- **Once in, damage is unpredictable**
  - Can often hopscotch from system to system

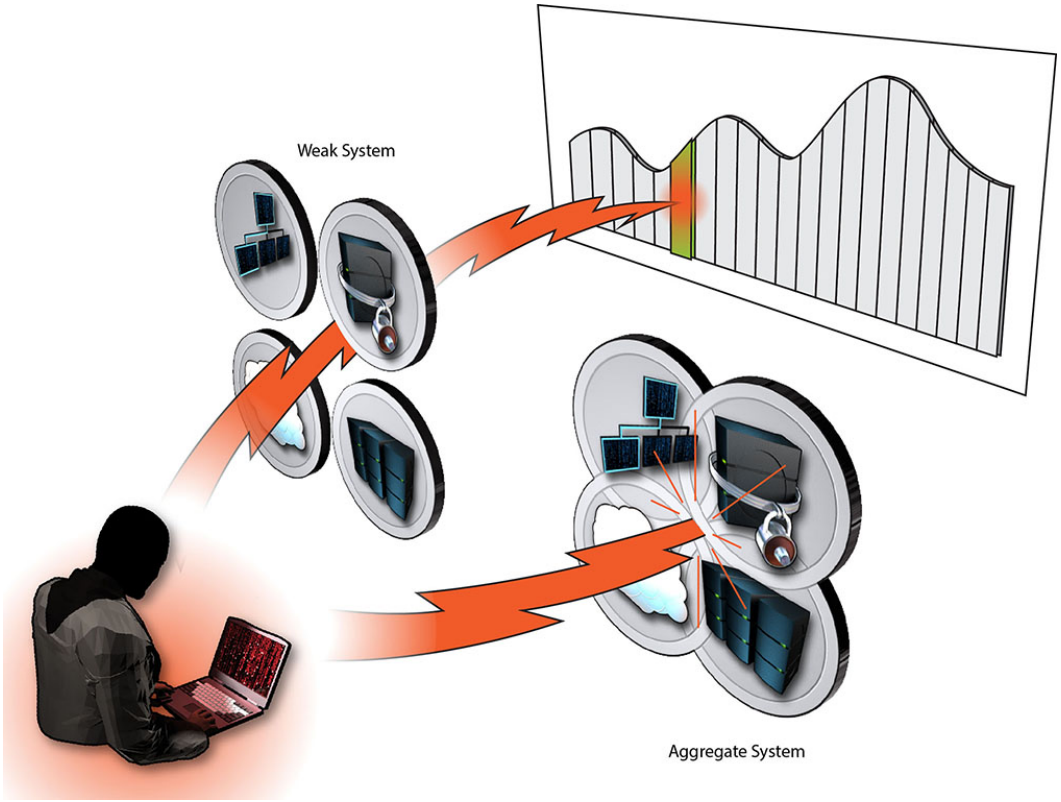


Spectrum Sharing Adds Complication

- **Spectrum sharing used to get access to spectrum**
- **May run into capacity limits. Hence-**
- **Get aggregate multiple data streams for capacity**
  - Data Stream Aggregation
  - Each stream in a different channel
- **Each channel may use a different protocol**
  - TD-LTE, FD-LTE, WiFi, etc.
- **This is different from channel aggregation**
  - Different channels used together, but with common protocol

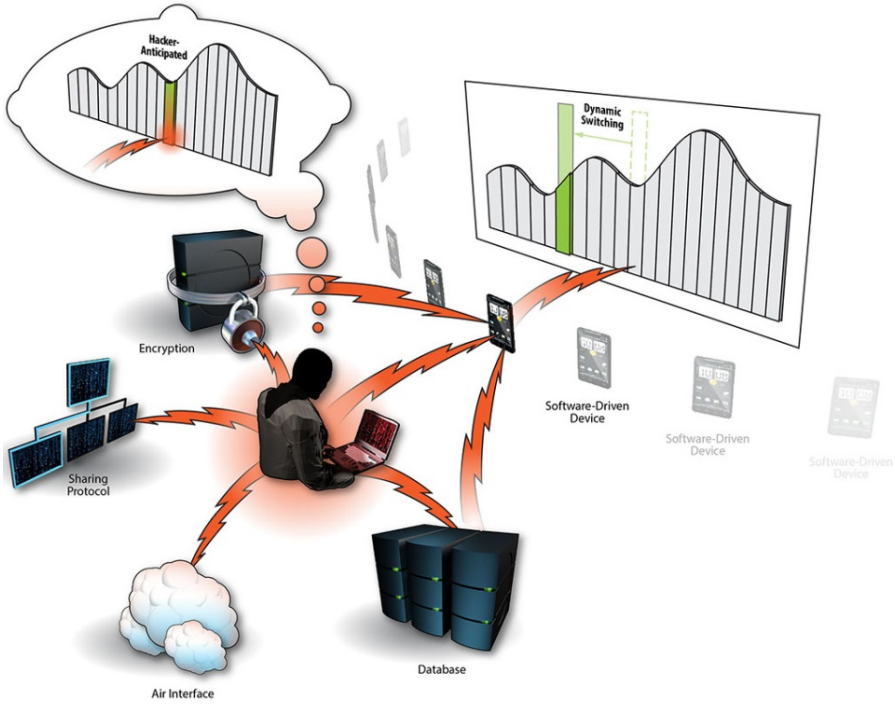
Weak Link Compromises Aggregation

- **Spectrum sharing may use data aggregation**
- **The weakest protocol compromises the whole**



Dynamic Sharing: Strength/Weakness

- **Measurements for dynamic spectrum sharing (DSS) differ at user and attacker locations**
- **Hence, attacker can guess wrong: More secure**
- **However, sharing databases could be weak point**



Security in DSS

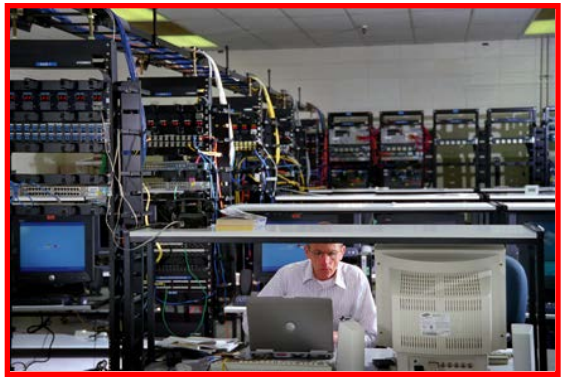
- **DSS requires secondary user jump in/out of shared spectrum**
  - Use spectrum when primary system releases it
  - Release spectrum when primary system needs it
  - Limited amount of raw bits over active link
  - Hence limited amount of bits for encryption
  - Long encryption keys are secure for longer time
  - Often RSA protocol with long keys and key exchange
    - KEK, TEK, etc
    - Key Exchange in public key systems?
  - Can this be leveraged/modified for spectrum sharing?

Practical Security in DSS

- **“Practical Security concept ”**
  - Security/Encryption only strong enough to protect link for the limited sharing time
  - Makes more bits available for user data
- **Some social messaging APPs may leverage this**
  - Short message bursts do limit security constructs
- **Spectrum sharing ideas and equipment proposed**
  - Most of them do not seem to include security
  - Yet may have used up about 50% of the raw bits
  - Unless security is built into the protocol, more bits needed

Communications Security / CERT

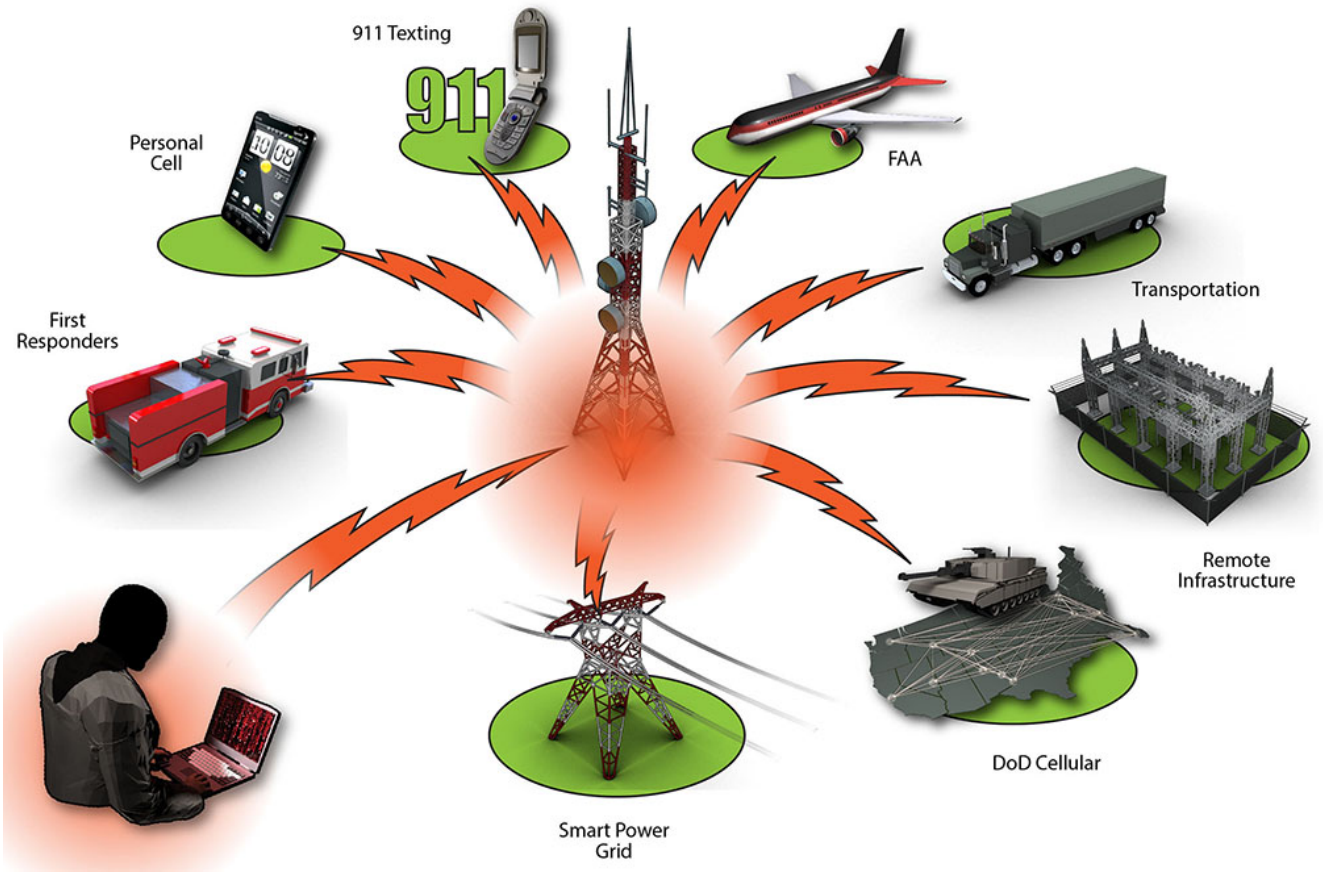
- Malware Lab
- Cyber Security Assessments on Comms & Control Systems
- Zero Day (New) Exploits
- Protocol Analysis
- Partial Code Review and Reverse Engineering
- Component Firmware and Embedded Devices
- Wireless Protocol Security
- IDS Review, Testing, Configuration and Design
- Forensics Review Recommendation for Implementation
- Controlled Information Sharing and Demonstrations
- Security Training



Summary

- **Wireless spectrum congestion/ underutilization is driving spectrum sharing**
- **Raises several unique security challenges**
  - Many different systems are vulnerable
  - Data aggregation for added throughput adds issues
  - Dynamic spectrum sharing has different security
- **Secure encryption more difficult with DSS**
  - We suggest Concept of “Practical Security Protocols”
  - Only sufficient to protect link while active.
  - Restart for next burst
  - Build security into spectrum sharing protocol design tradeoffs
- **Need attack monitoring, forensics & mitigation**

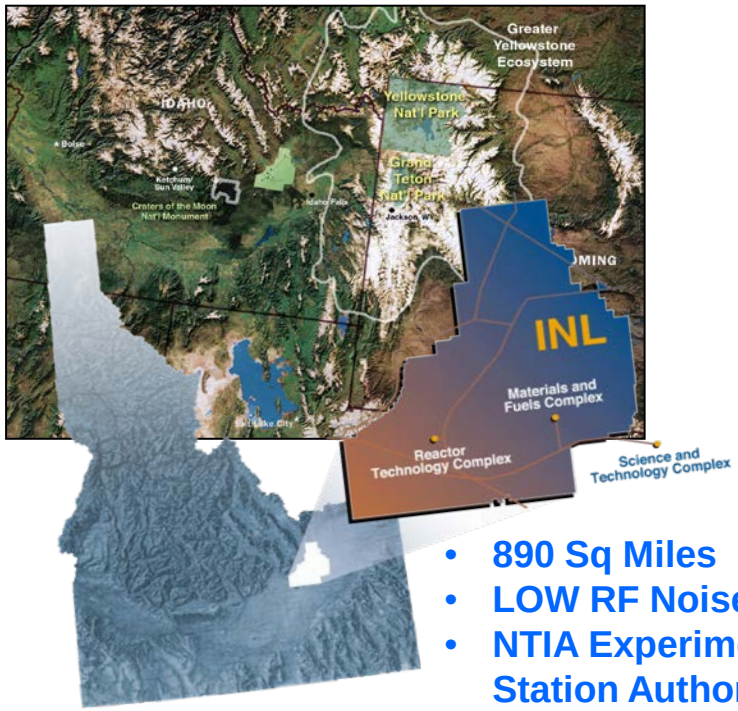
Security is Serious



Remember this Guy

Wireless Test Bed: Assets Capabilities

- **Engineering, Research Capabilities**
  - Live and simulation experimentation environments
  - Experienced research staff
    - Spectrum sharing hardware and software
    - Network implementation and control
    - Sensors and applications development
    - RF, Situational Awareness & Critical Infrastructure Protection modeling and simulation
    - Cyber engineering / reverse engineering / vulnerability assessments
  - Assembly & integrated technology level testing for conceptual, developmental, operational requirements
- **Existing Wireless Infrastructure:**
  - Outdoor (8 fixed and multiple mobile): HF/VHF/UHF/SHF
  - GSM, UMTS, CDMA, WiMAX, WiFi, HF, LMR
  - SONET, VSAT Satellite systems
  - UAV and UGV test areas
  - Mountain top line-of-site access
  - Indoor: DSA platforms, Anechoic isolation chambers



- **890 Sq Miles**
- **LOW RF Noise**
- **NTIA Experimental Station Authority**

- **Established Services & Processes:**
  - Spectrum approval & monitoring
  - Safety, Medical, Fire, Security (physical)
  - Resource management - personnel, networks, configuration control
  - Secure, IP protected multi-user facility

Test in a Safe Place

Dr. Daniel Devasirvatham

- Director,
  Wireless National User Facility
- Idaho National Laboratory
- (208) 526-4600
- Daniel.Devasirvatham@inl.gov