

Spectrum Sharing and Critical Infrastructure Protection:

Opportunities and Challenges

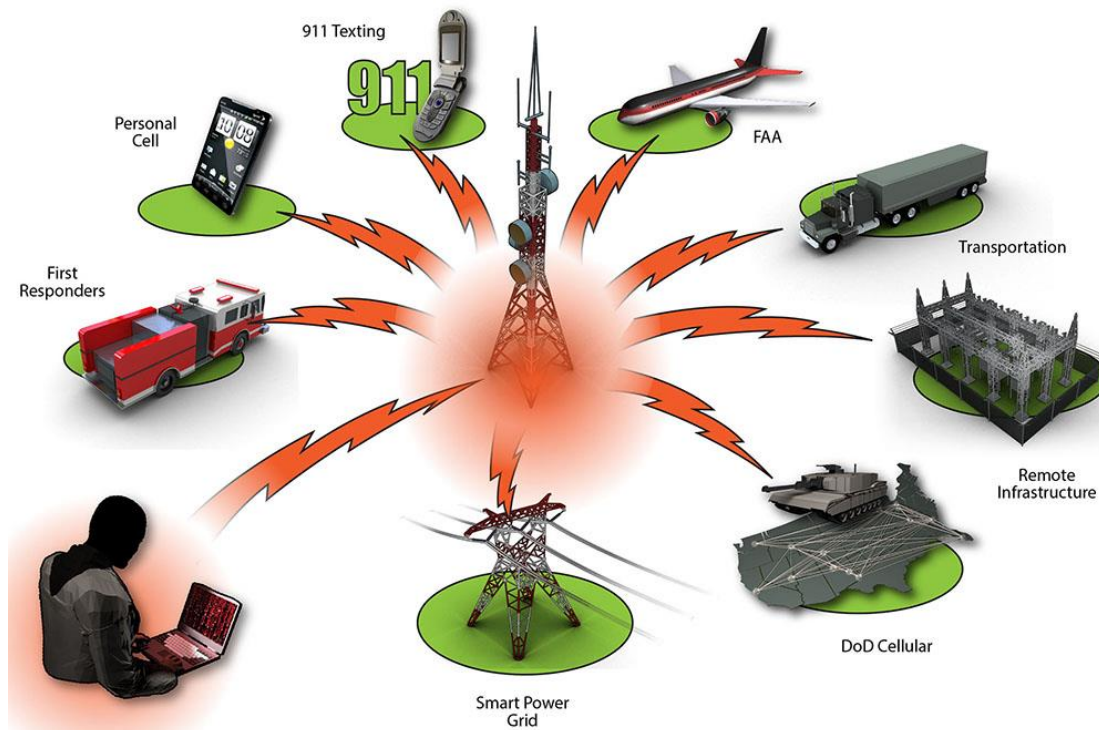
Daniel Devasirvatham
Director, WNUF
Idaho National Laboratory

Daniel.Devasirvatham@inl.gov

858-366-8994

Potential Wireless Security Targets

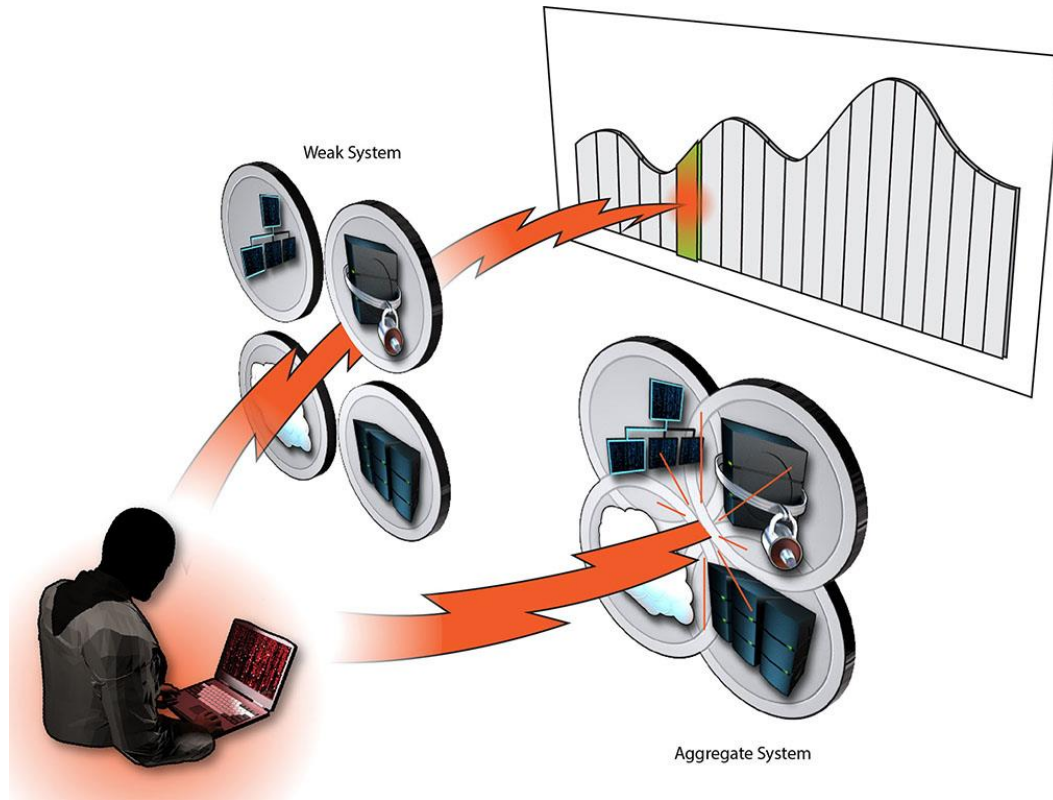
- **Wireless is ubiquitous**
- **Wireless protocols often easier to compromise**
- **Many types of systems are hence vulnerable**



Slide 2

Weak Link Compromises Aggregation

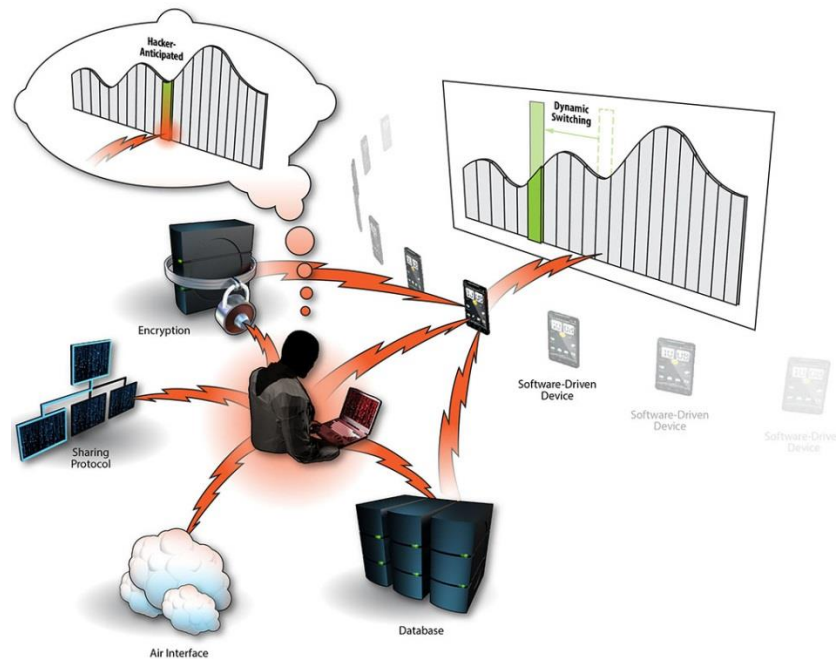
- Spectrum sharing may use data aggregation
- The weakest protocol compromises the whole



Slide 3

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



Slide 4

Practical 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
- **“Practical Security concept ”**
 - Security/Encryption only strong enough to protect link for the limited sharing time
 - Makes more bits available for user data

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 could strengthen 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