Information Assurance Considerations For Lightweight SDRs and Systems

Paul A. Philip, US Department of Defense
Mark Buckner, Oak Ridge National Laboratory
Michael Moore , Oak Ridge National Laboratory

Software Defined Radio Forum Technical Conference
1-4 December 2009

Outline

- Why Worry?
  (…about Information Assurance)
- Software Defined Radio Basics
- Example SDR-Based RFID System
  - ORNL Prototype Logistics Tracking / Sensing System
- Device Security Issues
- RF System Security Issues
- SDR Information Assurance Summary

Why Information Assurance?

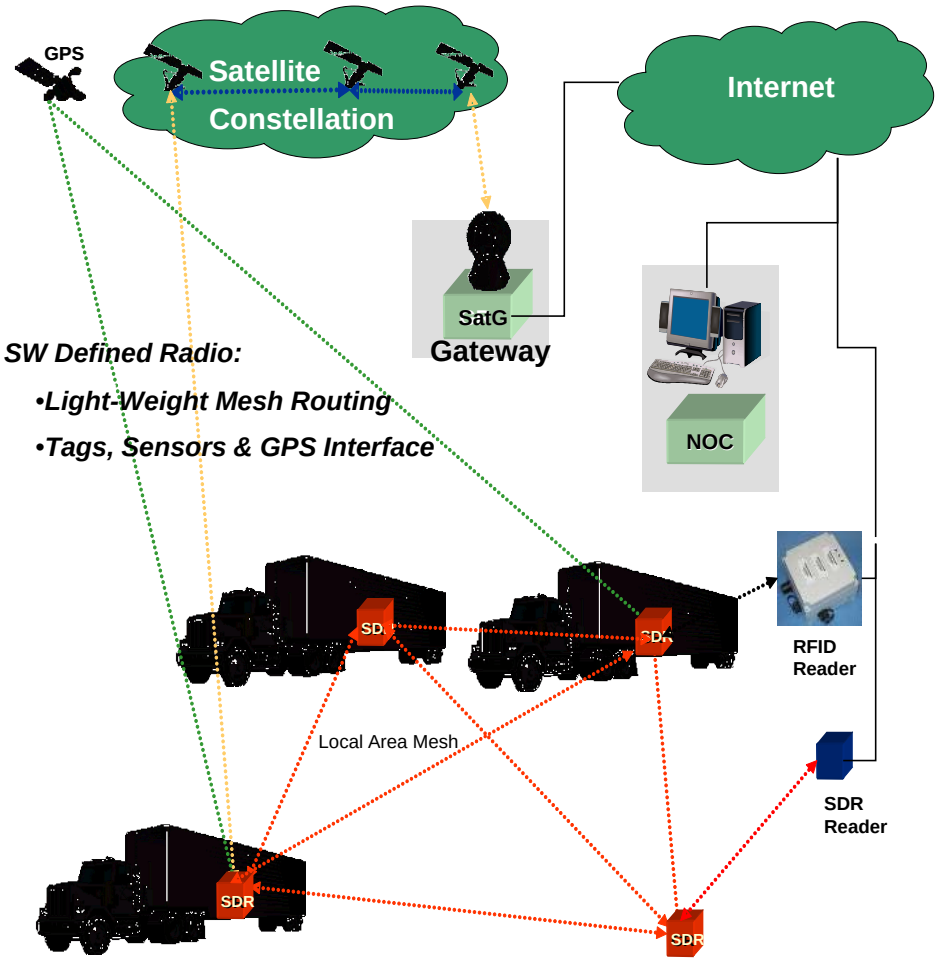
- Commercial and Industrial Systems
  - Proprietary Data, Patient / Customer Privacy
- Government Systems
  - Valid Identification / Access
    - Electronic Passports / PASS Card, TWIC
- Military
  - OPSEC: Location, Tactics, Troop Strength, Timetables
  - Accurate Data
- Who is Interested?
  - Organized Crime, Intelligence Organizations, Terrorists
  - Industrial Espionage, Hackers, Competitors
- Value of Data Drives Threat / Protection
  - Guidance: American Bar Association, NIST, NSA

aRFID SDR Basics

- Software Defined Radio-
  Reconfigurable Hardware Radio Platform
  - Programmable DSP Cores
  - Computing, Communications, Sensing / Response
  - Multiple Stored Radio Waveforms
  - On-the-Fly Waveform Switchover, Reprogramming
  - Over the Air Software Upload
    - New Waveforms, Operational Control
- ORNL aRFID System
  - SDR Capability
    - Lightweight Computing, Small Form-Factor
    - Software Upgradeable aRFID Reader Nodes
    - Processing: GPS, Sensors, Multi-path, Security (Future)
  - Waveforms
    - SATCOM Reach-back
    - SDR Node-Node Ad Hoc Routing
    - RFID Waveforms (WhereNet, et al)

aRFID System

- SDR Reader Nodes
  - Inter-Node Mesh Routing
  - Communications <> Satellite
- Downlink Control
  - RFID Reader Commands
  - SDR / Network Control
- Uplink Data
  - RFID Tags
  - Environmental Sensors
  - GPS Location Data
- Network Operations Center
  - Net / Gateway / SAT Link
  - Link to Terrestrial Readers



Device Level Vulnerabilities

- RFID Tag and SDR Node
  - Tamper / Substitution→ Masquerade
  - Hardware Reverse Engineering (HRE)
  - Side Channel Attacks (Including RF)
  - Skimming, Eavesdropping
  - All → Cloning / Counterfeiting
    - Obtain Access to the Network
- SDR Node
  - Malicious Over-the-Air Software Uploads
    - Malcode Insertion
    - Corrupt SDR Configuration & Cognitive Decision Data
  - Software / Hardware Development Process
    - Products and Tools (Auto-Code Generators)

Device Level Countermeasures

- Tamper Penalty for Penetration or Removal
- SDR Node Specific
  - CMMI Level 3 Development Process / Environment
  - Anti-Side Channel, Anti-HRE Design
  - Secured Audit Log
    - Pedigree of Software Updates, PKI Certificates
    - Retain Security Events and Cognitive Decisions
  - Secure OTA Transactions
    - Kerberos (Singh, et al) / NSA Suite B Authentication
  - Encrypt and Distribute Sensitive Data
    - Device Configuration, Waveforms, Audit Log
    - Cryptography: Keys, Certificates, Algorithms
  - Integrity Check Critical Data
  - Validate Internal Commands

Radio Frequency Link Vulnerabilities

- SDR Node-to-Tag Air Gap
  - Jamming
  - Increased RF Range / Exposure
  - Eavesdropping
    - Sensitive Data Acquisition, Geo-Location of Nodes
  - Skimming
- Wireless Network Vulnerabilities
  - Masqueraded Network Device
    - Session Highjacking, Man-in-the-Middle, Device Spamming
  - RF Traffic Analysis
    - Transmit Timing, Duration, Traffic Volume
  - Digital Traffic Analysis
    - Packet Sniffing to Enable Masquerade Attacks

Radio Frequency Link Countermeasures

- Minimize Signal Exposure
  - Encryption
  - Oxygen Absorption Spectrum (Cal Berkeley)
  - Faraday Anechoic Enclosure
  - Narrow Beam, Limited Power, Repeaters
- Adaptive Anti-Jam
- Transmission Security (TRANSEC)
- Protect the Network
  - Mutual Authentication between All Devices
    - Valid Credentials Defeat Masquerading & Skimming
  - Encrypted Data Exchange
  - Point to Point Integrity Checks
  - Proxy / RF Firewall Front End
    - Intrusion Detection / Prevention (Audit Log Security Events)
  - MetaData Balancing
    - Vanilla Packets: Timing, Length, Header, Packet Type

SDR Information Assurance Summary

- RF Increases Exposure to Threats
- Security Commensurate to Risk
- Raise the Bar with Multi-Layered Security
- Utilize SDR Processing Power
  - Encrypt / Distribute Sensitive Internal Data
  - Maintain (and Protect) Audit Log
  - Ensure Availability (Anti-Jam)
  - Protect Transmissions (TRANSEC)
  - Secure All OTA Transactions
  - Secure the Network

Questions?

“Having listened to your lecture I am still confused,
but on a higher level.”
Enrico Fermi

Paul Philip	***p.philip@radium.ncsc.mil***
Dr. Mark Buckner	***bucknerma@ornl.gov***
Michael Moore	***mooremr@ornl.gov***