RFID Safety and Security Applications and Issues in Transportation

Carl Kain, PE
Mitretek Systems
TRB/USDOT RFID Planning Conference
La Jolla, CA, July 7, 2006

Introduction

- Safety and security are a “two edged sword” in RFID
- RFID can be used to implement safety and security applications for transportation
  - HAZMAT tracking, shipping container tamper detection
- RFID can also create a safety or security risk
  - Unauthorized party can read a tag: identify item worth stealing
  - RFID tag can be used for unauthorized tracking
- RFID systems for security and safety applications need information security
  - Tags can be cloned, counterfeited
  - Accountability and tracking can be spoofed
  - Attacks on safety systems (man-in-middle, denial of service) can make safety applications very dangerous!
- Briefing will address both definitions since research is ongoing/needed

RFID Security Applications Definition

- Security refers to the real time visibility of assets
  - Tracking, identifying tampering
  - Keeping record of assets: where they are stored, what is stored, everything is accounted for
- RFID as part of a system can provide security
  - RFID, sensors, electronic seals, and wireless communications to monitor and track assets in real time
  - Couple with GPS and alarms if items are moved without authorization or tampered with
  - Can search/locate specific item (everything from a pallet to a railroad car)

Sample RFID-Based Security Applications

- Tracking, monitoring and reporting systems for HAZMAT, high risk items
  - Locate items
  - Tamper detection and reporting
  - Unauthorized movement
- Inventory control and reporting of high risk materials
- Customs and border crossing for individuals
  - Secure Electronic Travelers Rapid Inspection (SENTRI)
    - Pre-screened travelers cross Mexican border in dedicated lanes using RFID tag-enabled ID card
  - NEXUS program
    - Pre-screened travelers cross Canadian border; NEXUS ID card has embedded RFID chip; dedicated lanes, marine program for boaters in development
- Customs and border crossing inspections and procedures for shipping/freight

US Government Encouraging RFID-Based Security Applications

- Customs-Trade Partnership Against Terrorism (C-PTAT)
  - DHS program, voluntary (for now…)
  - Addresses supply chain and cargo security; customs and border crossings for cargo
  - Participating companies receive reduced inspections and expedited border crossings
- DHS Supply Chain Security Best Practices Catalog addresses RFID as acceptable solution to comply with C-PTAT requirements
  - RFID and electronic seals can be used to manage inventory discrepancies, manifest and invoice information at distribution center
  - RFID-based electronic tracking can be used for compliance

RFID Security Applications Issues

- RFID technology needs to be compatible among carriers, trading partners involved in shipping and transport
  - Need for standards and interoperability
  - Standards are developed for different features of RFID including air interfaces, transmission protocols, data syntax, structure, and encoding, test methods
  - Standards may be optimal for certain applications and multiple standards may be necessary
- International harmonization of both standards and frequency allocations/regulations are needed for tagged assets that cross international borders
  - Includes pallets, containers, chassis, trailers, railroad cars etc.
  - Different Countries allocate different frequency bands and different regulations for RFID use
    - Affects range
    - Affects tag readability
    - Determines whether device can be used at all (tag can be in an unauthorized frequency band, power level, modulation)

Examples of Safety Applications

- Automotive anti-theft devices
- Tread Act for tires (Transportation, Recall, Enhancement, Accountability and Documentation) – mandates auto mfg. track tires in case of safety recall
  - Michelin using RFID to comply, also coupling with sensors to alert driver of unsafe tire condition
- Commercial vehicle mainline automated clearance
  - Transponder read at weigh station, automated check of size, weight, registration, safety records etc.
  - Sensors monitoring tire and brake condition, load shifting, etc. send information via RFID at weight/inspection station possible
- Traffic signal priority for emergency responders
  - Also used by public transit for schedule adherence

Sample Future VII Automotive Safety Applications (Using DSRC)

- Cooperative Intersection Collision Avoidance Systems (CICAS)
  - Stop sign violation
  - Traffic signal violation (active signal control option)
- Crash Avoidance Metrics Partnership (CAMP)
  - Forward collision warning
- Vehicular Safety Consortium (VSC)
  - Curve speed warning
  - Extended brake light
- Some additional “Day One Applications”
  - In-vehicle signing
  - Weather/Road condition
  - Emergency vehicle approaching

DSRC vs. RFID; a Brief Digression

- Research under VII project uses DSRC for communications from vehicle to roadside
- RFID uses tags (usually stationary or moving slowly) and readers, DSRC uses 802.11a-based modems (complex OFDM modulation) capable of implementing advanced applications to vehicles moving at 120 MPH.
- DSRC can incorporate applications formerly implemented with RFID
  - toll collection, CVO applications, traffic signal priority/pre-emption, traffic management
- DSRC will incorporate new functions with a communications distance up to 1 km at power levels, data rates, and travel speeds not achievable by RFID
  - VII safety applications, media and map downloads, in-vehicle signing, transit vehicle data transfer, emergency vehicle approach warning etc.

Major Differences Between DSRC and RFID

- Most RFID governed by Part 15 FCC Rules; multiple frequency bands
  - Limitation on transmission duration, transmitted power
  - Most readers do not require license
  - Tags are meant to be simple and inexpensive
- DSRC governed by Part 90 FCC rules; 5850-5925 MHz band only
  - ITS Radio Service, higher power, no limit on transmission duration
  - Data rates between 6 and 27 Mbps
  - Uses modems, not tags; capable of IP-based communications
  - All reader (RSU) locations are licensed
- RFID tags are passive or battery powered with 1-5 year lifetime
  - transfer limited amount of data, limited processing, memory
- DSRC modems will consume standard laptop battery in 1-2 hours
  - process and transfer significant amounts of data/messages, can be interfaced to on-board computer

RFID Information Security Needs

- Access control and data privacy
  - Prevent unauthorized party from reading tag
  - Prevent unauthorized tracking
  - Prevent tag cloning, counterfeiting
- Data integrity
  - Prevent unauthorized party from writing or altering data on tag
  - Prevent tampering
- Authentication
  - Prevent unauthorized party from operating device (e.g. anti-theft, toll collection)
  - Ensure reader is authorized, tag is authentic
  - Allow tag to be disabled, but only by authorized party
- Mitigate denial of service attacks, spoofing, other system threats
- Use good security schemes that are difficult to “crack”

Information Security Issues for RFID

- Most security requires cryptographic functions
  - Computational power of tags is extremely limited
  - Available power for tag is limited
- Information security features raise cost
  - RFID tags for some apps are useful if inexpensive and/or disposable
- Security can limit usefulness of tags
  - Cryptographic processing takes time, increases volume of data and reduces read rate
- Encryption can provide authentication, data protection, but key management can be difficult
  - Public key (asymmetric key) cryptography requires too much power, computation
  - Secret key management (symmetric) requires distribution, storage etc.
- Encryption not a cure-all
  - Unauthorized party may not be able to decrypt specific information, but can use signature to track items, obtain inventory count (consider shipments of military ordinance or HAZMAT)

What is Available in RFID Security?

- Blocker tag
  - Device developed by RSA Security Inc. for privacy
  - Passive device that simulates multiple Electronic Product Code (EPC) tags that effectively block reader from obtaining data
- Kill command
  - EPC tag can be “killed” (no longer respond to reader) when a kill command/PIN number are applied by reader
  - Only required feature on EPC tags, additional security is optional
- Challenge-Response authentication
  - Used in devices like toll tags, SpeedPass, electronic payments
- ACCESS command (optional in EPC standard)
  - ACCESS command +PIN = secure state
  - Only certain commands will function when in secure state
- Password protection for tag read
- FIPS Level 3 compliant tags
  - Tamper detection and data destruction

Beware Weak Security

- SpeedPass, automobile anti-theft devices use Digital Signature Transponder (DST)
- DST challenge-response protocol
  - 40 bit challenge
  - Response encrypted with 40 bit secret key, truncated to 24 bits, returned to reader
- Johns Hopkins University used modest resources (few hundred dollars) to crack and clone devices in about an hour.
  - Scanned briefly at short range, provided two challenges and obtained two responses
  - Cracked key
  - Made purchases at Mobil and started Ford vehicle with cloned devices

System Security – Beyond RFID

- RFID is only one component of system that needs securing
- Need to prevent introduction of malicious data into back-office
- Need to prevent access to back-office system, protect data bases, information collected from RFID
  - Some systems have web access (e.g. fleet management, tracking systems)
  - RFID provides “data”; valuable information may be in data base or application software that processes the data
  - Standard information security safeguards need to be applied to every system segment

Summary

- RFID can be a great enabler of applications to provide safety and security applications for transportation
  - Secure supply chain, multi-modal shipping
  - Secure customs and border crossing transportation issues
  - Provide new safety applications on highways
- RFID systems used in safety and security applications have potentially huge liabilities and must be secured
- Securing RFID is a challenge
  - Security drives device complexity and power consumption
  - Security costs money and may make system operation more difficult, important to keep the per-tag cost low
  - Important research area