Layerone / 2006
RFID – Technology, Security & Privacy

Luiz Eduardo Dos Santos, CISSP
luiz AT arubanetworks.com

What are we talking about today?

- RFID history
- Technologies
- WiFi tags
- Privacy/ Security

Who am I?

- Networking guy
- Security guy
- Aruba's WSIRT Incident Manager
- Speaker at some conferences
- WLAN at Blackhat, DEFCON & CCC

What is RF-ID and why?

- Radio Frequency Identification
- “Derived” from the IFF (Identification Friend of Foe) transponder, used in World War II
- 1945, the Soviet government used a passive covert listening device which retransmitted incident radio waves with audio information
- First commercial use in 1976
- Anti-theft tags
- Inventory control (barcode replacement?)
- Detect misplaced products and expired goods
- Tracking and identifying “everything”

RFID “Components”

- Tags (also known as transponders), can be active, semi-active and passive
  Frequencies used can be: LF, HF, UHF, uW, GPS)
- Readers (transceiver)
- Back-end systems

More about tags

- Up to 1000 write cycles (some are read only)
- Some have some sort of write protection
- Each tag carries an unique identifier
- WiFi tags are programmable by the RTLS
- Some newer WiFi tags have a built-in crypto accelerator

Myths

- RFID will replace barcode
- RFID is just a “talking” barcode (nope, up to 2kB of info)
- Tags can ONLY (and are intended) to be read at relative short distances *

RFID technologies & applications

- Used to locate mobile items
- Two different technologies
  - Wi-Fi Tags
  - UHF 'RFID' passive tags
- Differing range, cost, capabilities

UHF RFID tags work at 915 MHz.
They are inexpensive,
usually passive (no batteries)
but very short-range

UHF RFID tag applications

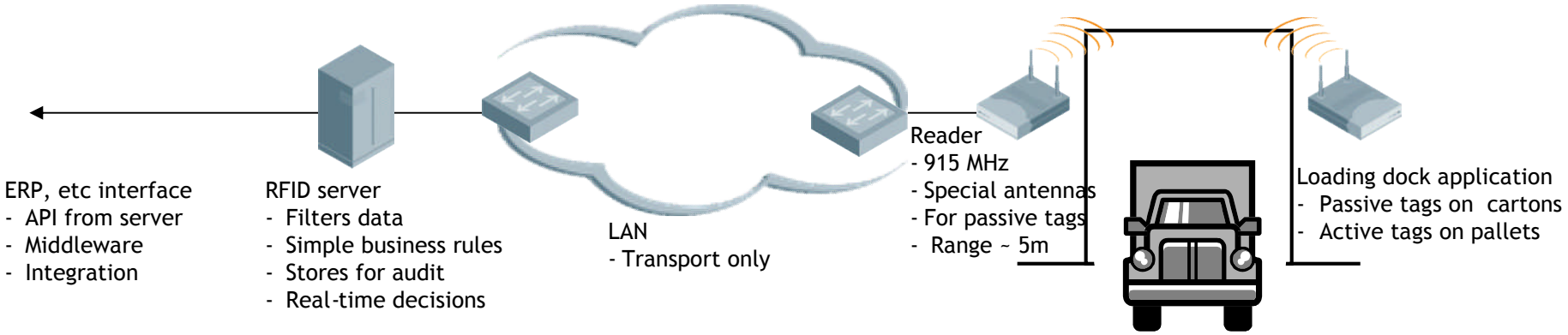
•Wholesale/retail distribution chain
•Carton-level tagging through the supply chain (groceries)
•Item-level tagging of high-value items (razor blade packages)
•Real-time checking of truck loading
•Homeland security implications of an audit chain for foodstuffs
•Manufacturing
•Potential to replace bar-codes

Wi-Fi tags work at 2400 MHz.
They are expensive,
active (batteries with relatively short life)
and longer-range

Wi-Fi tag applications

•High-value mobile equipment
•IV pumps & other equipment in hospitals
•Patients in hospitals
•Manufacturing (aero engines)
•Shipping industry (rail cars, shipping containers)
•Identify IT equipment in server farms
•Locate mobile equipment for on-site maintenance

RFID technologies – UHF



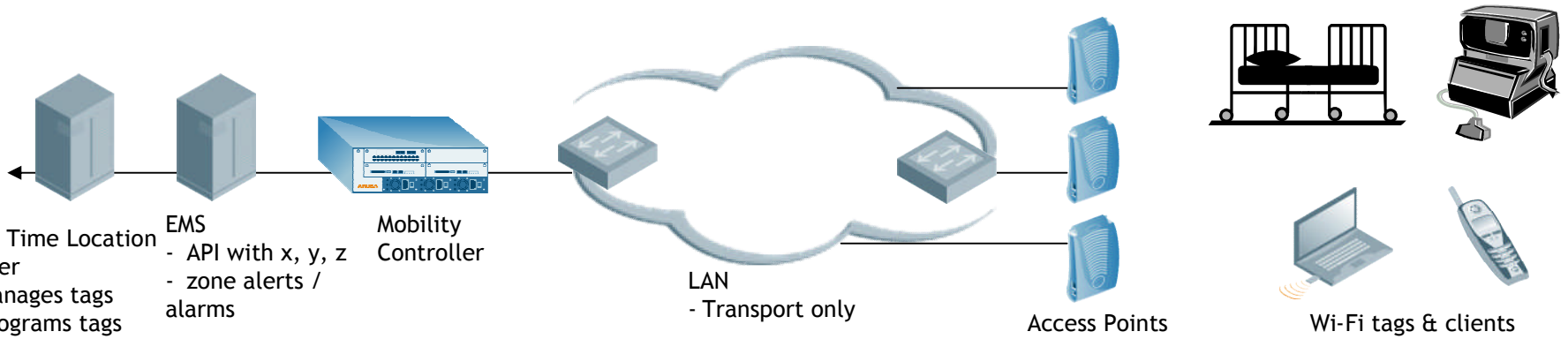
Technology

- Passive tags
  - Low-cost
  - Low-complexity
  - Carry UPC-like information
- Radio requirements
  - 902-928 (915) MHz
  - RF transmissions excite tags
  - Tags return information to reader
- Traffic characteristics
  - Many transactions, little data per transaction
- Back-end integration requirements
  - ERP & business systems integration

Characteristics & Issues

- Cost of tags (~50c but still too high)
- Cost of readers (~$1000 installed)
- Short range of detection (~2 meters)
- Not re-programmable
- Duplicate reads
- Missed reads & RF coverage holes
- Detecting vector motion (direction through a doorway)
- Management, coordination of many readers
- Middleware & ERP integration
- Immature technology – emerging reader architectures
- Business case difficult

RFID technologies – Wi-Fi Tags



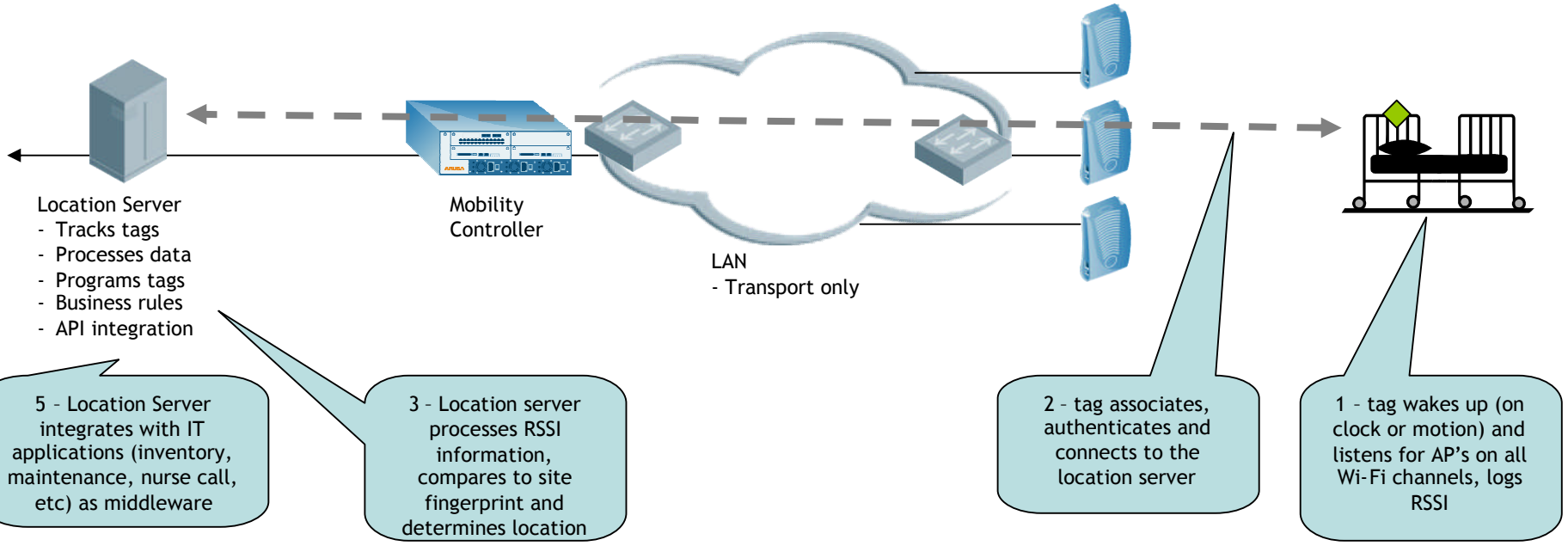
Technology

- Wi-Fi tags
  - High-cost
  - High-complexity (tag provisioning)
- Radio requirements
  - Wi-Fi
  - Association or 'Blink' (clock, motion, etc)
  - Longer range than UHF: 20+ meters
- Traffic characteristics
  - Few transactions, "larger" data sets (60 bytes data chunks)
  - RSSI from different BSSIDs
- Back-end integration requirements
  - Usually standalone business-rules engine
  - Any Wi-Fi client can be tracked, located
  - RTLS will generate alerts, reports, etc

Characteristics & Issues

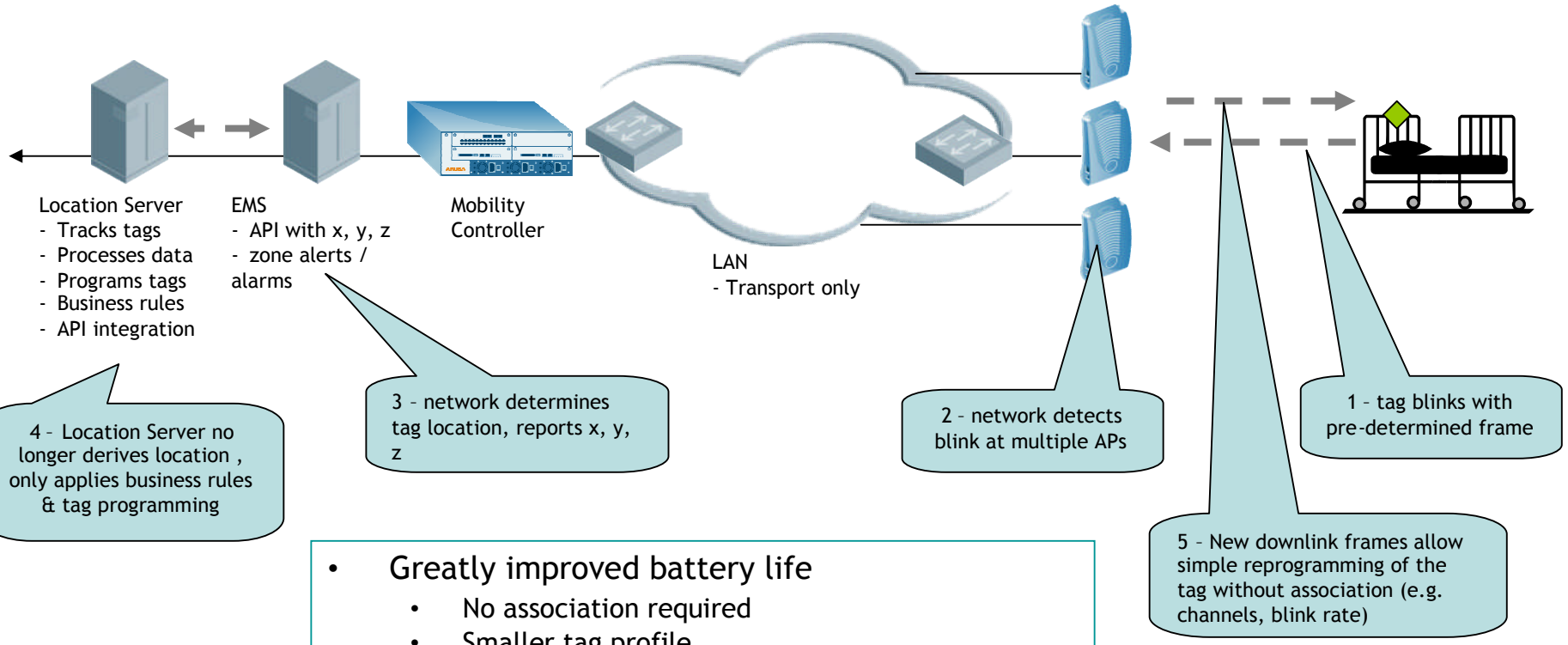
- Use existing WLAN infrastructure
- Cost of tags (~$50)
- Range (~ 30 meters)
- Lack of standards
- Battery life (~1 year) (depends on scan rate)
- Number of servers, complexity of administration
- Middleware, business rules integration
- Opensystem & WEP (now 802.11i)
- Some support multiple SSIDs
- All calculations done in the RTLS
- Ability to track any WiFi device

First-generation Wi-Fi tags



- Operates as an overlay over the WLAN infrastructure
- Requires long transmit times
  - 802.11 association for every transmission
  - Rather poor battery life
  - Large tag profile

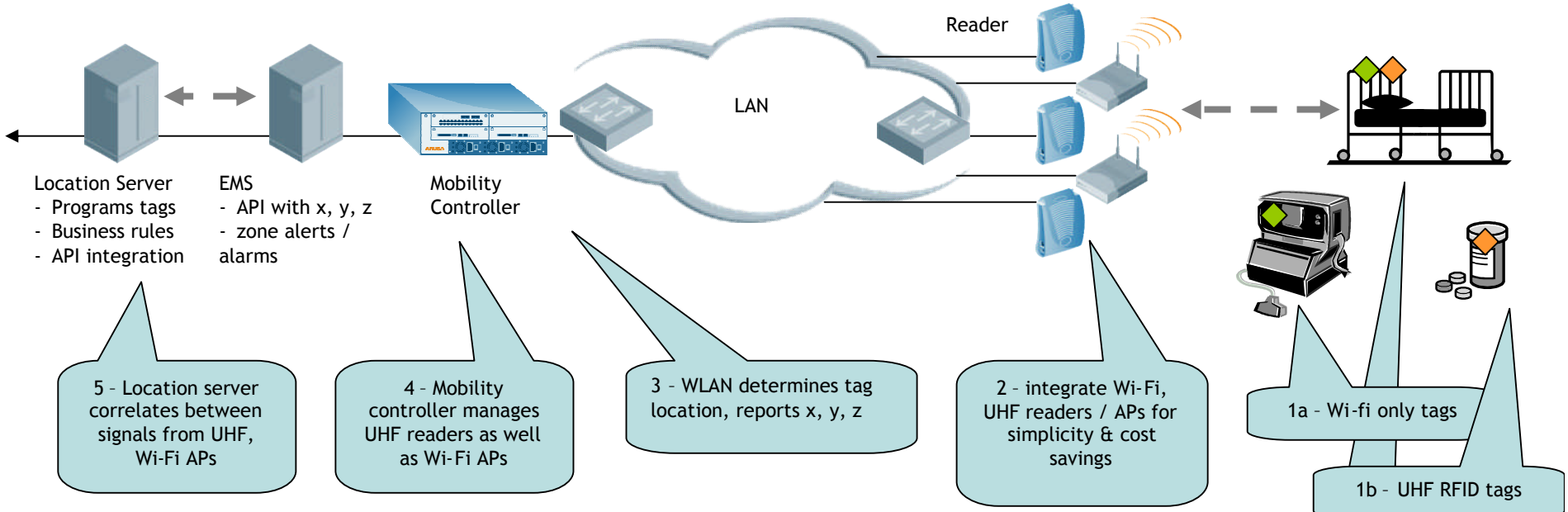
Second-generation Wi-Fi tags



- Greatly improved battery life
  - No association required
  - Smaller tag profile
- Simplified Location Server
  - WLAN infrastructure provides xyz on API
- Standardization opportunity
  - Mix-and-match tags & Location Servers & WLANs

Future Generations of RFID

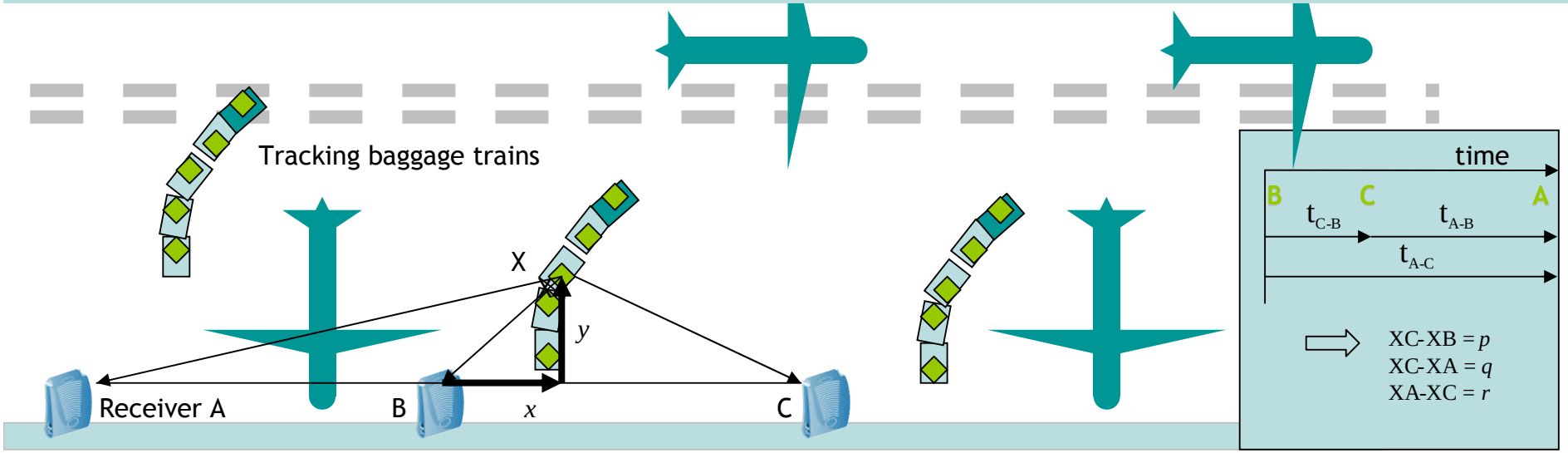
Several opportunities for integrating infrastructure and technology



- Multi-technology network
  - Single mobility controller architecture for UHF readers, Wi-Fi APs
- Multi-technology tags
  - Wi-Fi for range, UHF/Bluetooth for proximity
  - Expense constraints
- Unified Location Server
  - Single server handles UHF & Wi-Fi & combination tags

TDOA Location Technologies

Use standard Wi-Fi tags, but require special receivers: good outdoors



- TDOA (Time Difference of Arrival) accuracy is constant (dependent on the accuracy of time measurement, 1ft/nsec)
  - Accuracy of 10nsec is 10ft, regardless of distance measured: 10ft whether the measurement is 60ft or 180ft
- RSSI accuracy is proportional to distance
  - 25% of 60ft is 15ft, 25% of 180ft is 45ft
- Outdoor usually means long distances from tag to AP, so TDOA is often preferred
- TDOA technology requires special receiver hardware today
- Combined Wi-Fi AP with TDOA receivers are available, but expensive
- Mobile RF obstacles (e.g. planes, catering trucks) create shadows & multipath, so accuracy can vary
- Shadow, multipath effects may affect RSSI more than TDOA

(some of) Today's RF-ID Applications

- Inventory control (product tracking)
- Human and animal implants
- People tracking (parks/ clubs)
- Car keys
- Access control (badges)
- Luggage tracking
- Passports / immigration documents
- Customer loyalty cards
- Toll collection
- Libraries
- Exxon's Speedpass
- Cattle tracking

“New” RF-ID Applications

- MP3 player with smartcard
- Clothing
- Vending machines
- Casino chips
- Cellphones

Future RF-ID Applications

- Home appliances (refrigerators, washers, “smart” ovens)
- Money
- Smart paper (books, business cards)
- Sports
- And many more to come...

Security Concerns (RFID in General)

- No (or weak) encryption (overhead)
- User data memory can be modified
- No read protection *
- No “scanning” protection

Privacy Concerns

- Eavesdropping (customer AND business privacy issues)
- “better” customer profiling
- Possible person identification (when the tag has no read protection)
- “hotlisting” based on products you are carrying (books, etc)
- Collection and use of PII (personally indentifiable information)
- 21st century dumpster dive

Possible Solutions

- Kill the tag once it leaves the store
- RSA's blocker tag
- Lock unused memory on the tag
- Encryption? Overhead? ...

Hash lock access control

Attacks

- RF-Dump
  manipulates user data on the tag
- Tag swapping
- Convert products EPCs
- RF-ID Bombs

WiFi Tags Security Concerns

- Well, same concerns as you would have in any WLAN environment
- So, almost... What's new? The new components
- "Rogue" RTLS
- Spoofed tags
- Packet injection to confuse the RTLS
- And so on....

Resources

- http://www.rf-dump.org/
- http://www.spychips.com/
- http://www.nocards.org/
- http://www.rfidjournal.com/
- http://www.boycottgillette.com/
- And, well .. http://www.google.com

Done

- That’s all!
- Questions?

Thanks!

luiz AT arubanetworks.com
le AT wlansec.org