



Privacy and Opportunity in Passive RFID:
Authentication and Identification Using CDMA
May 1, 2006

Daniel D. Deavours, Weichao Wang,
and Shannon D. Blunt
ITTC, University of Kansas
deavours@ittc.ku.edu



Who We Are

RFID Alliance Lab

- ◆ Evaluate RFID products in a *scientific* way
- ◆ Provide useful, timely, credible, and unbiased data to end users of RFID products
- ◆ Constituents
 - ◆ **University of Kansas / ITTC:** Primary research contributor
 - ◆ **RFID Journal:** Initial funding, distributor, advertisement
 - ◆ **Rush Tracking Systems:** Initiator, industry lesion
- ◆ Business model
 - ◆ Sell reports (~\$1,000 / report) to finance future reports
 - ◆ Sponsorships

ITTC/KU Applied Research Labs

- ◆ Helping companies solve hard problems
 - ◆ Tagging small electronics devices
 - ◆ Seknion: direction of travel through portal
 - ◆ Tagging metal assets
- ◆ Adamas: high performance low profile metal tag
- ◆ Basic research
 - ◆ RFID privacy using CDMA
- ◆ We would like to talk with you about your hard problems



RFID: Now and Future

- ◆ Readers presently
 - ◆ Readers expensive
 - ◆ Independent
 - ◆ Portal applications
 - ◆ Identifying
- ◆ Tags presently
 - ◆ Copper/Silver + silicon tags
 - ◆ Tag cost: ~\$0.15
 - ◆ Millions of case & pallet tags
 - ◆ Targeted for ROI
 - ◆ Supply-chain focus
 - ◆ Little to no privacy
 - ◆ Increasing complexity
- ◆ Readers in 5-10 years
 - ◆ Readers \$50
 - ◆ Single MIMO system
 - ◆ Monitoring applications
 - ◆ Identifying + positioning +
- ◆ Tags in 5-10 years
 - ◆ Completely printed tags
 - ◆ Tag cost: \$0.01
 - ◆ Billions of item-level tags
 - ◆ Ubiquity maximizes ROI
 - ◆ After-sale focus
 - ◆ Privacy imperative
 - ◆ Decreased complexity



RFID Future Use Case(s)

- ◆ The future, ubiquitous RFID world will be fundamentally different from present
 - ◆ Constant monitoring more than portals
 - ◆ Consumer-driven (individual, corporate) surpassing supply chain
 - ◆ If there is ROI for retailers detecting out-of-stocks and maintaining proper inventory, what about insurance companies?
- ◆ This implies a fundamentally different use case
- ◆ Privacy becomes **first class** design constraint

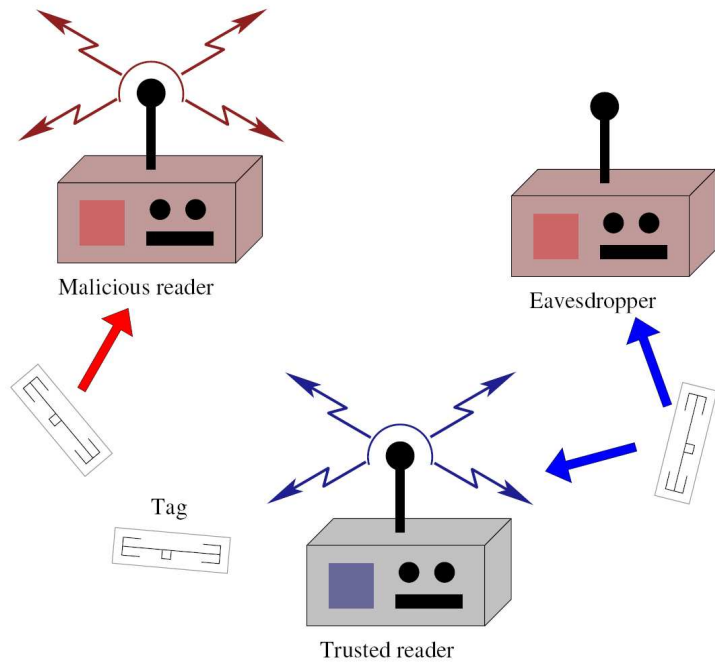


Solution

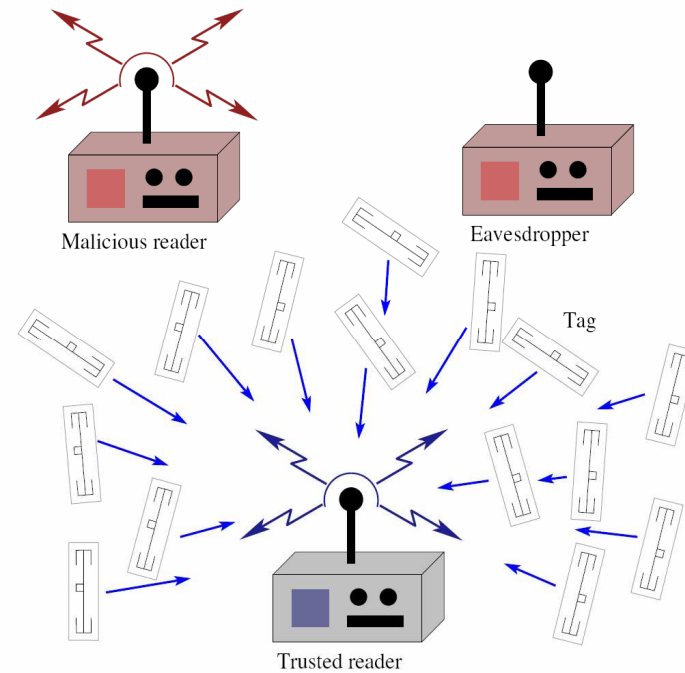
- ◆ Motivate consumers to *want* RFID-enabled products
- ◆ Remove barriers to acceptance
 - ◆ Perception is reality
- ◆ Be perceived as working *for* consumers
 - ◆ Not your bottom line
 - ◆ Not for “big brother”
- ◆ Enable RFID systems for high levels of privacy for after-market use



Paradigm Shift



Current paradigm: few, high speed devices, high SNR signaling, complex TDMA control, little security, and no privacy.



New paradigm: numerous, low data-rate devices, low SNR signaling, simple CDMA access, highly private.

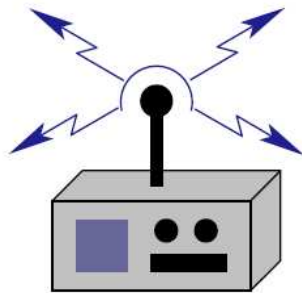


Approach

- ◆ R => T: authenticates sending clear-text
- ◆ T => R: all tags respond
 - ◆ Tags lacking authenticate send random response
 - ◆ Adds noise
 - ◆ Helps thwart brute force attacks
 - ◆ Authenticated tag responds with *Hash* of response
 - ◆ weak, long-running (perhaps seconds-long) CDMA signal
 - ◆ The waveform *is* the response
 - ◆ Long-integrating match filters required to detect
 - ◆ Return signal intensity can be well below N_0



Details of Cryptographic Layer: Initial Attempt



Pre-distribution
or current state

K_j, T_i, R_{j1}

Tag i

$K_j, T_i, H(K_j, R_{j1}, K_j)$

(1) Generate R_{j2}

(2)

(3)

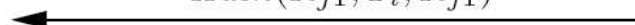
(4)

$R_{j1} \oplus K_j, Hash(K_j, R_{j2}, K_j),$
 $Hash(R_{j1}, Hash(K_j, R_{j2}, K_j), K_j)$



Verify and store R_{j1}
and $Hash(K_j, R_{j2}, K_j)$

$Hash(R_{j1}, T_i, R_{j1})$





Primary Benefits

- ◆ Two-layer security
 - ◆ Low probability of intercept (LPI) signaling
 - ◆ Probability of intercepting a symbol made arbitrarily small
 - ◆ Large (millions) of symbols per waveform
 - ◆ Intercepted signal is at best subspace of universe
 - ◆ Cryptographic layer with hashing, one-time keying
 - ◆ Relies primarily on one-time keys for cryptographic strength
 - ◆ Hashing more useful to generate long, non-repeating waveform



Secondary(?) Benefits

- ◆ Transfer media access control from protocol to signaling layer
 - ◆ Simplifies tag implementations
 - ◆ Transfers complexity to interrogator
- ◆ Decreased tag signaling power
 - ◆ Weak signals are *desirable* for LPI signaling
 - ◆ More power available to operate tag circuitry
- ◆ Easier to incorporate into location-positioning systems
 - ◆ Long, consistent signals vs. short, high-powered bursts



Research Tasks

- ◆ Formalize approach
- ◆ Simplify:
 - ◆ Minimize tag state
 - ◆ Key distribution, synchronization
- ◆ Can CDMA also simplify public-mode comm?
 - ◆ Good for bandwidth management
 - ◆ Detect multiple symbols simultaneously
 - ◆ Dynamically adjust to noise level
 - ◆ High channel utilization
- ◆ Prototype, measurement, and validation



Conclusions

- ◆ Fundamentally new use cases drive fundamentally new paradigms
 - ◆ Silicon-less RFID must be simpler
 - ◆ Additional cryptographic layer to current standards only adds complexity
 - ◆ Consumers (business and individuals) benefit from increased privacy
 - ◆ Market perception: working *for* consumer interests