Enhancing RFID Privacy via Antenna Energy Analysis

Ken Fishkin: Intel Research Seattle

Sumit Roy: U. Washington EE

Thanks to: Bing Jiang, U Washington EE

Introduction

- “With great power, comes great responsibility”
- Privacy worries have a legitimate basis
    - **“Deployed naïvely, embedding of RFID tags in consumer items presents a serious danger to privacy.” (Ari Juels)**
    - Can we address privacy worries realistically?
- Can we provide post-checkout value?

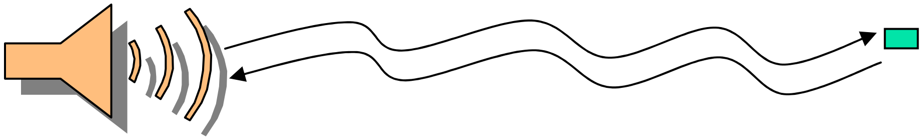
Isn’t this a known problem?

- Much investigation of privacy and security mechanisms in other domains:
  - File systems, Email, Ecommerce, Wireless
- We can leverage some of this
- One *qualitative* difference: the “donation” of energy by one party to the other.
  - Bad news: can’t do much computation
- Is there good news? Can we leverage this unique difference?
- Two proposals will be presented

Distance implies distrust

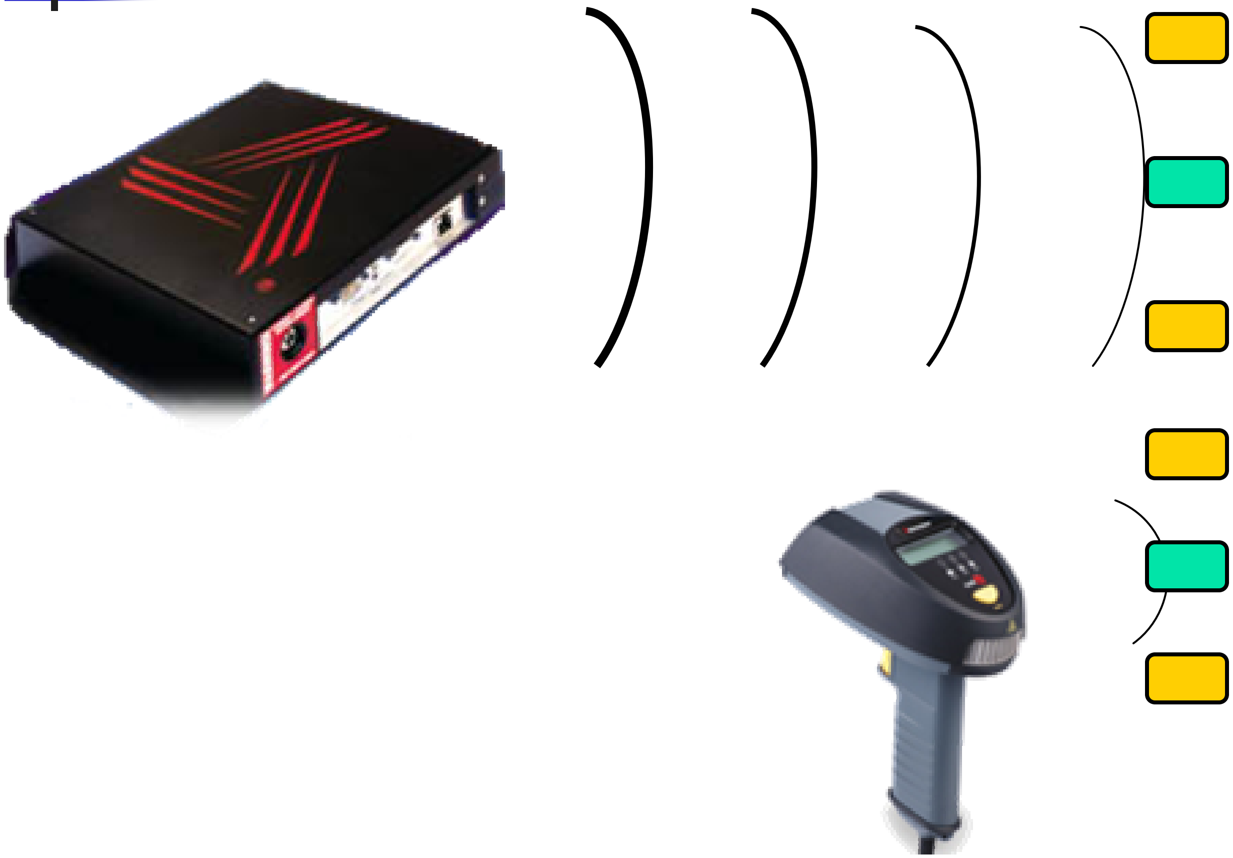
- Why aren’t people upset about bar codes?
  - Bar code scanners are *close* and *known*
- Most “nightmare” RFID scenarios involve *distant* and *unknown*
- Basic idea: can we require higher “bona fides” for more distant interrogators?

First idea: distance inference



- Does the energy wave change with distance?
- If so, can we infer distance from wave properties?
- Can we do it *robustly?*
  - RFID signal highly influenced by environment
- Three techniques presented
  - 1 largely negative result
  - 1 open for investigation
  - 1 initially positive result

#1: Look at wave curvature



#1: Look at wave curvature

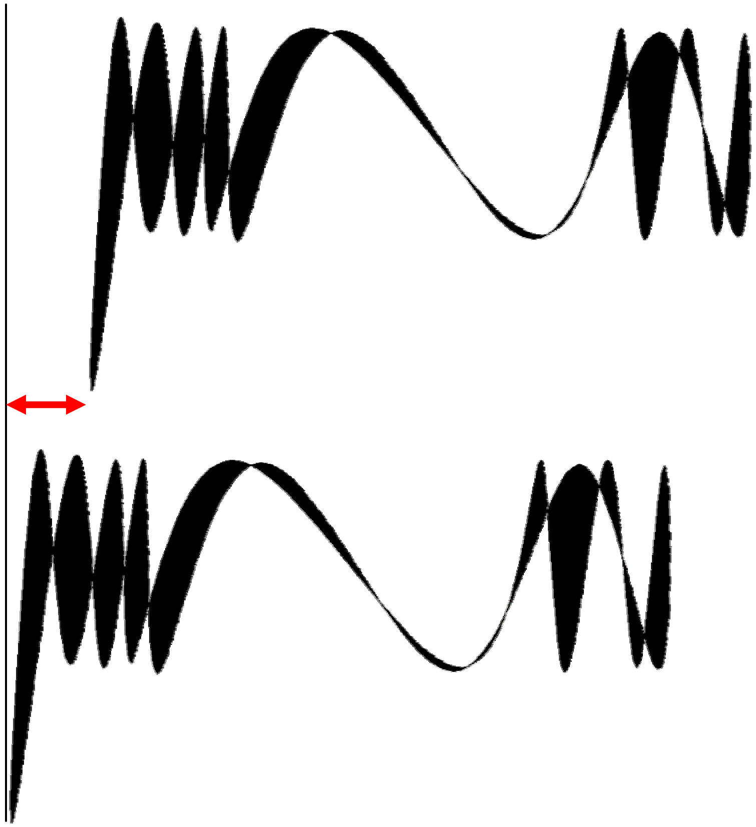
Fraunhofer far field effect: ≈(2 f d^2) / c

d f	0.3	0.05
13.56	0.01 m	0.00 m
900	**0.54 m**	0.01 m
2450	**1.46m**	**0.41m**

(Environmental fluctuation may swamp comparison)

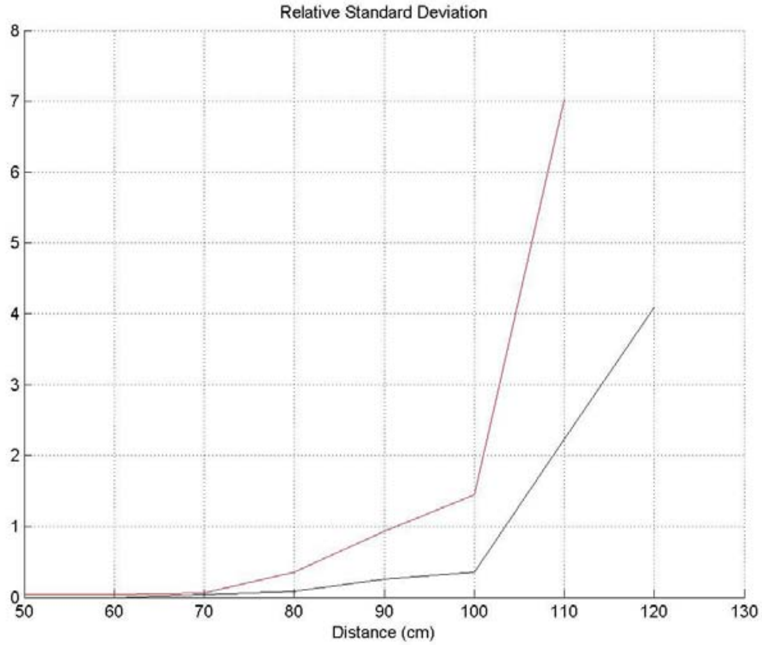
#2: Look at wave phase

- Need to compare amongst multiple tags.
- Under investigation



#3: Look at noise

- Signal/noise goes down with propagation
- Doesn't require multiple tags



Spoofing

- Can’t the hostile reader just change its energy signature to match that of a nearby reader?
- **NO** – you can’t have less than zero noise. You can spoof being *farther* (but why would you?) but not *nearer* than you really are.

Assuming it works

- Slight enhancement to tag circuitry: enforce maximum range, and/or report reads beyond that range
  - And/or turn yourself into a “blocker tag”
- Requires no reader modification
- Requires no protocol modification
- But limited: distant interrogators may be OK, nearby may not be

Second idea: tiered revelation

- Can we go “Beyond the kill switch”?
- “The problem with radio frequency ID is that it’s clear how retailers and manufacturers might benefit from attaching smart tags to their products, but it’s utterly unclear how this helps consumers.” (Technology review, 3 Nov 2003)
- Look at scenarios which provide post-purchase direct benefit to consumers

Energy-sensitive revelation

Nordstrom’s	Bought at Nordstrom’s, downtown Seattle
	Bought 7/28/03
Recall check	Made in Kuala Lumpur, Factory #17
	Made 2/5/03
Insurance	Benetton model X3J4
	Size L
Dryer	75% cotton, 25% poly
Washer	Mauve
	Shirt
	Object

- They don’t all require all the same information
- What if we make the “Bar” higher, the more information you want?

The proposal

- Tags move to a challenge-response system.
- Use energy
  - the closer the reader is, the more processing you can do
- Tag then reveals highest level of *authenticated* information

How this works

1. Reader specifies which level it wants
2. Tag specifies level of security, *and/or* amount of energy needed
3. Reader proceeds at that level of security
4. Respond if and only if get energy <u>and</u> security required

- Only *energy* increases – rough and simple distance requirement
- Only *security* increases – as existing protocols
- *Both* increase – interesting combination to explore

Assuming it works

- Requires changes to readers
- Requires changes to tags
- Requires changes to protocol
- But buys you a much more robust, extensible functionality

Conclusion

- Distance implies distrust: closeness implies comfort
- Energy can be used as a variable in the privacy equation
- Two examples presented: one easy and weaker, one hard and stronger