RFID Technical Tutorial

Presented by: Dale R. Thompson
Dept. of Computer Science and Computer Engineering
University of Arkansas

Goals

- Understand the details of RFID with focus on EPCglobal UHF Class-1 Generation-2 (Gen-2) passive tags being introduced into retail.
- Introduce the security threats *to* RFID and the privacy threats *by* RFID.
- Convince you that Privacy Assurance is necessary.

University of Arkansas RFID Research Center

- Fully student staffed with 24 industry members, which recently became the first open laboratory to be accredited by EPCglobal Inc.

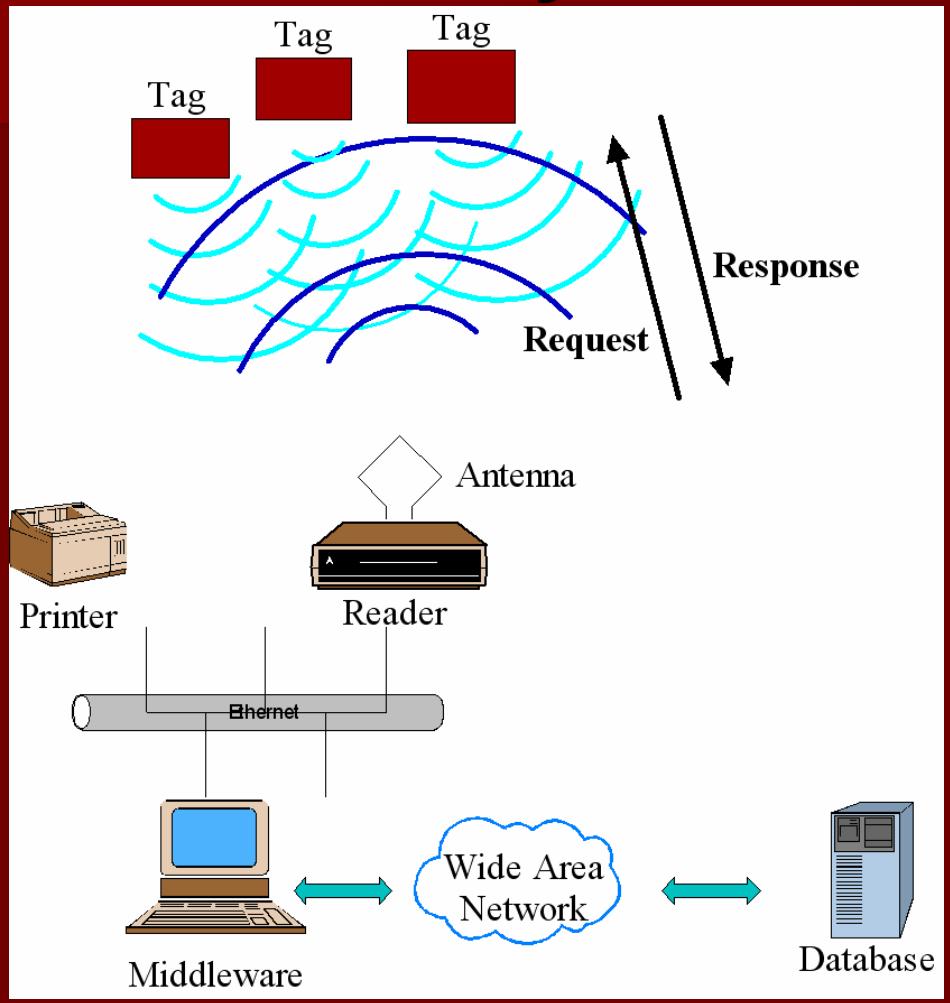
What is RFID?

- Stands for Radio Frequency Identification
- Uses radio waves for identification
- New frontier in the field of information technology
- One form of Automatic Identification
- Provides unique identification or serial number of an object (pallets, cases, items, animals, humans)

Applications

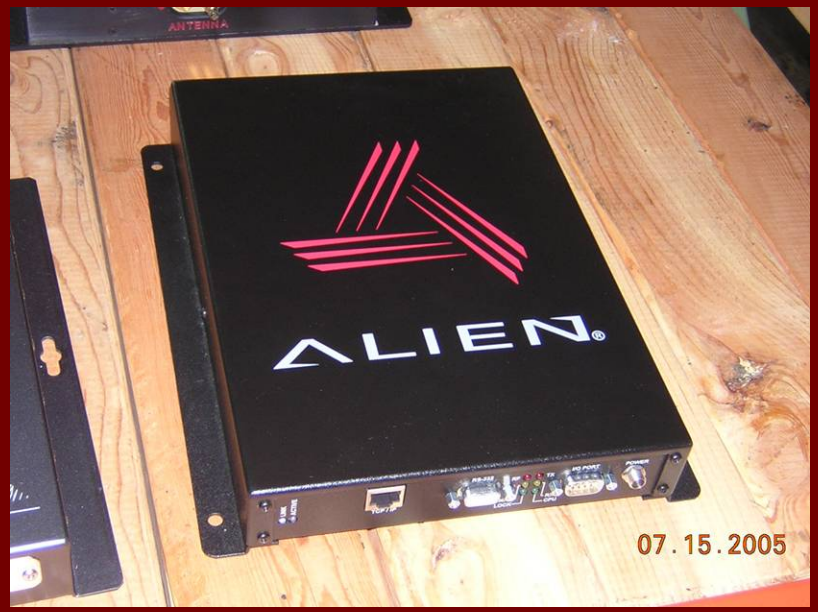
- Mobil Speedpass systems
- Automobile Immobilizer systems
- Fast-lane and E-Zpass road toll system
- Secure Entry cards
- Animal Identification
- Humans
- Supply chain management

RFID System


Tag
Tag
Tag
Response
Request
Antenna
Printer
Reader
Ethernet
Wide Area Network
Middleware
Database

RFID Reader

- Also known an interrogator
- **Reader powers passive tags with RF energy**
- Can be handheld or stationary
- Consists of:
  - Transceiver
  - Antenna
  - Microprocessor
  - Network interface



RFID Frequency range

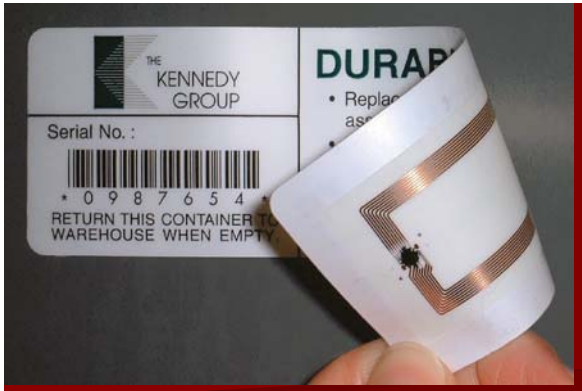
Frequency Band	Description
< 135 KHz	Low frequency
6.765 – 6.795 MHz	HF
7.4 – 8.8 MHz	HF
13.553 – 13.567 MHz	HF
26.957 – 27. 283 MHz	HF
433 MHz	UHF
868 – 870 MHz	***UHF***
902 – 928 MHz	***UHF***
2.4 – 2.483 GHz	SHF
5.725 – 5.875 GHz	SHF

FCC Rules for ISM Band Wireless Equipment

- Federal Communications Commission (FCC) regulates frequencies in United States
- FCC regulations appear in title 47 of the United States Code of Federal Regulations (47CFR) and radio spectrum issues are the subject of part 15 of the FCC rules
- Industrial, Scientific and Medical (ISM) devices

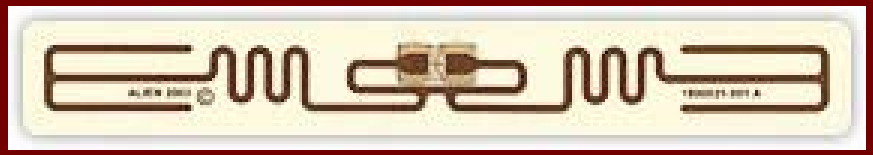
FCC Rules for 902-928 MHz

- Maximum transmitter power limited to 1 watt for systems that frequency hop across at least 50 channels (Gen-2 readers typically run 1 watt and frequency hop across 50 channels)
- Maximum EIRP (effective isotropic radiated power) is limited to 4 watts (36 dBm). For antenna gain greater than 6 dBi must reduce power. (For 1 watt reader transmitter the maximum gain antenna can be up to 6 dBI.)
- When frequency hopping, the transmitter must not use one frequency greater than 0.40 seconds within a 20 second period



RFID Tag

- Tag is a device used to transmit information such as a serial number to the reader in a contact less manner
- Classified as :
  - Passive – energy from reader
  - Active - battery
  - Semi-passive – battery and energy from reader



Printers

Middleware

- Each reader manufacturer
- Commercial middleware
- Open source middleware work at UofA

Database

- Store attributes related to the serial number of the RFID tag
- Examples
  - What is it?
  - Who made it?
  - Who bought it?
  - Where has it been?

Contactless Smart Cards

- ISO 7618 - A set of international standards covering the basic characteristics of contactless smart cards, such as physical and electrical characteristics, communication protocols and others.
- Proximity Smart Cards (13.56 MHz)
  - Range = 4 inches (10 centimeter)
  - Baud rate = 106 kilobaud
  - ISO/IEC 14443
- Vicinity Smart Cards (13.56 MHz)
  - Range = 3 feet (1 meter)
  - Baud rate = 26.48 kilobaud
  - ISO/IEC 15693

Animal Identification Standards

- International standard 134.2 kHz
  - ISO 11784: “Radio-frequency identification of animals” – code structure
  - ISO 11785: “Radio-frequency identification of animals” – Technical concept
  - ISO 14223: “Radio-frequency identification of animals” – Advanced transponders
- U.S. standard 125 kHz
- At these frequencies the RF can penetrate mud, blood, and water

VeriChip

- Human implantable RFID tag operating at about 134 KHz because at these frequencies the RF can penetrate mud, blood, and water
- About the size of uncooked grain of rice
- Oct. 22, 2002 – US Food and Drug Administration ruled VeriChip not regulated device
- Oct. 2004 – FDA ruled serial number in VeriChip could be linked to healthcare information
- Healthcare applications
  - Implanted medical device identification
  - Emergency access to patient-supplied health information
  - Portable medical records access including insurance information
  - In-hospital patient identification
  - Medical facility connectivity via patient
  - Disease/treatment management of at-risk populations (such as vaccination history)

Supply Chain Management

- RFID adds visibility as the items flow through the supply chain from the manufacturer, shippers, distributors, and retailers.
- The added visibility can identify bottlenecks and save money.
- Wal-Mart requested in June 2003 that their top 100 suppliers use RFID at the pallet and case level by January 2005.
- Wal-Mart currently has 300 suppliers sending products to 500 RFID-enabled Wal-Mart and Sam's Club stores.*
- Wal-Mart wants 1,000 stores with RFID by January 2007.*

*Source: http://www.extremerfid.com/article/WalMart+Forges+Ahead+with+RFID/172888_1.aspx

Does RFID Reduce Out of Stocks? A Preliminary Analysis

- Study by UA RFID Research Center
- Authors: Bill C. Hardgrave, Matthew Waller, Robert Miller, University of Arkansas
- From February 14 to September 12, 2005, out of stocks were examined daily in 24 Wal-Mart stores (12 RFID-enabled stores, 12 control stores)
- RFID reduced out-of-stocks by approximately 16% because RFID was able to identify if items were in the back room
- http://itri.uark.edu/research/display.asp?article=ITRI-WP058-1105

Standardization Item Management

- ISO/IEC [International Standards Organization (ISO), www.iso.org] and International Electrotechnical Commission, www.iec.ch]
  - 18000–1: Generic air interfaces for globally accepted frequencies
  - 18000–2: Air interface for 135 KHz
  - 18000–3: Air interface for 13.56 MHz
  - 18000–4: Air interface for 2.45 GHz
  - 18000–5: Air interface for 5.8 GHz
  - 18000–6: Air interface for 860 MHz to 930 MHz
  - 18000–7: Air interface at 433.92 MHz
- EPCglobal Inc., www.epcglobalinc.com
  - HF (13.56 MHz)
    - 13.56 MHz ISM Band Class 1
  - UHF (868 – 928 MHz)
    - UHF Class-0
    - UHF Class-1 Generation-1 (Class-1 Gen-1)
    - UHF Class-1 Generation-2 (Class-1 Gen-2)
      - Moving toward ISO 18000-6C

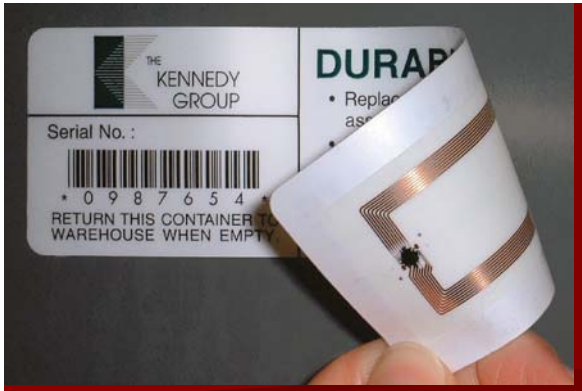
EPCglobal, Inc.

- Not-for-profit organization developing commercial, world-wide RFID standards
- Joint venture between EAN International and the Uniform Code Council (UCC).
  - UCC standardized Universal Product Code (UPC) barcodes in US
  - EAN standardized barcodes in Europe
  - UCC and EAN combined to form GS1
- http://www.epcglobalinc.org/
- UHF Class-1 Generation-2 (Class-1 Gen-2 or commonly known as Gen-2)
  - In process of becoming ISO 18000-6C standard

Electronic Product Code (EPC)

Version	EPC Manager	Object Class	Serial Number	
2 bit	21 bit	17 bit	24 bit	64 Bit Type I
2 bit	15 bit	13 bit	34 bit	64 Bit Type II
2 bit	26 bit	13 bit	23 bit	64 Bit Type III
8 bit	28 bit	24 bit	36 bit	96 Bit

96 bits can uniquely label all products for the next 1,000 years



EPC vs. UPC (Barcodes)

- Both are forms of Automatic identification technologies
- Universal Product Code (UPC) require line of sight and manual scanning whereas EPC do not
- UPC require optical reader to read whereas EPC reader reads via radio waves
- EPC tags possess a memory and can be written while UPC do not
- EPC tags cost 5 cents, UPC tags cost 1/10 cent

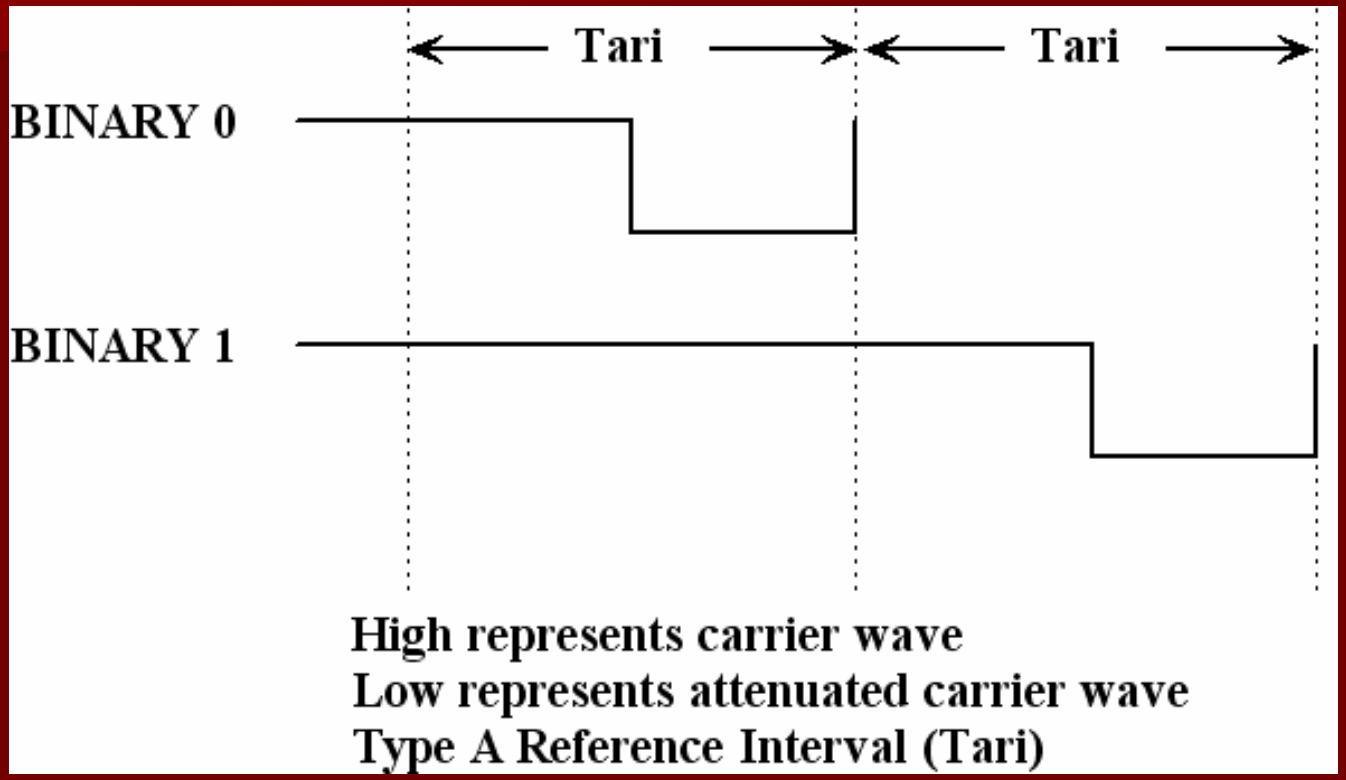
EPCglobal Inc. UHF Specification History

- EPCglobal UHF Class-0
- EPCglobal UHF Class-1 Generation-1
- EPCglobal UHF Class-1 Gen-2 (Gen-2)
  - In process of becoming ISO 18000-6C standard
  - Item management standard
  - Retail standard

EPCglobal UHF Class-1 Gen-2 Reader-to-Tag Physical and Link Layers

- Modulation
  - Double sideband amplitude shift keying (DSB-ASK)
  - Single-sideband ASK (SSB-ASK)
  - Phase reversal ASK (PR-ASK)
- Encoding - Pulse interval encoding (PIE)
- Data rate based on Tari
  - Tari 25 microsecond (TYPICAL SETTING)
    - 40 Kilobits per second (Kbps) maximum
    - 27 Kbps average
  - Tari 12.5 microsecond
    - 80 Kbps maximum
    - 53 Kbps average
  - Tari 6.25 microsecond
    - 160 Kbps maximum
    - 107 Kbps average

PIE Encoding



EPCglobal UHF Class-1 Gen-2 Tag-to-Reader Physical and Link Layers

- Backscatter modulation
  - Varies reflection coefficient of antenna
  - Switch load on antenna in time with bits, which varies input impedance
  - Varies amount of energy reflected from tag to reader
  - 80 to 90 dB less signal than reader-to-tag (10,000 times weaker!)
- Modulation
  - Amplitude shift keying (ASK)
  - Phase shift keying (PSK)
- Encoding – Reader chooses type
  - FM0
  - Miller (M=2, 4, or 8)
- Data rates are variable
  - FM0 [single reader mode] – 40 Kbps up to 640 Kbps
  - Miller (M=2) [multi-reader mode] – 20 Kbps up to 320 Kbps
  - Miller (M=4) [dense reader mode] – 10 Kbps up to 160 Kbps
  - Miller (M=8) – 5 Kbps up to 80 Kbps
  - Typical rates in the lab vary between 60-70 Kbps using Miller (M=4)

Class-1 Gen-2 Anti-Collision Protocol (media access control)

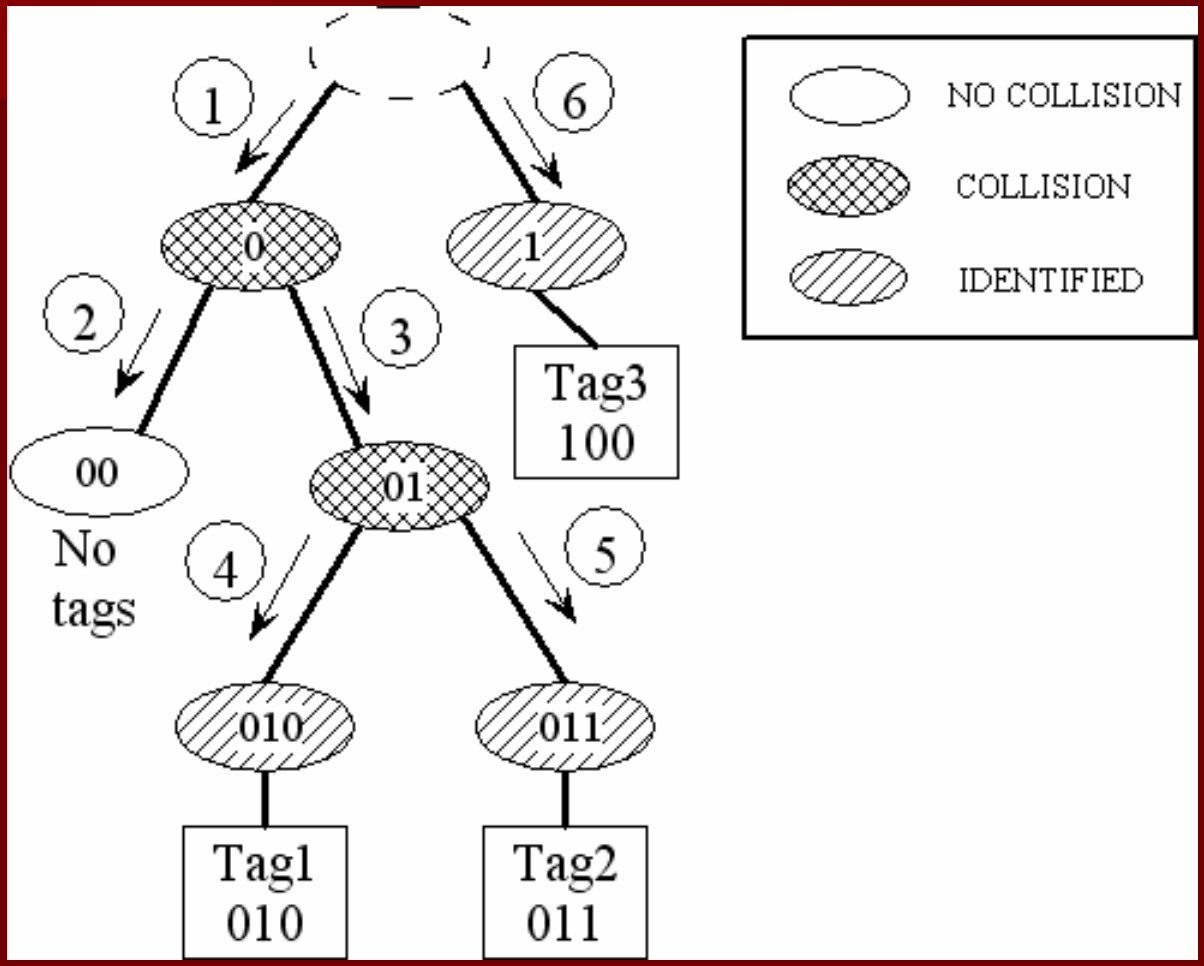
- Select phase
  - Single out particular tag population with one or more bits with query tree protocol
- Inventory phase – identify individual tag using Q protocol (slotted-aloha based)
  - Reader sends Query with parameter Q and Session number (Q=4 is suggested default)
  - Reader creates slotted time
  - Tags pick random 16-bit number for *handle*
  - Tags in requested session pick a random number in the range [0,2^Q-1] for *slot_number*
  - If *slot_number* = 0, backscatter *handle*
  - If *slot_number* != 0, wait that number of slots to backscatter *handle*
  - Reader ACKs individual tag with *handle* and goes to access phase. All other tags wait.
  - If more that one tag answers, reader can send same Q again or send modified Q
- Access phase
  - Reader interacts with tags requesting EPC number and any other information

Class-1 Gen-2 Select (Query Tree)

Time slice	0	1	2	3	4	5
Reader-to-Tag	0**		00*		01*	
Tag-to-Reader		collision		no answer		collision
Tag1 (ID = 010)		010				010
Tag2 (ID = 011)		011				011
Tag3 (ID = 100)						

Time slice	6	7	8	9	10	11
Reader-to-Tag	010		011		1**	
Tag-to-Reader		010		011		100
Tag1 (ID = 010)		010				
Tag2 (ID = 011)				011		
Tag3 (ID = 100)						100

Class-1 Gen-2 Select (Query Tree)



Class-1 Gen-2 Inventory (Q protocol, form of slotted Aloha)

Time slice	0	1	2	3	4	5	6	7
Slot number			0	1	2	3		
Reader-to-Tag	Query Q=2						ACK handle1	
Tag-to-Reader			handle1	collision	empty	empty		EPC1
Tag1		slot=0	handle1					EPC1
Tag2		slot=1		handle2				
Tag3		slot=1		handle3				

Time slice	8	9	10	11	12	13	14	15
Slot number			0	1	2	3		
Reader-to-Tag	QueryAdjust						ACK handle2	
Tag-to-Reader			empty	handle2	empty	handle3		EPC2
Tag1 (ID = 010)		wait						
Tag2 (ID = 011)		slot=1		handle2				EPC2
Tag3 (ID = 100)		slot=3				handle3		

Class-1 Gen-2 Security

- Ability to generate 16-bit pseudo-random number
  - Handle for singulation (better than using EPC)
  - Encrypt (obscure) reader-to-tag link
  - Pick slots in Q protocol
- 16-bit CRC for error detection
- 32-bit access password
- 32-bit kill password

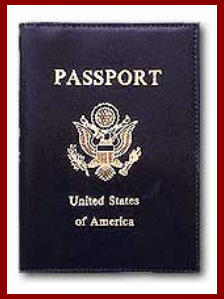
Trivia on Passive UHF RFID

- How far can a reader read a tag?
  - Less than 20 feet using legal equipment
- What causes interference at these frequencies?
  - Metal reflects the energy and can shield
  - Water absorbs the energy. Microwaves operate at 2.4 GHz because water absorbs energy at these frequencies. Passive UHF operates around 900 MHz, which is close enough.

Hacking Cryptographically-Enabled RFID Device

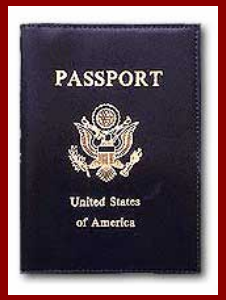
- Team at Johns Hopkins University reverse engineer Texas Instrument's Digital Signature Transponder
  - Paid for gas with cloned RFID tag
  - Started car with cloned RFID tag

- Lessons
  - Security by obscurity does not work
  - Use standard cryptographic algorithms with sufficient key lengths



RFID-enabled Passport

- May 2002: The Enhanced Border Security and Visa Entry Reform Act requires the USA and other countries whose citizens don't need visas for entering the USA to develop electronic passports. The act sets a deadline of October 2004.
- March 2004: The Bush administration asks Congress to delay the deadline to October 2006 to allow participating countries more time to address technical issues. Congress agrees.
- January 2005 - US Government Awards RFID Passport Contracts for testing RFID passports
- April 2005: The State Department closes comment period, begins to firm up plans for the new e-passport.
- April 2005 – State Department reconsiders adding security measures to RFID-enabled passports after public outcry because can be read at 30 feet (10 meters) instead of 4 inches (10 cm) [ISO 14443]
- August 2005 – State Department adds metallic ant-skimming material to cover and spine of passport to limit reading distance to 1 inch
- November 2005: State Department plans to make e-passports available to U.S. travelers by October 2006 that have features to prevent skimming and Basic Access Control (characters printed on passport act like PIN number)
  - Before being read PIN must be entered into reader
  - Encryption between reader and tag
- October 2005: E-passports available for U.S. travelers



RFID-enabled passport

- Metallic anti-skimming material added in cover and spine to reduce read distance to 1 inch
- PIN number printed on cover must be entered in reader to read tag and it encrypts communication
- New industry for wallet makers creating Faraday cages for passports

Passport Solution!

RFDump

- Open source software tool for RFID ISO-15693 and ISO-14443 readers (13.56 MHz)
  - Read/write data on RFID tags
  - Integrated cookie feature
    - Add cookie to tag and automatically increment counter when tag is in range of reader
    - Track number of times shopper enters reader field or picks up item
  - www.rf-dump.org

RFID Virus

- M. R. Rieback, B. Crispo, and A. S. Tanenbaum, “Is your cat infected with a computer virus?,” in *Proc. IEEE Int’l. Conf. Pervasive Computing and Communications (PerCom)*, Pisa, Italy, Mar. 13-17, 2006.
- More to do with attack against RFID middleware software than RFID
  - SQL injection attack
  - Buffer overflow attack

RFID Security and Privacy Threats

- Security threats *to* the RFID system
- Privacy threats *by* the RFID system

Threat Modeling

- Assemble team
- Decompose system into threat targets
- Identify/Categorize threats to threat targets
- Attack graphs for each threat target
- Assign risk to each threat
- Sort threats
- Mitigate threats with higher risks

Security Threats Categorized with STRIDE

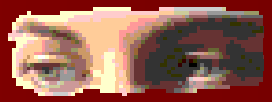
- Spoofing identity
- Tampering with data
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege

STRIDE Categories and Mitigation Techniques

Category	Techniques
Spoofing identity	Appropriate authentication Protect secrets Don't store secrets
Tampering with data	Appropriate authentication Hashes Message authentication codes Digital signatures Tamper-resistant protocols
Repudiation	Digital signatures Timestamps Audit trails
Information disclosure	Authorization Privacy-enhanced protocols Encryption Protect secrets Don't store secrets
Denial of service	Appropriate authentication Appropriate authorization Filtering Throttling Quality of Service
Elevation of privilege	Run with least privilege

Security Threats *to* RFID

- A competitor or thief performs an unauthorized inventory of a store by scanning tags with an unauthorized reader to determine the types and quantities of items.
  - Spoofing
  - Information disclosure
- An attacker modifies the EPC number on tags or kills tags in the supply chain, warehouse, or store disrupting business operations and causing a loss of revenue.
  - Tampering with data
  - Denial of service
- An attacker modifies a high-priced item's EPC number to be the EPC number of a lower cost item.
  - Tampering with data



Privacy Threats *by* RFID

- A bomb in a restaurant explodes when there are five or more Americans with RFID-enabled passports detected.
- A mugger marks a potential victim by querying the tags in possession of an individual.
- A fixed reader at any retail counter could identify the tags of a person and show the similar products on the nearby screen to a person to provide individualized marketing.
- A sufficiently powerful directed reader reads tags in your house or car.
  - The ISO 14443 standard proposed for passports specifies about 4 inches (10 cm) as the typical range. However, NIST with a special purpose antenna read it at 30 feet (10 meters)!
- RFID enables tracking, profiling, and surveillance of individuals on a large scale.

Top Privacy Threats by RFID

- Tracking – Determine where individuals are and where they have been
- Hotlisting – Single out certain individuals because of the items they possess
- Profiling – Identifying the items an individual has in their possession

How far can a passive tag be read?

Assume distance limited by power available to run the tag's circuits.

$$P_T = \frac{P_R G_R G_T \lambda^2}{(4\pi)^2 r^2}$$

P_T = power available to tag (100 μW needed)

P_R = reader transmit power (1 watt)

G_R = reader antenna gain (6 dBi)

G_T = tag antenna gain (1 dBi)

$\lambda = c/f$ = wavelength (meters)

$c = 3x10^8$ meters/s

f = frequency (915 MHz)

r = distance in meters

Maximum Distances to Read UHF Passive Tag

Antenna Gain (dBi)	Distance (meters)	Distance (feet)
6 (legal)	5.8	19*
9	8.3	27
12	11.7	38
15	16.5	54

*Reality: Today, in the lab 8 to 12 feet.

What is Privacy?

- Privacy includes the right to make decisions about one's own life, to keep personal secrets, and to keep secrets about where we come and go.
- It is the right to make decisions without interference from the government or economic pressures from commercial entities.

What Privacy is Not!

- Privacy does NOT apply to an organization. It only applies to data about an individual, which is called personally identifiable data.
- Privacy is NOT security.
  - Security is important to privacy.
  - Security is only part of the story.

5 Principles of Privacy

- **Notice**. There must be no personal-data, record-keeping systems whose very existence is a secret.
- **Access**. There must be a way for a person to find out what information about the person is in a record and how it is used.
- **Choice**. There must be a way to prevent personal information that was obtained for one purpose from being used or made available for other purposes without the person's consent.
- **Recourse**. There must be a way for a person to correct or amend a record of identifiable information about the person.
- **Security**. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

Alan F. Westin's Privacy Classifications

- Privacy Fundamentalist (11%)
  - Very concerned
  - Unwilling to provide data
- Privacy Unconcerned (13%)
  - Mild concern
  - Willing to provide data
- Privacy Pragmatists (75%)
  - Somewhat concerned
  - Willing to provide data if they are notified and get a benefit

Future Work

- Study and develop a systemic solution to quantify and control privacy when exchanging personally identifiable data.
- This will create a more secure RFID system that provides privacy assurance by protecting the privacy of individuals.

References

- N. Chaudhry, D. R. Thompson, and C. Thompson, *RFID Technical Tutorial and Threat Modeling*, ver. 1.0, tech. report, Dept. of Computer Science and Computer Engineering, University of Arkansas, Fayetteville, Arkansas, Dec. 8, 2005. Available: http://csce.uark.edu/~drt/rfid
- S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device," in *Proc.14th USENIX Security Symposium*, Baltimore, MD, USA, July-Aug. 2005, pp. 1-16.
- EPCglobal Inc., http://www.epcglobalinc.org/
- *EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz*, ver. 1.0.9, EPCglobal Inc., Jan. 31, 2005. Available: http://www.epcglobalinc.org/.
- K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, R. Waddington, Trans., 2nd ed., Hoboken, New Jersey: John Wiley & Sons, 2003.
- S. Garfinkel and B. Rosenberg, Eds., *RFID: Applications, Security, and Privacy*, Upper Saddle River, New Jersey: Addison-Wesley, 2006.
- S. Karthikeyan and M. Nesterenko, "RFID security without expensive cryptography," in *Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, Alexandria, VA, USA, Nov. 2005, pp. 63-67.
- Opinion Research Corporation and Alan F. Westin. *"Freebies" and Privacy: What Net Users Think.* Sponsored by Privacy & American Business. Hackensack, NJ: P & AB, July 1999. Available: http://www.privacyexchange.org
- M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "Is your cat infected with a computer virus?," in *Proc. IEEE Int'l. Conf. Pervasive Computing and Communications (PerCom)*, Pisa, Italy, Mar. 13-17, 2006.
- Verichip, http://www.verichipcorp.com/

Contact Information

Dale R. Thompson, P.E., Ph.D.
Department of Computer Science and Computer Engineering
University of Arkansas
311 Engineering Hall
Fayetteville, Arkansas 72701
Phone: +1 (479) 575-5090
FAX: +1 (479) 575-5339
E-mail: d.r.thompson@ieee.org
WWW: http://csce.uark.edu/~drt/