Session #R6
RFID Security for Retail Enterprises

MIS TRAINING INSTITUTE

RFID Security for Retail Enterprises

Session #R6

Joe Grand

Grand Idea Studio, Inc.

Tuesday, 1:45pm – 2:45pm

SECURITY WORLD CONFERENCE & EXPO 2006

MIS TRAINING INSTITUTE

Agenda

- Overview of RFID Technologies
- RFID Use and Implementation
- Security Risks and Attacks
- Demonstration of Portable RFID Readers
- Resources

What is Radio Frequency Identification (RFID)?

- Generic term for non-contacting technologies that use radio waves to automatically identify people or objects
- Has been available for decades, but just now becoming popular for mainstream
  - **Access control, automatic identification (passports, driver license), payment systems, inventory (human?) tracking, car immobilization, casino chips**

RFID System Overview

- Most common use is to store unique serial number or electronic product code (read-only) on a microchip that is attached to an antenna
  - **Combined antenna and microchip called a "transponder" or "tag"**
- Typical RFID system contains a reader (also called an "interrogator") and one or more tags
  - **The reader is usually a combination of hardware and software**
  - **Each tag's unique serial number identifies a specific person or object**

RFID System Overview 2

- Two major tag types:
  - **Passive: No internal power source or transmitter, shorter range**
  - **Active: Power source (battery) and transmitter, longer range**
- Four typical frequency ranges:
  - **LF (Low Frequency), 125 to 134.2kHz**
  - **HF (High Frequency), 13.56MHz**
  - **UHF (Ultra-High Frequency), 868 to 928MHz**
  - **uW (Microwave), 2.45 and 5.8 GHz**

RFID System Overview 3

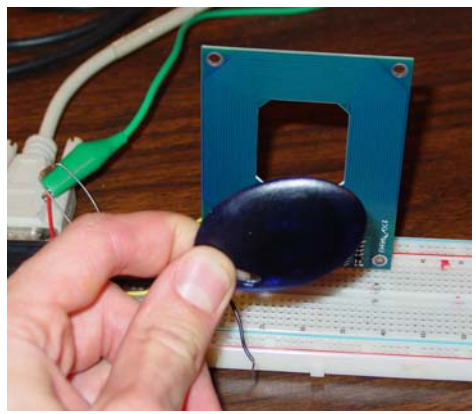
- Three tag flavors:
  - **Read-Only**
  - **Read/Write**
  - **Cryptographic**
- No security between most tag and reader transmissions
  - **If you have a reader for the correct tag family and frequency, you can communicate with the tag**
  - **Can easily create an RFID "scanner" to snoop around for RFID tags and retrieve their data**

RFID System Overview 4

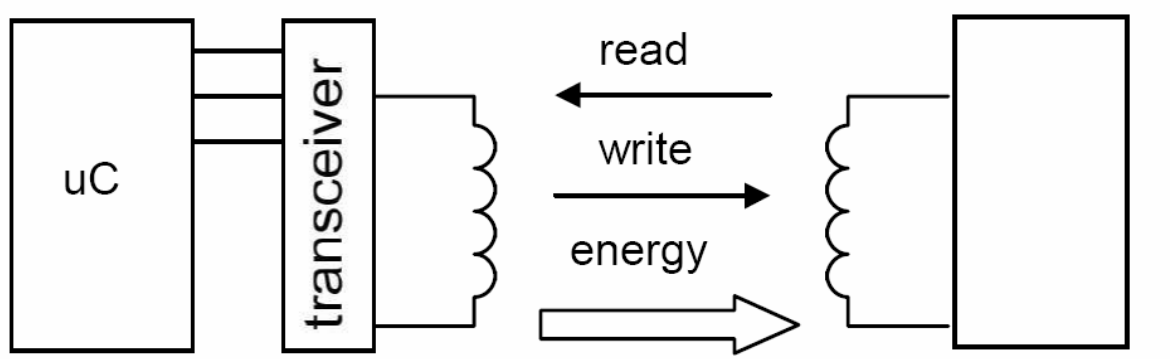
- The effective range of a tag depends on many factors:
  - **RFID system frequency**
  - **Transmit power of the reader**
  - **Quality of the reader's antenna**
  - **Tag type**
  - **Interference from other RF devices**
- Some systems governed by public standards to make them more "universal"
  - **Ex.: ISO 18000, ISO 15693, ISO 14443**

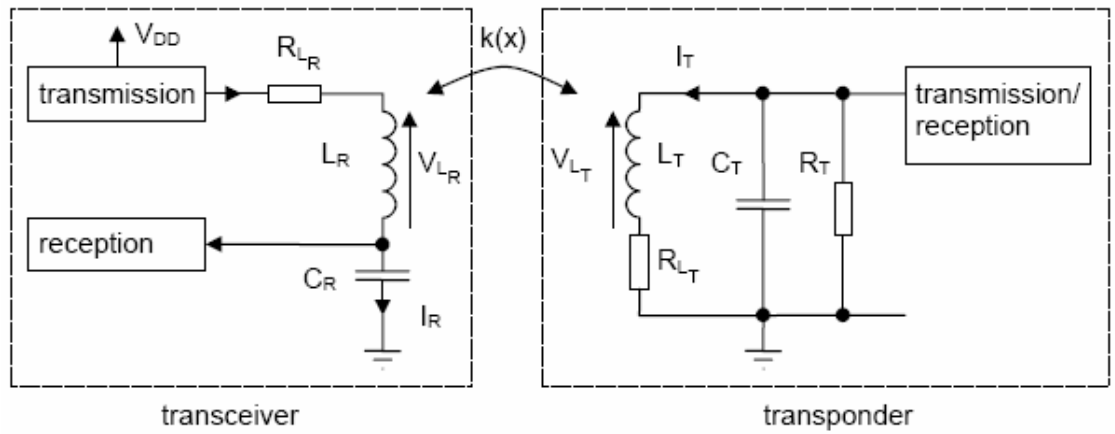
RFID System Overview 5

1. Reader's antenna transmits electric field or magnetic field (called a "carrier")
2. Energy "harvested" by tag's antenna and used to power up internal circuitry
3. Tag will modulate electromagnetic waves generated by the reader to transmit data
4. Receiver demodulates waves and converts to digital signal



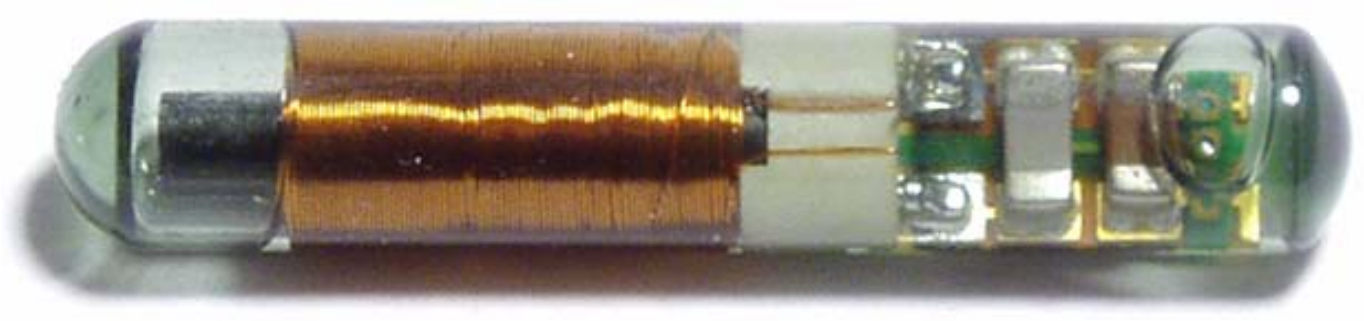
RFID System Overview 6





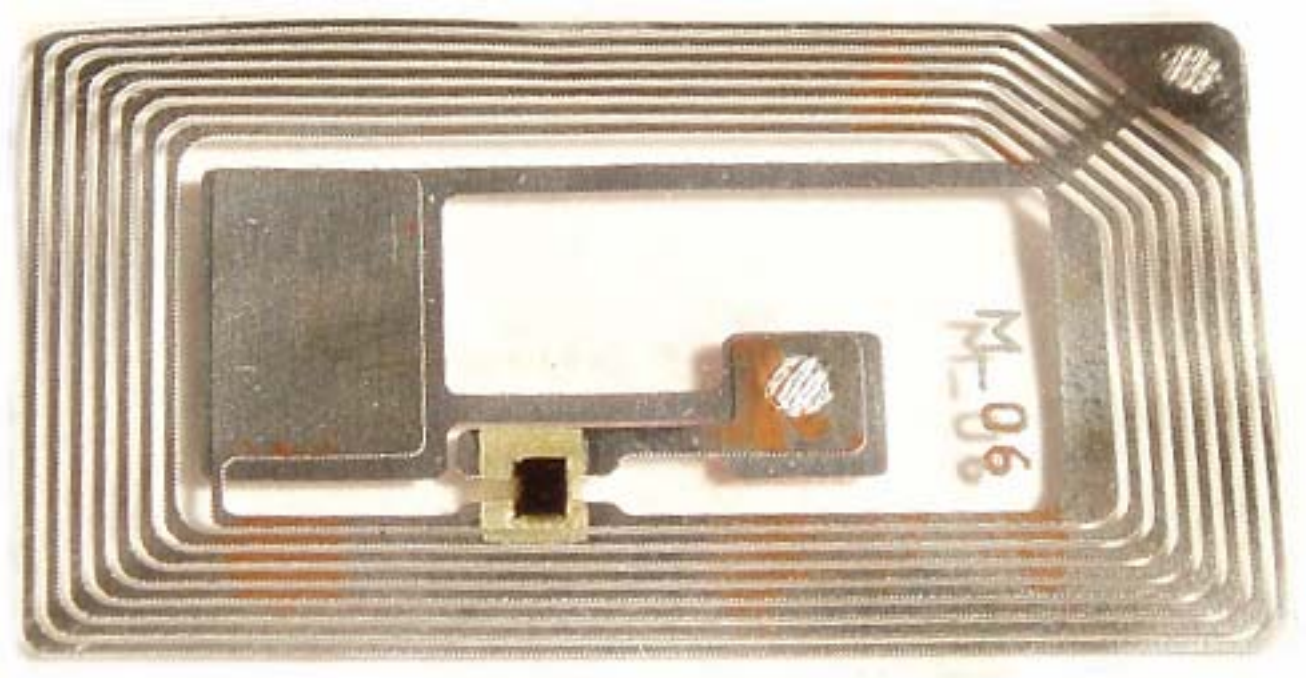
Images from **www.emmicroelectronic.com**

Tag Example: TI 125kHz



(Approx. 3/4" long)

Tag Example: 13.56MHz Label



(Approx. 3" long)

Tag Example: Smart Labels

- ISO standard designed to replace UPC (Universal Product Code) barcodes on products
- Each label stores a unique EPC (Electronic Product Code)
- Typically uses 13.56MHz range
- Ex.: Inventory tracking, Customer auto-checkout, Track behavior of customer in the shop, etc.

EPC Type 1			
01	0000A66	00016F	000169DCD
Header	EPC Manager	Object Class	Serial Number
8 Bit	24 Bit	24 Bit	36 Bit

Retail/Inventory Tracking

- All assets labeled with RFID tags to track item from manufacture to sale (Ex.: Smart Labels)
- Benefits:
  - **Easy integration at the production plant**
  - **Easy sorting and tracking of stock**

Retail/Inventory Tracking 2

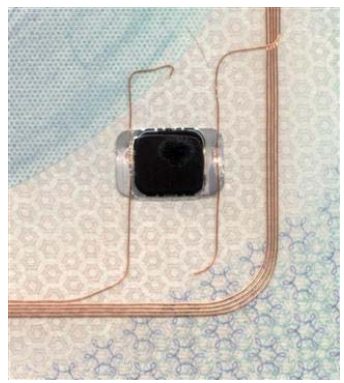
- Ex.: The Gillette Company
  - **Up to 35% loss of their product from plant to retail**
  - **Shoplifting a major problem for razor blades**
  - **Most products contain RFID tag on/inside product**
  - **Major privacy concerns: `www.boycottgillette.com`**

Retail/Inventory Tracking 3

- Ex.: Vienna, Austria Main Library
  - **RFID tags placed on over 240,000 books and 60,000 CDs/DVDs**
  - **Label contains: ISBN (International Standard Book Number), Author, Title, Location in the library, Last individual who checked out the book, Status**
  - **Self-service terminals ("EasyChecks") available for easy media check-out and return**

Passports

- Mandate for US and 27 other countries to transition to electronic passports in 2005/2006
  - **Ex.: Malaysia's national ID card, "MyCard," already has RFID**
- Electronic passports will contain ISO 14443-compliant RFID tag
- Passport to be readable from 4 inches away
  - **User must open passport before communications can begin**



Passports 2

- Tag stores personal information and biometric data
  - **Ex.: EU to store fingerprints, US to store digital representation of ID photo**
  - **To be encrypted?**
- Baseline implementation has no access control
  - **Anyone with the proper equipment can uniquely identify individual passports**
  - **Even if data is encrypted, could still identify who has a passport and possibly from what country**

Casino Chips

- Casinos are starting to embed RFID tags into chips to:
  - **Monitor gambling activity (for "comps")**
  - **Detect counterfeit chips**
  - **Catch cheaters who try to surreptitiously add or remove chips from a wager**
  - **Track movements of the chips/player within the casino?**
  - **Ex.: Wynn Casino the first to announce and use?**

Other Applications

- Credit Cards
  - **September 19, 2005: MasterCard to distribute 4 million "PayPass" cards, `www.paypass.com`**
- Transportation Systems
  - **London Underground, `www.oystercard.com`**
  - **Washington, DC Metro, "SmarTrip" card launched May 1999, 360,000 users**
  - **EZ Pass (New York, Massachusetts, many other places), FasTrak (SF/Bay Area) for toll roads, active tag**

Other Applications 2

- Cheese
  - **"Who Made My Cheese? Tags Track Parmesan's Age, Origin," The Wall Street Journal, July 7, 2005, pg. B1**
  - **94-member co-op of Parmesan cheese makers in Northern Italy**
  - **Branding 30kg (66lb) tire-sized cheese wheels to uniquely track & update the status of each wheel and assure buyers of its authenticity**

RFID Security Concerns

- Confidentiality
  - **Prevent reading/copying of data from RFID tag**
- Integrity
  - **Prevent modification, spoofing or replay attacks of RFID system or tag data**
- Availability
  - **Prevent denial-of-service of RFID system or deletion of RFID tag data**
- Liability
  - **Prevent abuse or misuse of RFID tag data**

RFID Attacks

- Tag Placement
  - **Switch label between assets**
  - **Apply label to incorrect assets**
  - **Cover label with blocking material**
  - **Destroy label**
- Physical
  - **Modify the reader or back-end server/database**
  - **Advanced techniques to modify/alter the IC within the tag**
    - Data is typically stored in cleartext on the microchip

RFID Attacks 2

- Passive
  - **Simply retrieve information from tag using off-the-shelf/custom reader system (also known as "skimming")**
  - **Sniff tag-to-reader or reader-to-tag communication**
    - Capacitively-coupled RFID tags (UHF/uW) more vulnerable than inductively-coupled (LF/HF) due to signal propagation range
  - **Side-channel attacks (e.g., differential power analysis)**
    - Ex.: **`www.cryptography.com/resources/whitepapers/DPA-technical.html`**

RFID Attacks 3

- Active (also known as "Air Interface Attacks")
  - **Reprogram tags (many tags are not write-protected)**
  - **Spoof tag/reader communication**
  - **Clone tag (label impersonation)**
  - **Denial-of-Service with noisy/overpowering RF signal**
  - **Enable tag-specific "Kill" command**
    - Tag cannot be restored once killed
    - Created due to privacy concerns of tag remaining active after its not needed anymore
    - EPC G2 uses password protection to enable

RFID Attacks 4

- RFID Virus/Malware
  - **Rogue tag sends malware to system via reader interface**
  - **Ex.: Melanie Rieback, RFID Viruses and Worms, `www.rfidvirus.org`**

RFID Attack Example: Data Modification

- Modifying data stored on an RFID tag
- Popular with EPC-based Smart Labels (13.56MHz) used in retail environments
  - **Ex.: The Metro Future-Store, `www.future-store.org`**

Image from **www.rf-dump.org**

RFID Attack Example: Data Modification 2

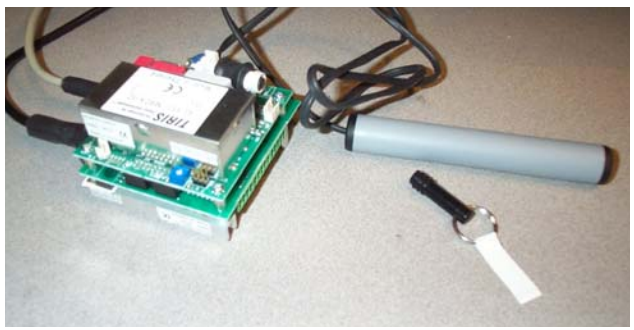
- Attack becomes a new class of shoplifting
  - **Ex.: Change EPC codes from one product to another**
  - **Ex.: Change the age-restriction on adult materials**
  - **Ex.: Deactivate the tag (if supported) so it is not readable**
- Attack can be succeeded with publicly-available RFID reader/writer hardware

RFID Attack Example: Card Simulation

- RFID/Proximity Card Simulation by Jonathan Westhues, **`http://cq.cx/prox.pl`**
- Designed for HID-style cards
- Attack process:
  1. **Read a legitimate card to get its ID code**
  2. **Store the ID in memory**
  3. **Replay the ID to a legitimate reader**

RFID Attack Example: TI DST

- In January 2005, challenge/response scheme of Texas Instruments Digital Signature Transponder (DST, `www.ti.com/rfid`) tag was cracked
  - **Ex.: Mobil SpeedPass, vehicle immobilizers, etc.**
  - **"Analysis of the Texas Instruments DST RFID," `www.rfidanalysis.org`**



RFID Attack Example: TI DST 2

- Weak, proprietary cipher (based on 40-bit key) reverse engineered from a single PowerPoint slide
  - **Properly designed crypto systems should depend solely on the secrecy of the *key***
  - **Discovery of TI's proprietary algorithm was the Achilles' heel of the DST**
- Over 150 **million** deployed devices are now at risk and could be cloned or spoofed!
- TI acknowledged the discovery, but still nothing has changed (they do not find the threat something that is likely to occur in the mainstream)

Joe says... "It's only a matter of time!"

RFID Attack Example: TI DST 3

- Attack process:
  1. **"Skimming": Retrieve DST reader challenge and subsequent tag response**
  2. **Key cracking: Used custom hardware to recover the unique cryptographic key of the DST**
  3. **Simulation: Used custom hardware and software routines to impersonate the original DST tag**

Images from **www.rfidanalysis.org**

Making a Portable RFID Reader

- Trivial to create system to read/write RFID tags
  - **If you have a reader for the correct tag family and frequency, you can communicate with the tag**
  - **Can easily create an RFID "scanner" to snoop around for RFID tags and retrieve their data**
- We demonstrate two systems:
  - **Parallax RFID Reader Module (125kHz)**
  - **ACG H102022 PC Handheld Reader Module (13.56MHz)**

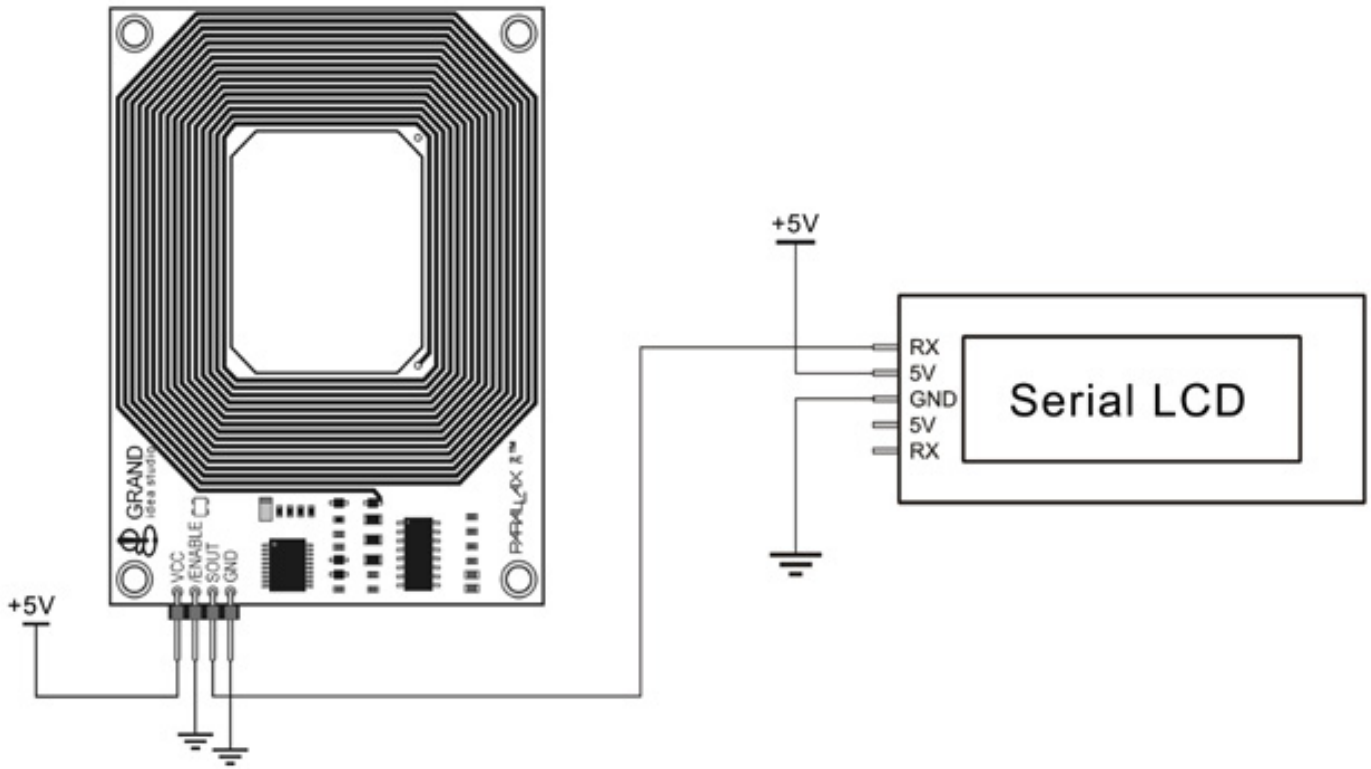
Making a Portable RFID Reader 2

- We used the Parallax RFID Reader Module (designed by yours truly), **`www.parallax.com/detail.asp?product_id=28140`**
  - **Reads passive, low-frequency (125kHz) RFID tags from up to ~4" away**
  - **Works specifically with the EM Microelectronic EM4100-family read-only tags**
    - Some of the most widely used throughout the world
  - **Each tag contains a unique identifier (one of 2^{40}, or 1,099,511,627,776, possible combinations)**

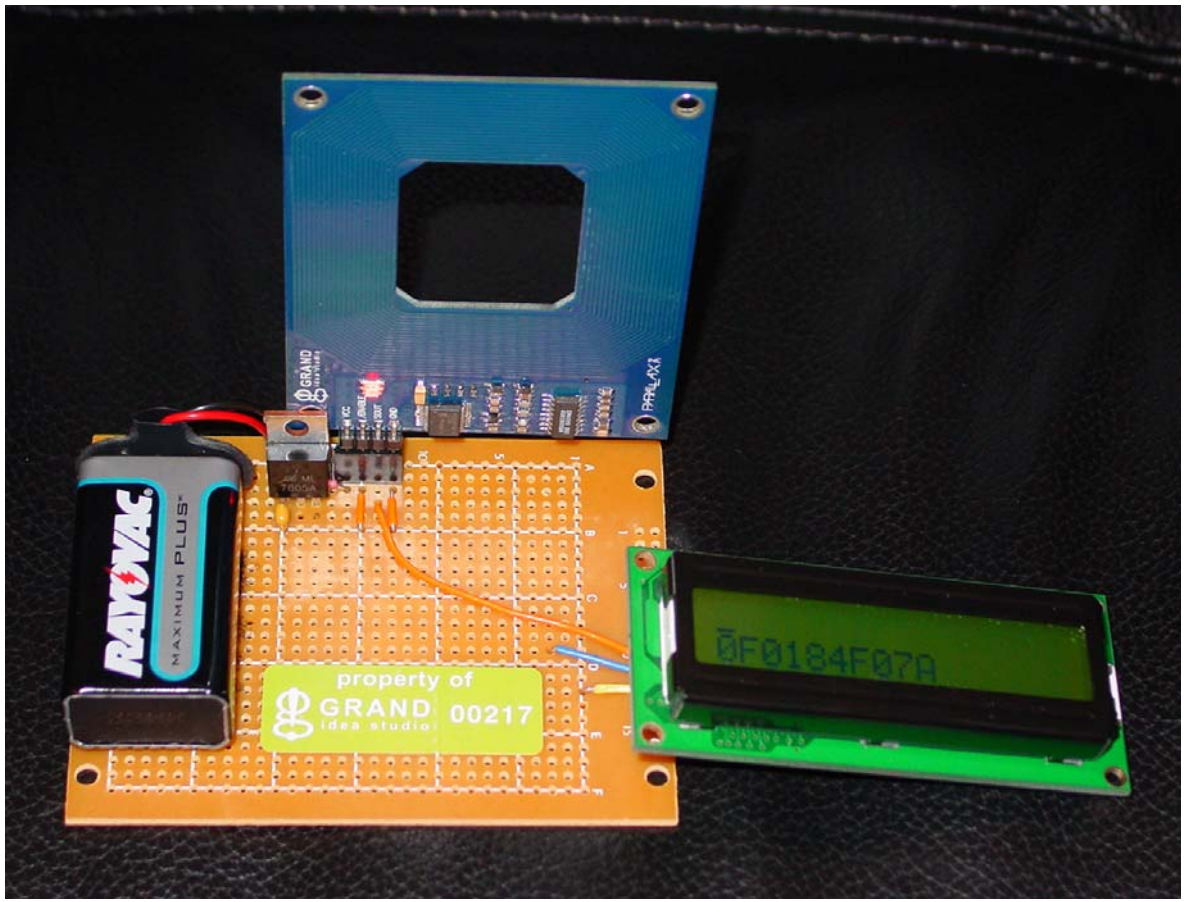
Making a Portable RFID Reader 3

- If a valid tag is read, the RFID Reader Module sends a 12-byte ASCII string containing the tag's unique ID via simple serial interface
- By connecting the output to an off-the-shelf Serial LCD Module, we can see any RFID tag IDs that are in the vicinity
  - **Ex.: Parallax 2x16 Serial LCD Backlit, `www.parallax.com/detail.asp?product_id=27977`**

Making a Portable RFID Reader 4



Making a Portable RFID Reader 5



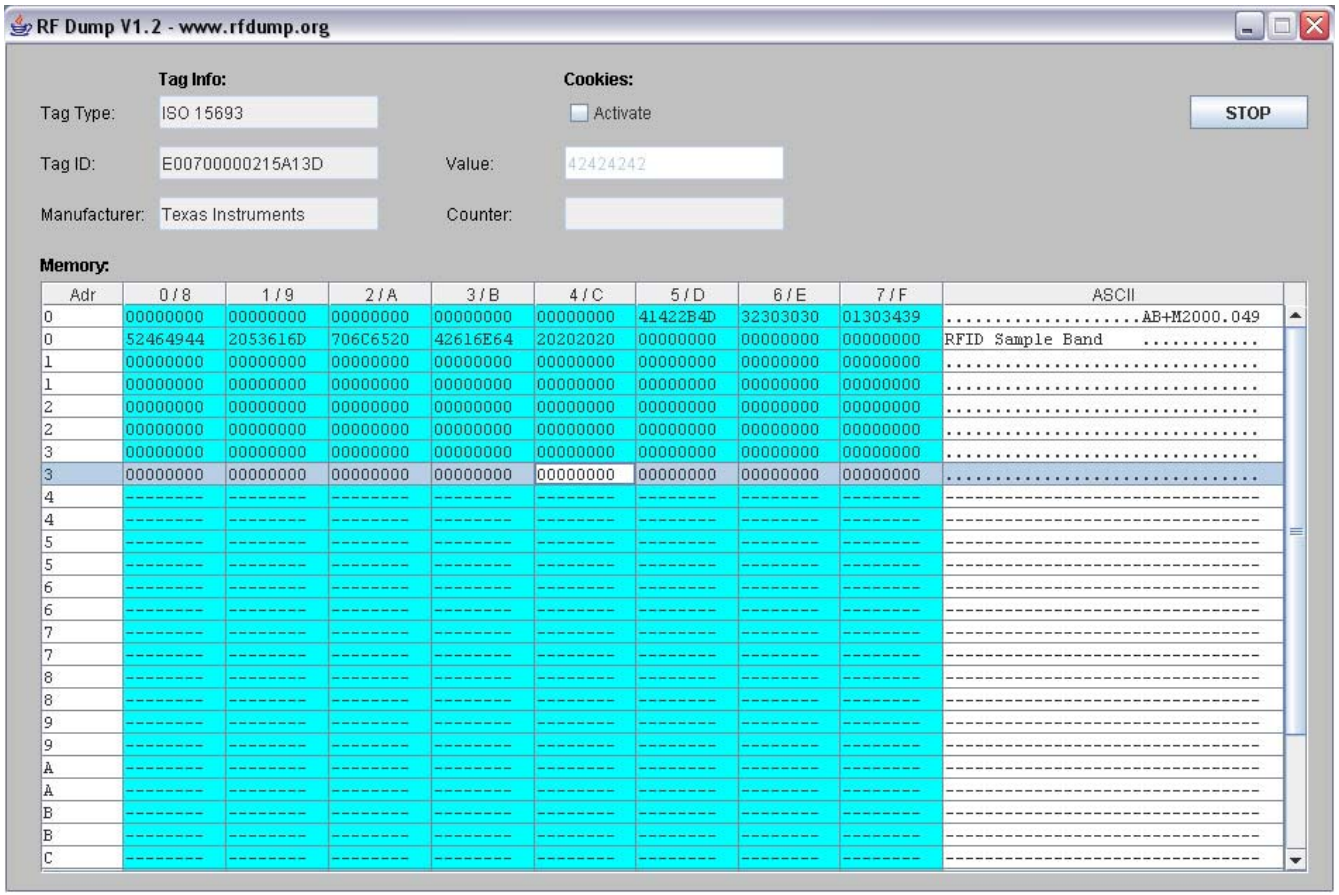
SECURITY WORLD CONFERENCE & EXPO 2006

MIS TRAINING INSTITUTE

Making a Portable RFID Reader 6

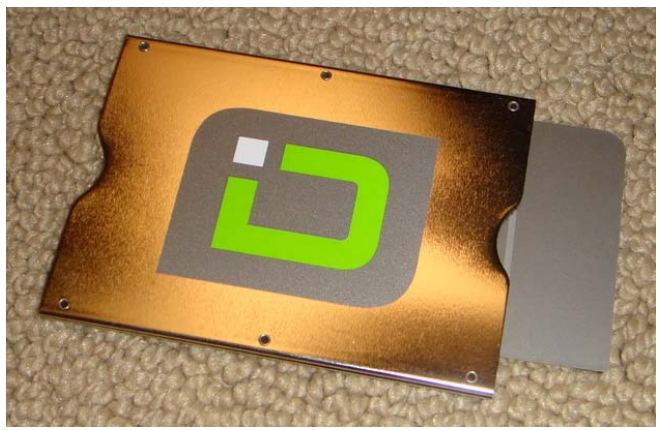
- ACG Identification Technologies' H102022 13.56MHz RF PC Handheld Reader Module (**`www.acg.de`**)
  - **Uses CompactFlash (CF)/PCMCIA interface to connect to PC or PDA**
  - **Supports ISO 15693 (Tag-it ISO, My-d, I-Code SLI, LRI512, TempSense), ISO 14443 A (Mifare Standard, Mifare UltraLight), ISO 14443 B (SR176)**
- RFDUMP (**`www.rf-dump.org`**), by Lukas Grunwald and Boris Wolf, allows complete reading/writing support of the above tags using the ACG reader
- RFIDIOt (**`www.rfidiot.org`**) by Adam Laurie, an open-source python library for exploring RFID devices

Making a Portable RFID Reader 7



Protection Methods?

- Secure Sleeve (formerly SMARTSHIELD), **`www.idstronghold.com`**
  - **Blocks the magnetic field emitted by LF/HF tags**
    - Prevents tag from receiving power it needs to operate
  - **Approximates a Faraday Cage to block any electric field from entering or exiting the shield**
  - **Works great with the tags I've tested!**



Protection Methods? 2

- Low-Tech: Tinfoil to create Faraday Cage
  - **Intended for capacitively-powered (UHF) tags**
  - **Will not stop inductively-powered (LF/HF) tags**

Conclusions

- Current RFID technologies are open to attack
  - **Can lead to identify theft, privacy breaches, and theft-of-service**
  - **RFID tags can easily be read through clothing, from large distances (up to ~50 ft.), and without detection**
- Most RFID systems/software are not designed with security in mind
  - **Challenge/response and rolling code tags > ID/stored value, but still not unbreakable**

Conclusions 2

- Overall privacy/security issues should be seriously considered before making a switch to RFID
  - **Understand what data is being stored on the tags**
  - **Evaluate all technologies before deployment**
- Protect access to RFID tags and data whenever possible

Resources: Magazines

- RFID Journal, **`www.rfidjournal.com`**
- RFID Gazette, **`www.rfidgazette.org`**
- RFID News, **`www.rfidnews.org`**

Resources: Vendors

- IDmicro, **www.idmicro.com**
- ActiveWave, **www.activewaveinc.com**
- On Track Innovations, **www.oti.co.il**
- Sokymat, **www.sokymat.com**
- ACG Identification Technologies, **www.acg.de**
- Texas Instruments, **www.ti-rfid.com**
- RSI ID Technologies, **www.rsiidtech.com**
- EM Microelectronic, **www.emmicroelectronic.com**

Resources: Web Sites/Articles

- RSA Laboratories: RFID Privacy and Security, **www.rsasecurity.com/rsalabs/node.asp?id=2115**
- Spychips: RFID Privacy Website, **www.spychips.com**
- MAKE: Blog: Interview with RFID implanter, **www.makezine.com/blog/archive/2005/04/interview_with_1.html**
- Proposal to Implant Tracking Chips in Immigrants, **www.livescience.com/scienceofficiton/060531_rfid_chips.html**

Resources: Presentations

- Lukas Grunwald, RF-ID and Smart-Labels: Myth, Technology and Attacks, Black Hat Briefings USA 2004, **www.blackhat.com/presentations/bh-usa-04/bh-us-04-grunwald/bh-us-04-grunwald.pdf**
- Kevin Mahaffey, Passive RFID Security, **www.blackhat.com/presentations/bh-usa-05/bh-us-05-mahaffey.pdf**
- Melanie Rieback, A Hacker's Guide to RFID Spoofing and Jamming, DEFCON 14
- Lukas Grunwald, First We Break Your Tag, Then We Break Your Systems: Attacks to RFID Systems, DEFCON 14

Resources: Books

- RFID Security, Frank Thornton, et al., ISBN 1597490474
- RFID Toys, Amal Graafstra, ISBN 0471771961, **`www.rfidtoys.net`**

Thanks!

Joe Grand
Grand Idea Studio, Inc.

joe@grandideastudio.com