Radio Frequency ID (RFID)

CSI Asia 2004

John O'Leary, CISSP

Computer Security Institute

Abstract -1

We've read some articles in trade pubs. We've felt the buzz. "RFID is the future. RFID is coming soon. RFID is here, and you better be ready for it. RFID will revolutionize how we do business." We might even have heard our physical security guys or warehouse group talking about how they're going to implement RFID for inventory control or article surveillance or building access or something else. But we're IT security people, and we know that RFID involves wireless communication, so we're concerned. However, we don't know exactly what to be worried about, or what to do about our nebulous fears, or how to convince management to allocate us the resources we need to definitively analyze the threats and build a structure of appropriate countermeasures.

Abstract -2

In this session, we'll look at RFID – what it is and how it can be used – and try to give, or at least approach a more definitive focus for our security concerns. We'll do a basic overview of the technology and then put our security hats on to analyze some specific implementations, looking for threats, vulnerabilities, countermeasures, implementation strategies and ways to explain and sell RFID security throughout our organizations.

Format

- Exchange of ideas
- Open to questions at any time
  - Anyone can ask
  - Anyone can answer
- RFID relevance to your organization
  - Now
  - 2005 (if you're a Walmart partner)
  - Future

Overview

- Multiple technologies using RFID
- Some fit together well, some don't
- Major users driving suppliers to convert
- Security issues exist
- Privacy is a concern
- RFID still evolving
- New uses
- Laws trailing

Agenda - RFID

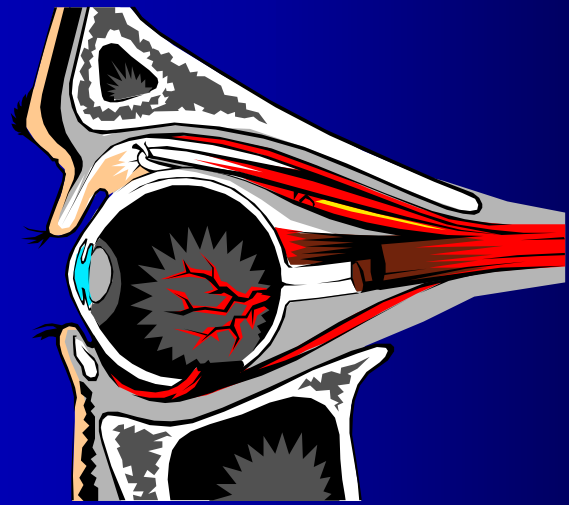
- What RFID is
- How it can be used
- Security issues
- Privacy
- Recommendations

What RFID is

- A subset of Automatic Identification Procedures (Auto-ID)
  - Provide information about
    - People
    - Animals
    - Goods
    - Products in transit
  - A merger of communication and identification technologies

What RFID is

- Automatic Identification Technologies (Auto-ID)
  - OCR
  - Barcodes
  - Smart cards
  - Biometrics
  - RFID

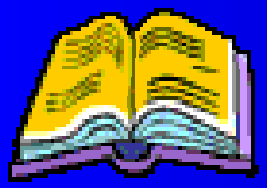


What RFID is

- Why not just use barcodes?
  - They're omnipresent
  - They triggered a revolution in ID Systems
  - They're extremely cheap
  - However…..
  - They have low storage capacity
  - They cannot be reprogrammed

What RFID is

- Klaus Finkenzeller -*RFID Handbook, 2E,* 2003 (primary source for this session)
  - "RFID systems are closely related to …smart cards…data is stored on an electronic carrying device – the transponder. However, …the power supply to the data-carrying device and the data exchange between the data-carrying device and the reader are achieved without the use of galvanic contacts, using instead magnetic or electromagnetic fields."



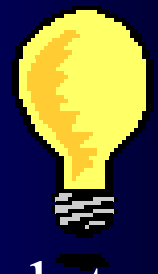
What RFID is

- Hiawatha Bray (Boston.com –***Boston Globe*** 4/12/04)
  - "…These little tiny devices that will soon be used by businesses and the military to wirelessly track cartons of Barbie dolls and crates of ammo. The tags are little radio transmitters with very short range. ……Consumers could even have their own RFID readers built into cellphones. Point it at a circular saw at the Home Depot. Your phone could not only display the price, but automatically log onto a Consumer Reports-type Internet service and display product reviews and prices at competing retailers…."

What RFID is

- Victor Godinez (Dallas Morning News 5/16/04)
  - Wal-Mart Stores, Inc. will require its 100 biggest suppliers to adopt RFID chips on their cases and crates starting next year
  - Target and DoD have also issued 2005 RFID mandates
  - Retail supply chain has always been the "Holy Grail" for RFID
  - Huge demand for systems integrators next 5-10 years
  - Companies hoping to profit are staffing up
  - A tiny technology may soon spark a major hiring drive

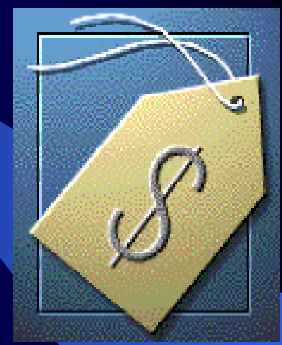
What RFID is



- Dan Kaminski (DoxPara research)
  - RFID…is essentially a Tesla-esque hack to allow contactless, bidirectional storage of small amounts of data on trivial circuits powered by the reader infrastructure itself
  - …What if you could just have a few sensors throughout your warehouse do a "mass ping" and acquire from the mass of replies precisely what needs to be restocked?

Components - ***Transponder***

- Usually built into tags or strips
- Sometimes encased in plastic
- Located on each object you wish to identify and/or track
- May or may not have on-board power supply
- Multiple ways to induce current to communicate to reader
- Must be low cost to make RFID viable



Components - ***Reader***

- Interrogator
- May be “read” or “Read/write” device
- Emanates in a geographic domain to set up field in which to capture data (contactless)
- Characteristics of field may activate the transmitter in the transponder
- Can be built into door or passageway

Transponder Formats

- Disks and coins – most common
- Plastic housing – car keys, immobilization
- Glass housing – animals, construction
- Metal surfaces – tools, gas bottles
- Keys and fobs – high security door locks
- Contactless smart cards – ID1 format
- Smart labels – paper-thin, self-adhesive
- Coil on chip – very small, plastic cased

Transponder Formats

- Disks and coins
  - Transponder in a round, injection-molded housing
  - Diameter up to 10cm
  - Usually a hole for fastening (screw, etc.)
  - May use special materials for temperature operability

Transponder Formats

- Plastic housing
  - For applications with particularly high mechanical demands
  - Housing can be integrated into other products
  - Longer coil than glass gives it greater operational range
  - Vibration tolerant (good for autos)
  - Can accept large microchips

Transponder Formats

- Glass housing
  - Can be injected under the skin of an animal
  - Identification
  - Microchip mounted on a carrier
  - Chip capacitor to smooth the current
  - Internal components in an adhesive for stability
  - For kids??.....the homeless??...employees??

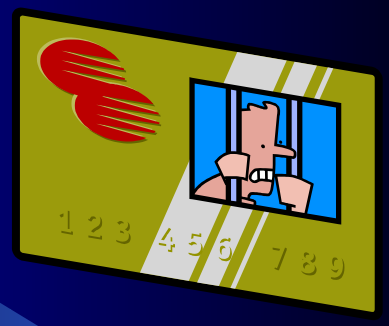
Transponder Formats

- Metal surfaces
  - Tools
  - Gas Bottles
  - Identification
  - Transponder coil wound on ferrite rod
  - Transponder chip mounted on ferrite, contacting the coil
  - Encased in epoxy resin, etc., for stability and temperature tolerance, vibration tolerance

Transponder Formats

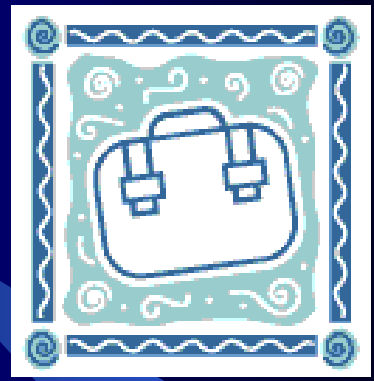
- Keys and fobs
  - Physical access to office and work areas
  - Transponder in a plastic housing
  - Cast or injected into key fob

Transponder Formats



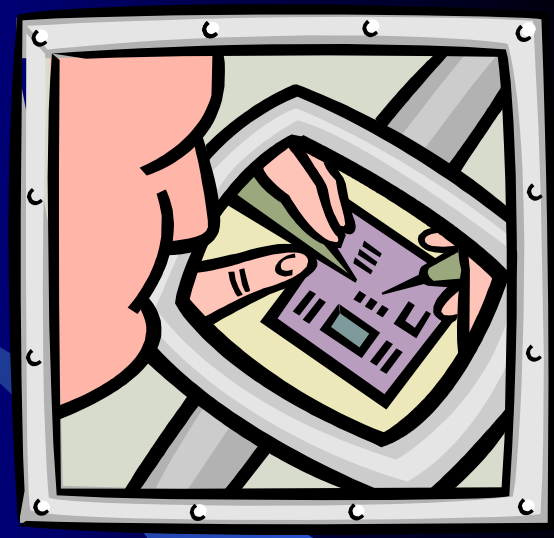
- Contactless smart cards
  - ID1 format (credit cards and telephone cards)
  - Large coil area
  - Increased range
  - Laminate a transponder between 4 PVC foils
  - Foils baked at high pressure above 100C for permanent bonding
  - Affinity and other overprints common

Transponder Formats



- Smart labels
  - Very thin transponder
  - Applied to 0.1mm plastic foil via screen printing or etching
  - Sometimes has an adhesive back
  - Sticky labels, can tie to barcode printed on them
  - Can be used on luggage, packages, books, etc

Transponder Formats



- Coil on chip
  - Integrates the coil onto the chip
  - Microgalvanic process on a CMOS wafer
  - 3mm x 3mm and getting smaller
  - Frequently embedded in a plastic shell

How RFID Can be Used

- Electronic article surveillance
- Metropolitan travel
- Air ticketing
- Ski tickets
- Physical Access control
- Freight transport
- Animal Identification
- Toll Collection

How RFID Can be Used

- Electronic Immobilization
- Container Identification
- Waste disposal
- Sporting events
- Tool Identification
- Industrial production
- Temperature control for transported perishables

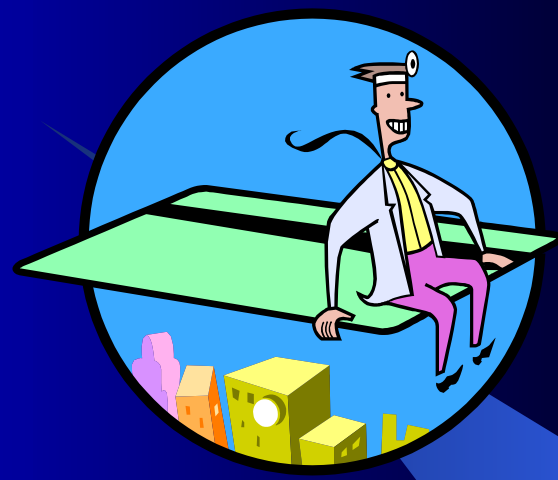
Electronic Article Surveillance

- 1-bit transponder
  - "Transponder in field"
  - "Transponder not in field"
  - Alarm if present (or absent)
  - Go back to clerk and have them remove the tag containing the transponder that got set off by the field generated by the panels bracketing the doorway

Metropolitan Travel

- Automatic fare collection
- Possible electronic payment tie-in
- Seoul, Korea
  - bus card
- Oldenburg, Germany
  - "Fahrsmart II"

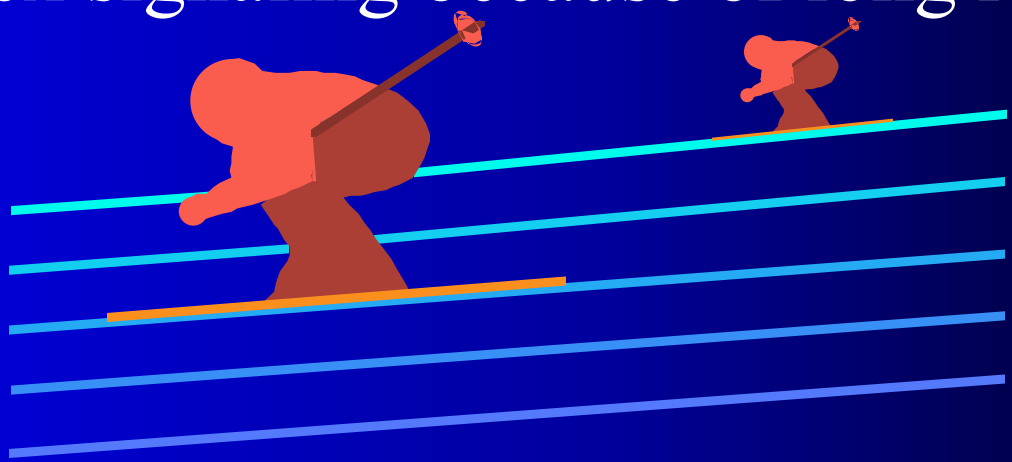
Air Ticketing



- Lufthansa
- Miles and More
- Contactless smart card
- Replaces paper ticket and conventional boarding pass
- Get a ticket with it up to 1 hour before flight

Ski Tickets

- Replaces daily or weekly pass (cardboard, date-stamped)
- Deposit of 5-10 euro plus price of card
- Turnstile senses valid contactless cards
- Complex signaling because of long range



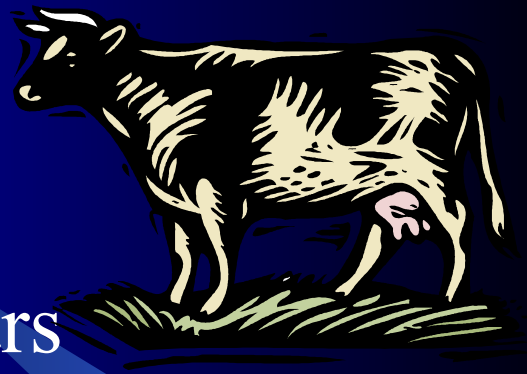
Physical Access Control

- **Online systems** – Small business
  - Large number of people
  - Few entrances
  - Network connection to central DB
- **Offline systems** - Hotel
  - Many locations (rooms, etc.)
  - Smaller number of people with access
  - Transponder programmed at a central station
  - Access info stored on the "key"
  - Can be date sensitive
  - If lost, deactivate that "key" number

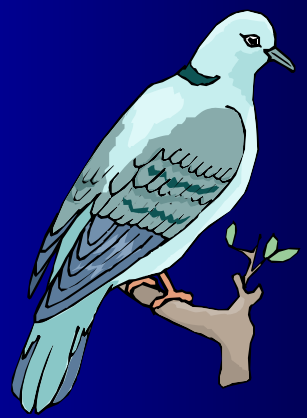
Freight Transport

- For containers – ISO 6346 – unique number
- Used by almost all of the 7 million containers worldwide
- Transponder use avoids transcription errors (up to 30%)
- ISO 10374 in 1991 for this use
  - Owner's code, serial number, test digit
  - Container length, width, height
  - Container type
  - Laden or tare weight
- Battery-powered transponders
  - 10 to 15 year life
  - Same as containers

Animal Identification



- Livestock for more than 20 years
- Heavily used in Europe
- Collar transponders – easily transferable
- Ear tags – readable at distances to 1 meter
- Injectible transponders –
  - Origin verification
  - Epidemic control
- Carrier pigeon races



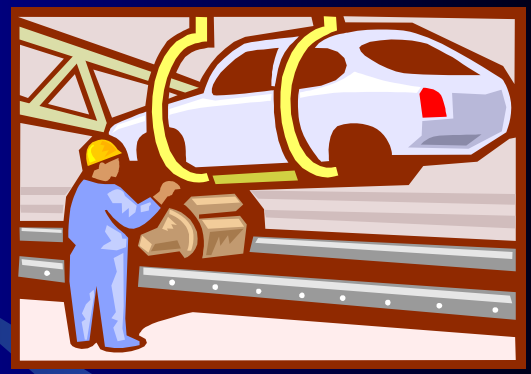
Toll Collection

- Zoom through the toll plaza
- Reader in plaza lane activates chip attached to your windshield
- Chip transmits its ID
- Reader collects data
- Billing ensues
- If “no tag,” take picture of license plate
- Ticket ensues
- “Dog ate my tolltag” doesn’t work

Electronic Immobilization

- Vehicles
- At ignition, reader is activated
- Data exchanged with transponder in ignition key
- 3 possible validity checks
  - Serial number
  - Rolling code (new for each use)
  - Crypto
    - Fixed keys
    - Transponder authenticated by reader
- No validity, no start

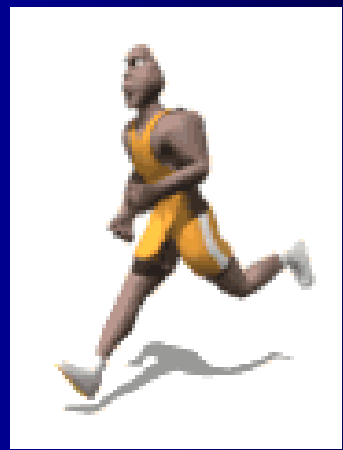
Industrial Production



- General Motors
  - To track carriers that move auto chassis and materials around assembly plants
  - Standards coming from the AIAG (same action group that did EDI standards, etc.)
  - Rewritable RFID chips may soon be built into cars to maintain maintenance histories

Sporting Events

- Marathons
  - Did that crosser of the finish line actually run all 26.2 miles?
  - Transponder on runner's tag
  - Readers at various points along route
  - Need large reading field



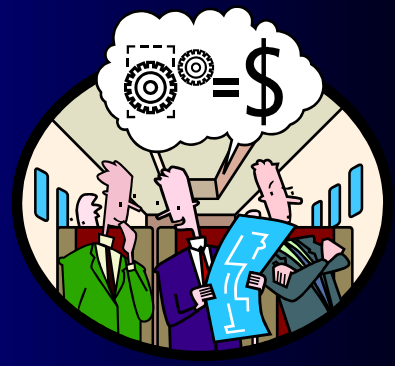
Temperature Control in Transit

- Perishables
- FreshLoc – Internet-based monitoring
  - Warehouses or on the road
  - Trucks and storage sites equipped with sensors
- Dallas Morning News, May 16, 2004
  - "RFID – How cool is that?"
  - "Chips monitor temperature of food in transit"

RFID Security Issues

- Nature of the Beast
- Data Glut
- Misuse or Malfunction
- Business Intelligence
- Military Intelligence
- Tag Blockers

Nature of the Beast



- ***RFID Transmits information to a receiver***

- "Your RFID tag makes 802.11 look like Alcatraz" (Dan Kaminski in a posting on DoxPara)
- Activate the transponder and it'll transmit every time
- No matter what triggered the transmission
- No matter who is in a position to receive it
- If I can activate and collect your access card information while sitting near you on a subway train, maybe I can produce something that lets me access your site as you.

Data Glut

- ***RFID chips, in the billions, will produce mountains of information***

- What plans do we have for handling the growth in incoming data?
- How much and what kind of data do we collect?
- What uses will we make of it?
- How do we recognize what's valuable?

Data Glut

- ***RFID chips, in the billions, will produce mountains of information***

- How do we protect it?
- What do we share with trading partners?
- How do we avoid getting buried by data?
- Ancillary physical problem - What are we going to do with all the RFID chips we generate?

Data Glut

- ***RFID chips, in the billions, will produce mountains of information***

- How do we synchronize what we collect?
- How will we summarize and aggregate all this stuff?
- How smart do the readers need to be?
- What business rules do we use to manage and direct the flood of information?

Misuse or Malfunction of RFID Technology

- ***Immobilizers***

- Trucking business
- Military
- Portable computing devices
- Movement route barriers

Business Intelligence

- ***Open beam RFID transmissions***

- Limited area, …but
- Cleartext
- Collectible
- Standard formats
- How much info are we giving away?
- How sensitive is it?
- How could it hurt us?

Military Intelligence

- ***Intercepted RFID force locators***

- Exactly who is exactly where
  - Unit identifiers
  - Numbers
  - Placement & movement
- Depending on data stored and transmitted and effectiveness of encryption codes
  - Plans
  - Fallback positions
  - Timing

Tag Blockers

- ***Shown at RSA 2004***

- An RFID tag itself
- Ron Rivest
- Prevents scanners from tracking people or goods after purchases have been made

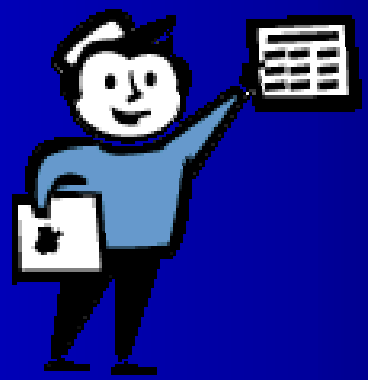
Privacy

- ***The*** "hot button" issue surrounding RFID
- Lots of hand-wringing
- Mumblings of "Big Brother," etc.

- Real worry is for inadvertent disclosure of possibly sensitive information
- Ignorance of what's being given away and what's being collected

RFID and Privacy

- Hiawatha Bray (Boston.com 4/12/04)
  - So what's annoying…?...the prospect of a world in which everything you buy – every single thing – can shout "here I am" to any passerby armed with the right detection gear. Privacy advocates are understandably horrified…"



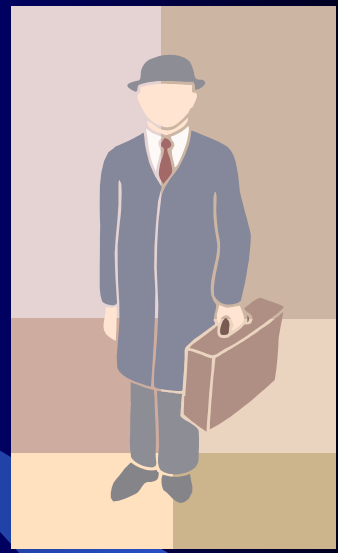
Privacy

- Cal State Sen. Debra Bowen – Feb 04 introduced a bill to regulate RF that can track people or products in retail stores
- 3 requirements
  - Tell customers
  - Get consent to track or collect or sell info
  - Deactivate tags on products before customer leaves the store

Privacy

- Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) pushing for more laws and stringent controls
- Vendors, users, others disagree, especially with disabling the transponder & thus killing stored data
  - "may needlessly and myopically impede the beneficial deployment of RFID" - RSA

Recommendations



- Assign someone to keep up with developments in the area
  - They're coming at a fast and furious pace
  - Identifying a point person helps focus efforts
- Point person should set up a library (books, clippings, website postings, etc.,) and canvass relevant internal and external groups regarding their uses of RFID and security/privacy controls

Recommendations

- See if some RFID is not already at work in your organization
  - Chances are that it is or is in planning stages
  - Evaluate security needs and postures for currently running applications
  - Make sure existing policies are not being violated
  - Make sure security controls are included in planning for future add-ons and new applications

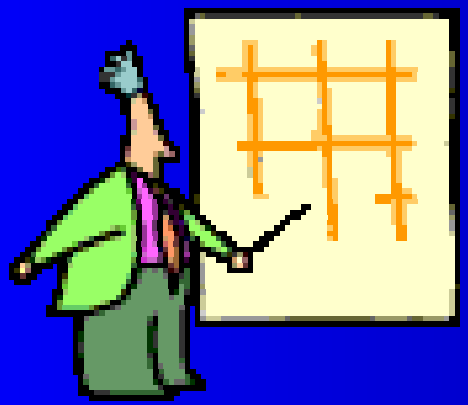
Recommendations

- Check what your trading partners are doing and planning to do
  - Evaluate security requirements and costs from your side and theirs for RFID applications
  - Balance your security policies and requirements and initiatives against theirs
  - Find out what data they're collecting via RFID and how they plan to use it
  - Set up joint teams for RFID integration

Recommendations

- Get your legal department, CPO and PR involved
  - Getting to be a hot political issue
  - Privacy makes headlines and spawns laws
  - Different laws in different venues
  - Changing frequently
  - Must know and comply with the laws wherever you do business
  - Possibility for bad PR is very high

Summary – *We have covered:*



What RFID is
How it can be used
Security issues
Privacy
Recommendations

More RFID Security Information

- ***RFID Handbook, 2E***, Klaus Finkenzeller, Wiley, Chichester, 2003 ISBN 0-470-84402-7

- Google or AOL or … search on "RFID Security"