

Security and Authentication Technologies

power and
direction
power online

Peter Winer
Big Chief Partners, Inc.
pwiner@bigchief.com

RFID-World
May 13, 2003
Fort Lauderdale, Florida



Technology Observations

power and
direction
power online

- Inexpensive tags could
 - Enlarge RFID adoption and/or
 - Delay RFID adoption
- Antenna breakthrough is needed
- Software keys
 - Middleware
 - Infrastructure
 - Systems integrators

RFID promise

power and
direction
power online

“RFID will provide an unprecedented view into a product’s life – changing the way goods are produced, shipped, marketed, and sold.”

Christine Spivey Overby

Forrester Research, Inc.

(RFID: The Smart Product (R)evolution, 8/02)

Security Problem

power and
direction
power online

“RFID systems are different from other means of identification because RF communication is non-contact and non-line-of-sight... It is more difficult for the owner of the RF tag to physically impede communication with the tag.”

Sanjay E. Sarma, Stephen A. Weis, Daniel W. Engels
Auto ID Center
Massachusetts Institute of Technology
(RFID Systems, Security & Privacy Implications, 11/02)



Introductory Comments

power and
direction
power online

- Security is a major, extensive issue in RFID-based systems.
- A system overview will provide the context for this presentation.
- Focus will be issues that are specifically relevant to RFID.
- General network security issues will not be extensively covered.
- These security issues are relevant in multiple RFID applications and markets.



Peter Winer: Background

power and
direction
power online

- Computer scientist by training
- Interest and focus on RFID for about 2 years
- My company built WebLink for Philips Semiconductors
- I am particularly interested in RFID Infrastructure

Big Chief Partners

power and
direction
power online

- Company: 10 years of...
 - Software development
 - Business evaluations for investors
 - Strategic consulting
- People turning technology into business

Methodology

power and
direction
power online

- Input from vendors & customers
- Auto ID Center
- Analysts
- Our own original thinking
- Experience building, deploying WebLink



WebLink from Philips Semiconductors

power and
direction
power online

- RFID Infrastructure and Services
 - Middleware: event management & trust
 - Reader application platform
- Platform is desktop, hand held computers and gaming consoles
- Industrial and consumer applications
- For more information:
 - <http://semiconductors.philips.com/identification/markets/weblink>
 - <http://weblink.philips.com>



Overview

power and
direction
power online

- Definitions
- Security and Authentication
- Case Studies
- Companies to Watch
- Questions and Discussion

Definitions

power and
direction
power online

Security: Freedom from danger or risk

Authentication: To establish as genuine, valid or authoritative

Focus for Security in RFID-based Systems

power and
direction
power online

- RFID security should focus on end-to-end security and authentication of the information flow from RFID tags to the destination in enterprise applications
- The goal is to guarantee integrity and prevent intrusions.

Links in the Information Flow Chain

power and
direction
power online

- Tag to Reader
- Reader to the network edge
- Within the network
- Delivery to enterprise application

Focus for this Presentation

power and
direction
power online

- Detailed focus on securing and authenticating access to RFID tags.
- The steps within the network are interesting, but not specific to RFID.
- Skipping generic network issues will allow more time to dive deeper and provide more unique information on RFID-specific issues.

Tag Types with Varying Levels of Security

power and
direction
power online

- ePC Class 0 and 1
- Read/Write memory with write protection
- Secret keys for protecting memory access
- Shared secret encryption
- Public Key Infrastructure (PKI)
- Java Card Operating Platform (JCOP)
- Global Platform

ePC Class 0 and 1

power and
direction
power online

- Unique identity that is locked during manufacturing process
- Cyclic Redundancy Check (CRC) for identity verification
- KILL command that erases the unique identity and makes tag unresponsive to queries
- ePC Class 2 and 3 are under design but not disclosed beyond Auto ID Center membership
- These classes build on the functionality of ePC Class 0 and 1



Read/Write Memory with Write Protection

power and
direction
power online entire

- Small amount of memory (less than 1K)
- Divided into blocks with a write-protect flag for each block
- Write-protection can be set but not cleared

Secret Keys for Protecting Memory Access

power and
direction
power online

- Larger amount of memory (1K – 4K)
- Divided into sectors, each containing a group of blocks
- Each sector has two secret keys and a set of permissions for each key
- Typically, one key grants 'user' access and the other grants 'administrator' access

Shared Secret Encryption

power and
direction
power online

- Larger amount of memory (Up to 16K today)
- Divided into variably sized files with limited file system functions
- All information transfer is encrypted using shared secret keys
- Typically use DES, 3DES and AES encryption methods

Public Key Infrastructure (PKI)

power and
direction
power online

- Includes feature set of shared secret encryption tags
- Tag is queried for it's public key
- Reader client produces challenge encrypted with public key
- Tag produces response by decrypting with private key
- Tags can support multiple key pairs granting different levels of access



Java Card Operating Platform (JCOP)

power and
direction
power online

- Includes feature set of shared secret encryption and PKI tags
- Tag implements *minimal* Java Virtual Machine (JVM)
- Enables limited application-specific logic on tag
- Emerging standard for payment systems

Global Platform

power and
direction
power online

- Standard promoted by Visa International
- Allows choice of operating platforms including JCOP and Multos
- Allows choice of languages including Java and Visual Basic
- Recommended standard for Bank-issued credit cards
- EMV is a competing standard

Reader to Network Security

power and
direction
power online

- Wide variety of
 - Reader interface capabilities
 - Reader connection topologies
- Emerging space, still subject to major landscape shifts
- Readers with Internet interfaces emerging

Four Reader to Network Interface Configurations

power and
direction
power online

- Serial-based
- TCP/IP-based (with or without XML-based Web Services)
- Embedded reader modules
- Gateway server appliances
- Wired and wireless connections

RFID Applications that Require Security and Authentication

power and
direction
power online

- Bank-issued credit cards
- Toll roads
- Mass transit
- Electronic cash
- Identity and loyalty cards
- Pharmaceuticals

Case Study #1: Octopus Card, Hong Kong

power and
direction
power online

- Electronic cash system, launched in 1998
- Originally focused exclusively on mass transit
- Recently expanded to include retailers and vending machines
- Early problems due to overwhelming demand



Octopus

power and
direction
power online

- 7,000,000 cards in active use
- Average 36 transactions per card per month (by far the world's highest)
- \$6,000,000 in transactions per day
- 95% of HK residents aged 15-65 own an Octopus card
- Anonymous stored value or tied to credit card account

Octopus

power and
direction
power online

- Based on Sony Felica card
- Stored value implemented as an electronic purse
- Mutual, two-way authentication using PKI and random challenge
- Octopus has never been successfully hacked

Case Study #2: Smart Bands at Amusement Parks

direction
power online

- Smart Bands developed by Precision Dynamics
- RFID inlay is embedded in plastic wrist band
- Cannot be removed without destroying the wrist band
- Deployed with Philips and TI tags

Smart Bands for Providing Safety

power and
direction
power online

- Implemented for Hawaiian Adventures water theme park
- Employs Philips I-Code tag (ISO 15693)
- Groups attending park share a unique identity
- Group leader is also uniquely identified
- Members check in at Kiosks
- Instant messaging between Kiosks
- Provides safety for groups attending the park



Smart Bands for E-Commerce

power and
direction
power online

- Implemented at two Georgia theme parks
- Employs TI tag
- Smart Band stores cash and is debited whenever a purchase is made
- Also supports a floating locker system.



Smart Bands Summary

power and
direction
power online

- Utilizes read/write capabilities
- Good candidate for elevated security functions

RFID Security Companies to Watch

power and
direction
power online

- PKI Software
 - Ntru
 - ARM
 - Mips
- ePC Class 1 Support
 - Matrics
 - Alien Technologies
- Chips
 - Philips
 - Texas Instruments
 - Infineon
 - Sony
 - Hitachi

Companies to Watch

power and
direction
power online

- Tags
 - Alien Technologies
 - EmbedTech
 - Impinj
 - Intellex
 - Matrics
 - NanoPierce
 - Paralec

Companies to Watch (cont'd)

power and
direction
power online

- Readers and Printers
 - ThingMagic
 - SAMSys
 - Zebra
 - Symbol
 - Intermec

Companies to Watch (cont'd)

power and
direction
power online

- Infrastructure
 - Ember
 - Globe Ranger
- Solutions
 - Apexion
 - Oat Systems
 - Savi
 - Vizional
 - WhereNet



Companies to Watch (cont'd)

power and
direction
power online

- SIs
 - Accenture
 - IBM Global Services
 - Innovision
 - Intellident
 - Burall Infosmart
 - Traxus Technologies

Future Direction

power and
direction
power online

- Focus on Identification applications and markets
- Continued interest in RFID infrastructure
- Working to identify next generation RFID-based opportunities

Discussion and Questions

power and
direction
power online

Peter Winer
Big Chief Partners, Inc.
pwiner@bigchief.com

RFID-World
May 13, 2003
Fort Lauderdale, Florida



Resources

power and
direction
power online

- Big Chief

- <http://www.bigchief.com>
- <http://weblink.philips.com>
- <http://semiconductors.philips.com/identification/markets/weblink>

- Analysts

- AMR: Bruce Richardson
- Forrester: Christine Spivey Overby
- Gartner: David Flint

- Industry Associations

Auto ID Center	AIM (Assoc. for Automation Identification & Data Capture)
ISO	AIAG (Automotive Industry Action Group)
UCC	ANSI

- Trade Shows

RFID World 5/13	RFID In Action (London) 5/30 – 5/21
RFID Journal Live! 6/11	Sensors Expo 6/3

- RFID Proponents

P&G	Gillette	WalMart
SAP	Philips	Marks and Spencer



Commercial Tag Configurations

power and direction
power online

Frequency	Benefits	Limitations
Low (125-134Khz)	<ul style="list-style-type: none"> Worldwide acceptance Works near metal Wide current use 	<ul style="list-style-type: none"> Limited read-range (1.5m)
High (13.56Mhz)	<ul style="list-style-type: none"> Worldwide acceptance Works in moist environ. Wide current use 	<ul style="list-style-type: none"> Doesn't work near metal Limited read-range (1.5m)
UHF (868-928 Mhz)	<ul style="list-style-type: none"> Longer read-range (>1.5m) Rapid commercial growth 	<ul style="list-style-type: none"> Not licensed in Europe Detuning when in close proximity Doesn't work when moist
Microwave (2.45Ghz)	<ul style="list-style-type: none"> Longer read-range (>1.5m) 	<ul style="list-style-type: none"> Not licensed in Europe Complex systems dev. Not in wide use

Source: Forrester Research, Inc., "RFID: The Smart Product (R)evolution" (8/02)



Thank You!

power and
direction
power online

Peter Winer
Big Chief Partners, Inc.
pwiner@bigchief.com

RFID-World
May 13, 2003
Fort Lauderdale, Florida

