

Security, Authentication, Privacy and Trust

power and
direction
power online

RFID Dev Con

Chris Meisl
Big Chief Partners, Inc
November 10, 2004



Why Does Security Matter?

power and
direction
power online

- Need authentic, private and trusted transactions
- Reducing transaction risk
- Specific to wireless (e.g. RFID)
 - Broadcasting proprietary data
 - Non physical access
 - Limited computational capacity

How to Approach Security

power and
direction
power online

- Cost vs. benefit
 - What is the value of the transaction being protected?
- Stay ahead
 - Security is a race against attackers
 - Understand sophistication of attackers

Examples

power and
direction
power online

- EPC
 - Virtually no security available
 - Value of transactions cannot be high
 - Products must be protected by other means
- Smartcards (e.g. EMV)
 - Extensive security possible
 - Value of transactions high

Common Deployments with Security

power and direction
direction
power online

- Octopus and EZLink (Sony FeliCa)
- SpeedPass, Dexit, PowerPay (TiRFID)
- Mastercard Paypass (Philips and others)



Components of security

power and
direction
power online

- Authentication
 - Who can access the system
- Authorization
 - What they are allowed to do
- Integrity
 - Information is not corrupted
- Confidentiality
 - Information is private
- Proof of transaction
 - Non-repudiation

Kinds of Security

power and
direction
power online

- Physical – defending the device
 - Tamper proof packaging
 - Hardened packaging
- Logical – defending the connection
 - Encryption
 - Frequency hopping
- Auditing
 - Track state and look for unusual events
 - CC fraud protection, tag pedigree

Where is the Risk?

power and
direction
power online

- Tag – Reader interface
 - Over the air communication
 - Forward and backward range
- Reader – Host interface
 - Wire or air
 - Onboard storage
- Upstream
 - Use established security protocols

Failures

power and
direction
power online

- Eavesdropping – listening in
 - Reading tag contents
 - Location privacy by tracking id or product constellation
- Spoofing – pretending to be something
- Tampering – changing something
- Copying – duplicating something
- Disabling – preventing access
 - Triggering kill switch
 - Denial of service

Cryptography

power and
direction
power online

"Cryptography is about communicating in the presence of adversaries" [Rivest]

- Protocols
- Encryption
 - Symmetric
 - Based on previous agreement of shared secret
 - 3DES, AES
 - Asymmetric
 - No previous agreement required
 - Used to exchange key for symmetric encryption
 - RSA

Cryptography Infrastructure

power and
direction
power online

- PKI
 - Certificate Authorities
- Standards
 - 3DES, AES, SSL
- Implementations
 - Java
 - .NET
- Crypto processors

Authentication

power and
direction
power online

- Who can access the system
- Is it the same person
- Methods
 - Passwords
 - Challenge-response identification
 - Specialized methods

Passwords

power and
direction
power online

- Weak authentication
 - Secret never changes
 - Secret transmitted in the clear
- Easy to break
 - Eavesdropping
 - Dictionary attack

Challenge - Response

power and
direction
power online

- Time-variant challenge
- Response based on shared secret mixed with challenge
- Variation in challenge increases difficulty in determining shared secret
- Public Key Infrastructure (PKI)

Specialized Authentication

power and
direction
power online

- Zero knowledge proofs
 - Sequence of challenges
- Hash-based access control
 - Lock and unlock access
- Pseudonyms
- Randomized access control
- Silent tree walking

Authorization

power and
direction
power online

- Usually built into authentication
- Access control list (ACL)
- Access audit
- On-chip application separation

Integrity

power and
direction
power online

- Ensuring the message is correct
 - Multiple reads with compare
 - Checksum
 - Message authentication code (MAC)
 - Digital Signature

Confidentiality

power and
direction
power online

- Message privacy
 - What rights does each party have
 - Ensuring that expressed rights are enforced
- Read/Write lock
- Re-encryption

Proof of Transaction

power and
direction
power online

- Non-repudiation of contract implicit in transaction
- Use trusted third party (escrow)
- Generate unique, shared digital signature

Privacy

power and
direction
power online

- What is a company's responsibility to customers?
 - Financial Sector – competitive advantage
 - Healthcare Sector – legislation (HIPAA)
- Start with policy
- Implement with technology
- Enforce

Privacy – Proper Use

power and
direction
power online

- Will copyright law apply to personal data?
 - Who owns personal data?
 - Can it be licensed?
 - DRM for personal data
- Does the simple existence of RFID violate privacy?
- Example: Passports

RFID Bill of Rights

power and
direction
power online

- Consumer knows which items have tags
- Consumer can remove/deactivate tags after purchase
- Consumer can access data associated with tags
- Consumer can access services without requiring tag
- Consumer knows when, where, why of data usage

Privacy – Protection

power and
direction
power online

- EPC
 - Kill switch
 - Blocker tag
 - Faraday cage
- Smartcards
 - Leverage cryptographic capabilities

Conclusion

power and
direction
power online

- Security is about proper implementation of well defined protocols
- Need security mindset throughout an RFID system implementation and deployment
- Developers must have a base understanding of security protocols and tradeoffs – do not depend on the infrastructure to “take care of it”

Questions

power and
direction
power online

RFID Dev Con

Chris Meisl
Big Chief Partners, Inc
chris@bigchief.com
November 10, 2004

