
Security Issues in RFID systems

By

Nikhil Nemade

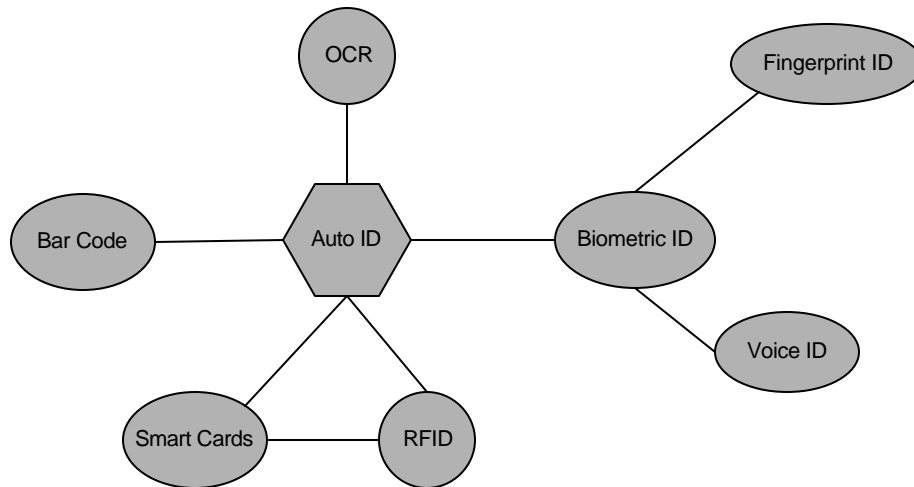
Krishna C Konda

Agenda

- Introduction to an RFID System
 - Possible Application Areas
 - Need for Security
 - Vulnerabilities of an RFID system
 - Security Measures currently employed
-

Auto ID systems

Broad classification of the Auto-ID systems



■ What is Automatic Identification

- A host of technologies that help machines identify objects
- Coupled with automatic data capture
- Increase efficiency, reduce data entry errors, and free up staff

Introduction to RFID Technology

- Acronym for Radio Frequency Identification
 - Enables automatic identification (unique) of physical objects through radio interface
-

RFiD Systems

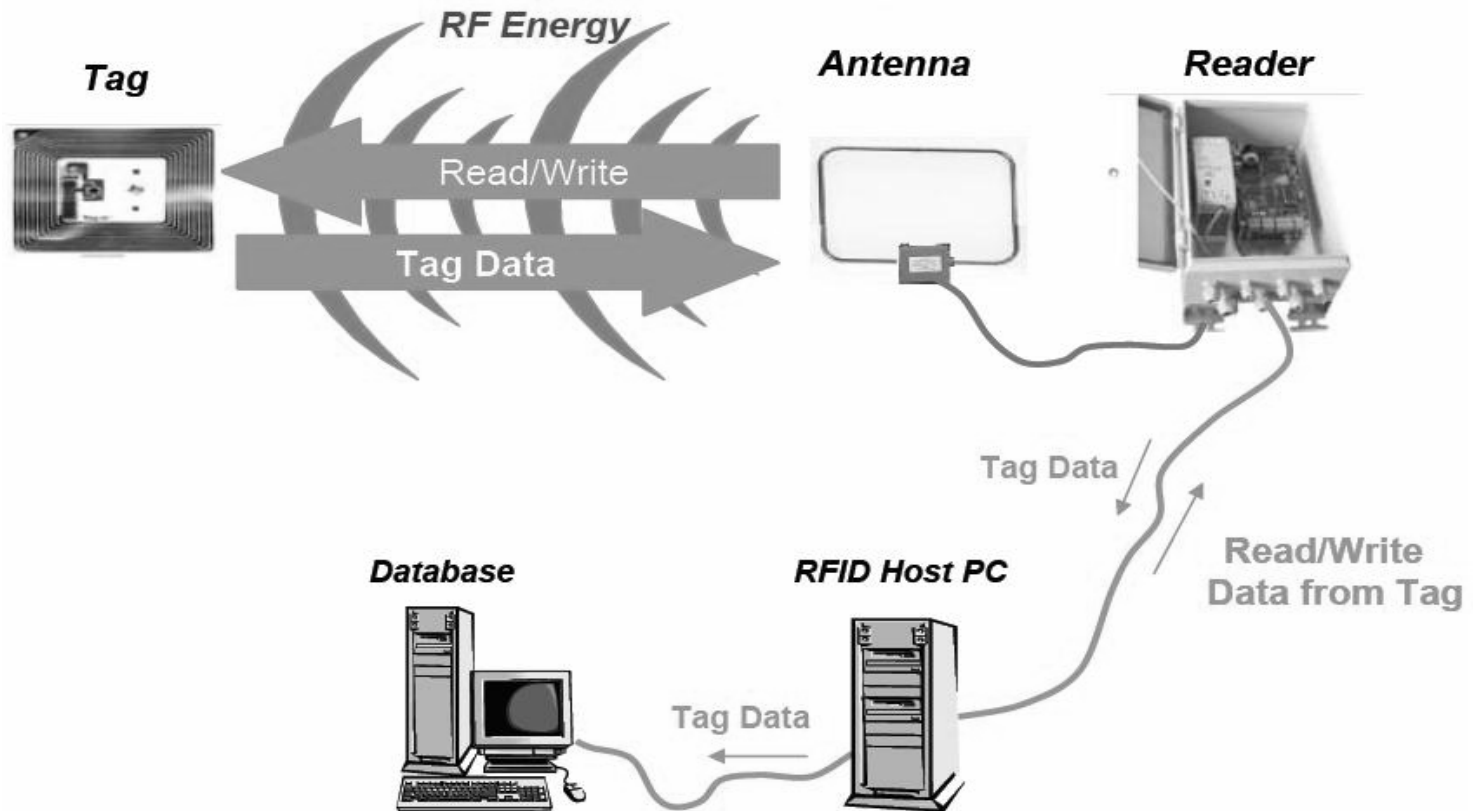
- Three main components:
 - **Tags**, or *transponders*, carry identifying data.
 - **Readers**, or *transceivers*, read or write tag data.
 - **Back-end databases** associate records with tag data collected by readers.
-

RFiD Systems cont.

- Every object to be identified in an RFID system is physically labeled with a tag.
 - Tags consist of a microchip attached to an antenna.
 - Readers query tags via radio signals and the tags respond with identifying information.
-

RFiD Systems cont.

Illustration of a passive RFiD System



RFiD Tags

- The RFiD Tags can be classified on the following basis
 - Active / passive
 - LF / HF / UHF / micro
 - Read-only / read-write
 - State-machine / CPU
 - n-bit / 1-bit
-

RFiD Tags cont.

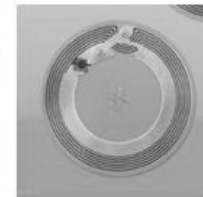
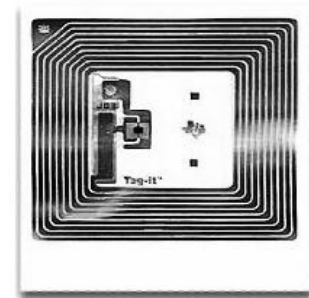
- They are classified as
 - Passive Tags
 - All power comes from a reader's signal
 - Tags are inactive unless a reader activates them
 - Cheaper and smaller, but shorter range
 - Semi-passive tags
 - These have battery power for the circuitry – so can function in absence of a reader
 - Communication is through the power that comes from the reader's signal
 - Active tags
 - On-board battery power
 - Can record sensor readings or perform calculations in the absence of a reader
 - Longer read range but costly
-

RFiD Tags cont.

Characteristics	Passive RFID tag	Active RFID tag
Power Source	Provided by a reader	Inbuilt
Availability of power	Within the field of reader	Continuous
Signal Strength (Reader to Tag)	High	Low
Signal Strength (Tag to Reader)	Low	High
Communication range	< 3meters	>100 meters
Tag reads	< 20 moving tags @ 3mph in few seconds	>1000 moving tags @ 100mph in 1 sec
Memory	128 bytes	128 Kbytes
Applicability in supply chain	Applicable where tagged items movement is constrained	Applicable where tagged items movement is variable and unconstrained

RFiD Tags cont.

- RFiD tags can take various forms depending on the applications they are used for



RFiD Tags cont.

■ Power classification of RFiD tags

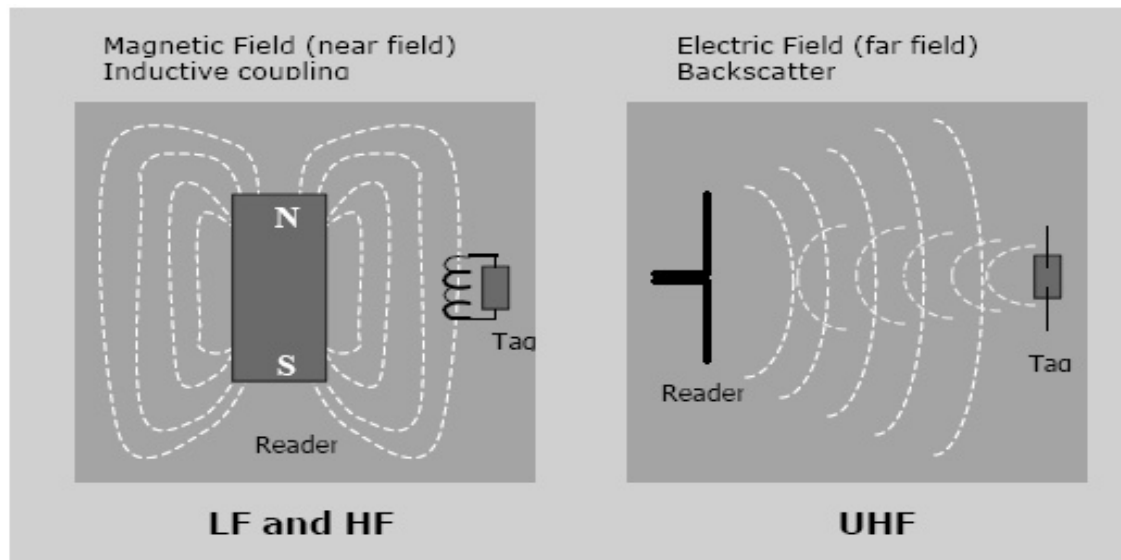
Range Class	LF	HF	UHF
Frequency Range	120-140 MHz	13.56 MHz	868-956 MHz
Maximum Range?	3 meters	3 meters	10 meters
Typical Range	10-20 centimeters	10-20 centimeters	3 meters

RFiD Readers

- Queries for tags by sending out radio waves
 - Can be handheld or stationary
 - They are composed of
 - Transmitter
 - Receiver
 - Antenna
 - Microprocessor
 - Memory
 - Controller or Firmware
 - Communication channels
 - Power
-

RFiD Readers cont.

- Readers are different for different frequencies
 - Inductive Coupling
 - Backscatter Coupling



RFiD Readers cont.

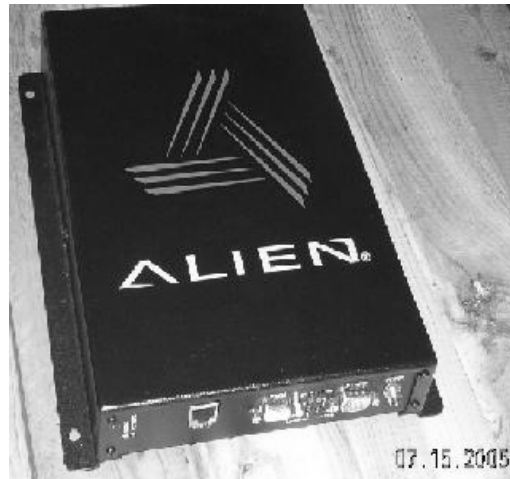
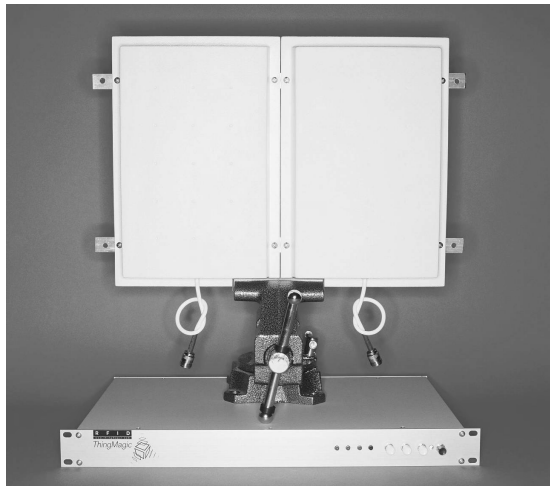
- Modulation
 - The characteristics of radio waves are changed to encode data and transmit
 - Techniques employed depend on power consumption, reliability and bandwidth – ASK, PSK, FSK

 - Encoding – chosen from the many available techniques (NRZ, Manchester etc) based on the protocol employed by the reader to read the tags

 - Anti-collision protocols
 - Tag anti-collision
 - Aloha/Slotted Aloha
 - Deterministic binary tree walking
 - Query tree walking
 - Reader anti-collision
 - TDM
 - FDM
-

RFiD Readers cont.

- The shape and size of the readers again depend on the application they are used for



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

RFiD Applications

- Healthcare
 - Access control
 - Logistics / Supply chain
 - Shopping
 - Travel – passport
 - Traffic – Fast-lane and E-Z pass
-

RFiD Applications cont.

- Hypertag (advertisement) – read info like movie that are playing, ads, info regarding an item on sale etc using mobile etc
 - Payment systems – Mobil Speedpass
 - Animal tracking
 - RFiD appliances – refrigerator, closet etc
 - Automobile immobilizers – anti theft devices
-

Need for security

- Current RFID systems unsafe
 - No authentication
 - No friend/foe distinction
 - No access control
 - Rogue reader can link to tag
 - Rogue tag can mess up reader
 - No encryption
 - Eavesdropping possible (esp. reader)
-

Need for security cont.

- So far none of the RFiD protocols have been standardized – closely guarded secrets, but susceptible to reverse engineering
 - The first attempt at standardization is the Electronic Product Code (EPC) by EPCGlobal – public knowledge, so can easily be broken into
-

EPC Standard

- There is a 96-bit tag that is used to identify the tags. It consists of
 - Header
 - EPC manager (identifies the company)
 - Product code (identifies the product)
 - Serial (uniquely identifies the product)

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

- The 96-bit tag is to be extended to 128-bits, later to be extendable to 256-bits

EPC Standard cont.

- EPCglobal Network consists of five component
 - Electronic Product Code (EPC) number
 - ID system (tags and readers)
 - EPC middleware
 - Discovery Service (ONS)
 - Information service
-

EPC Standard cont.

EPC Class	Definition	Programming
Class 0	Read-only tags	Semiconductor manufacturing
Class 1	Write-once, read-many passive tags	Personalization
Class 2	Rewriteable passive tags	Many times (65 KB read-write)
Class 3	Semi-passive tags	Many times (65 KB read-write)
Class 4	Active tags	Many times
Class 5	Readers	Communicates with other class tags and devices

EPC Standard cont.

- The following protocols are available
 - Generation 1 Class 0 and Class 1 protocol
 - Read only – Class 0, write-once – Class 1
 - Both use different air protocols to communicate – can not communicate with each other and different readers are required to talk to them
 - Generation 1 Class 2 protocol
 - Includes write-many – can respond to both air protocols
 - Generation 2 protocol
 - Common air protocol across all classes of tags
 - Orthogonal to Gen1 – co-exists but not backward compatible
-

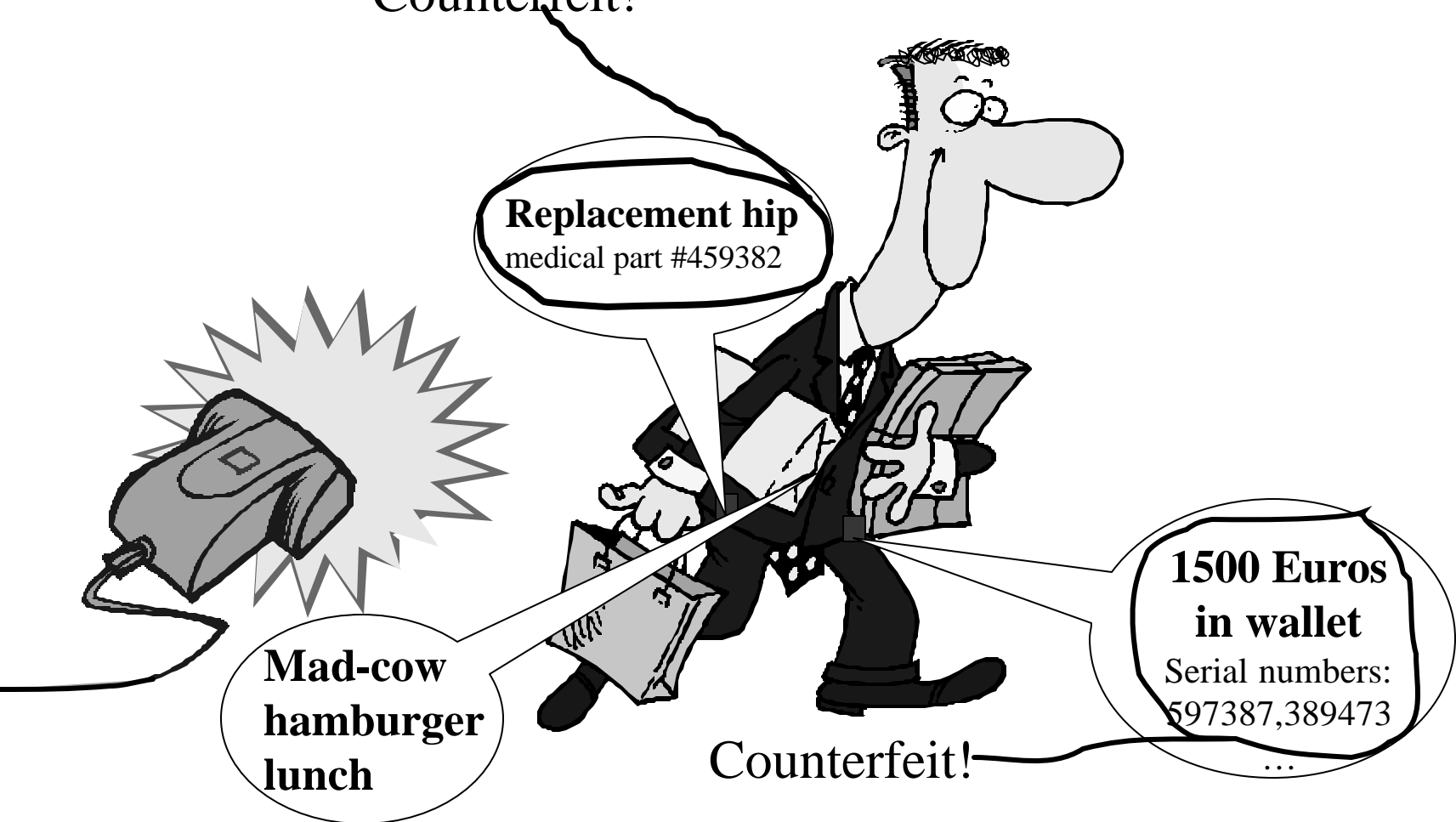
The privacy problem

■ *Malicious readers, good tags*



The authentication problem

- Good readers, *malicious tags*
Counterfeit!



Threats in RFID Systems

- Privacy
 - Spoofing
 - Data Integrity of Tags
 - Denial of Service
 - Corporate Espionage
 - Physical attacks
 - Weak Implementations
-

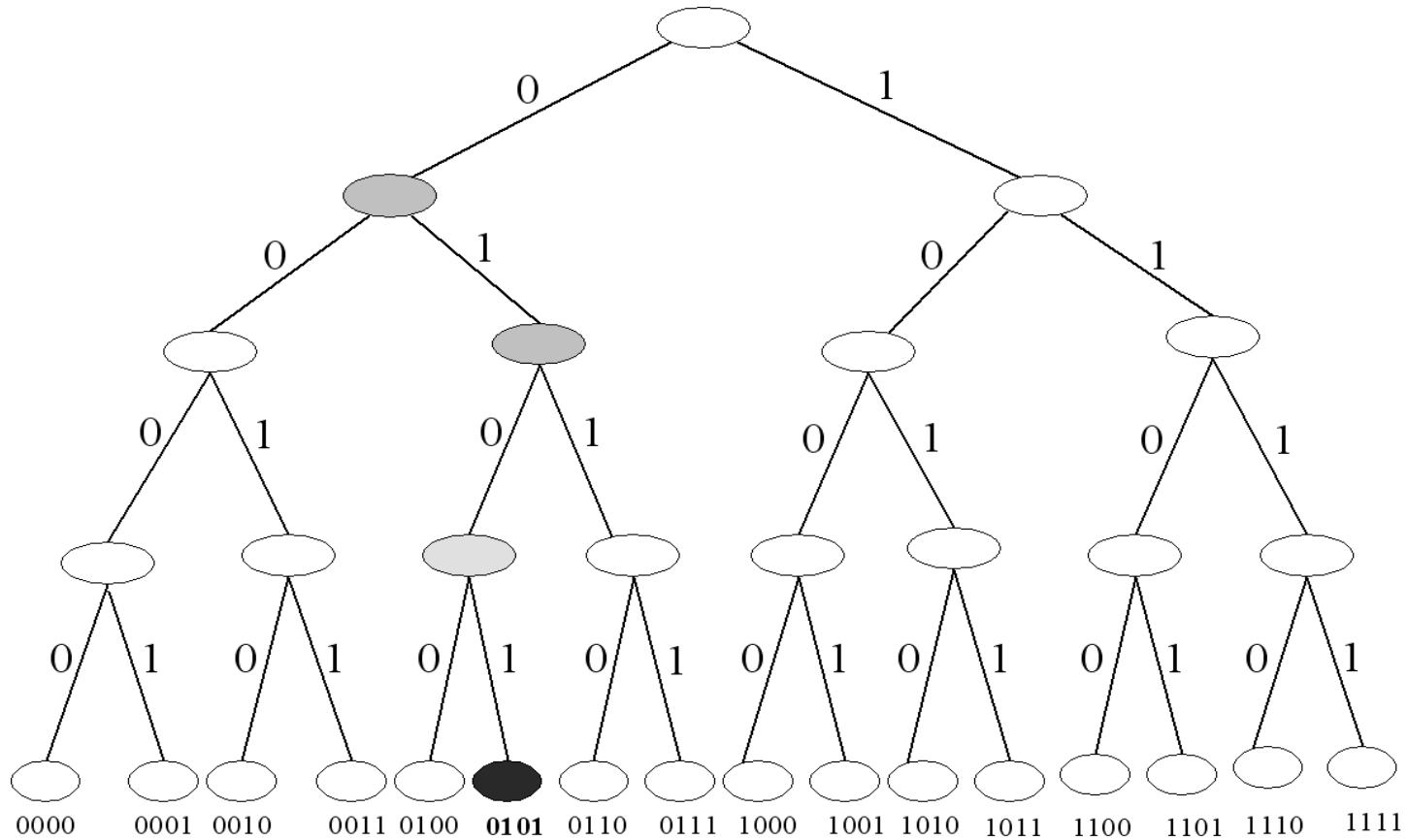
Threats cont. - Examples

- An attacker blackmails an individual for having certain merchandise in their possession
 - A thief could create a duplicate tag with the same EPC number and return a forged item for an unauthorized refund
 - An attacker blackmails an individual for having certain merchandise in their possession
 - A bomb in a restaurant explodes when there are five or more individual of a particular nation with RFID-enabled passports detected
-

Threats cont. - Examples

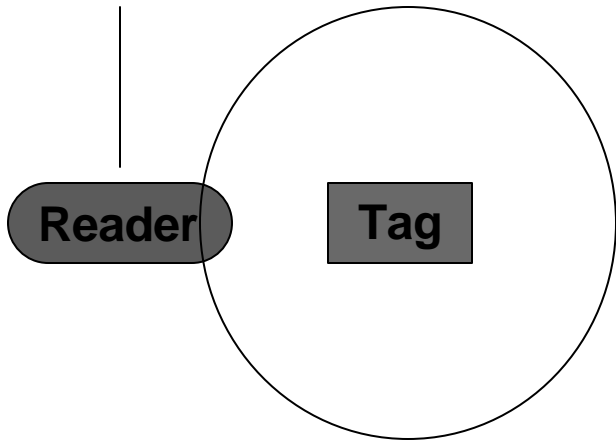
- Falsely implicate someone in a crime by cloning that person's RFiD tags at a reader near to the crime location
 - An attacker modifies a high-priced item's EPC number to be the EPC number of a lower cost item
 - An attacker adds additional tags in a shipment that makes the shipment appear to contain more items than it actually does
 - An attacker exchanges a high-priced item's tag with a lower-priced item's tag
-

Tree-walk protocol for scanning



Ubiquitous scanning

Anti-collision
scheme



Eavesdropper

Backward Channel Range (~5m)

Forward Channel Range (~100m)

Tag privacy protection approaches

- Deactivation
 - Public-key protocol
 - User intervention
 - Blocker tags
 - Metal shielding
 - Silent tree-walking
 - One-time identifiers
-

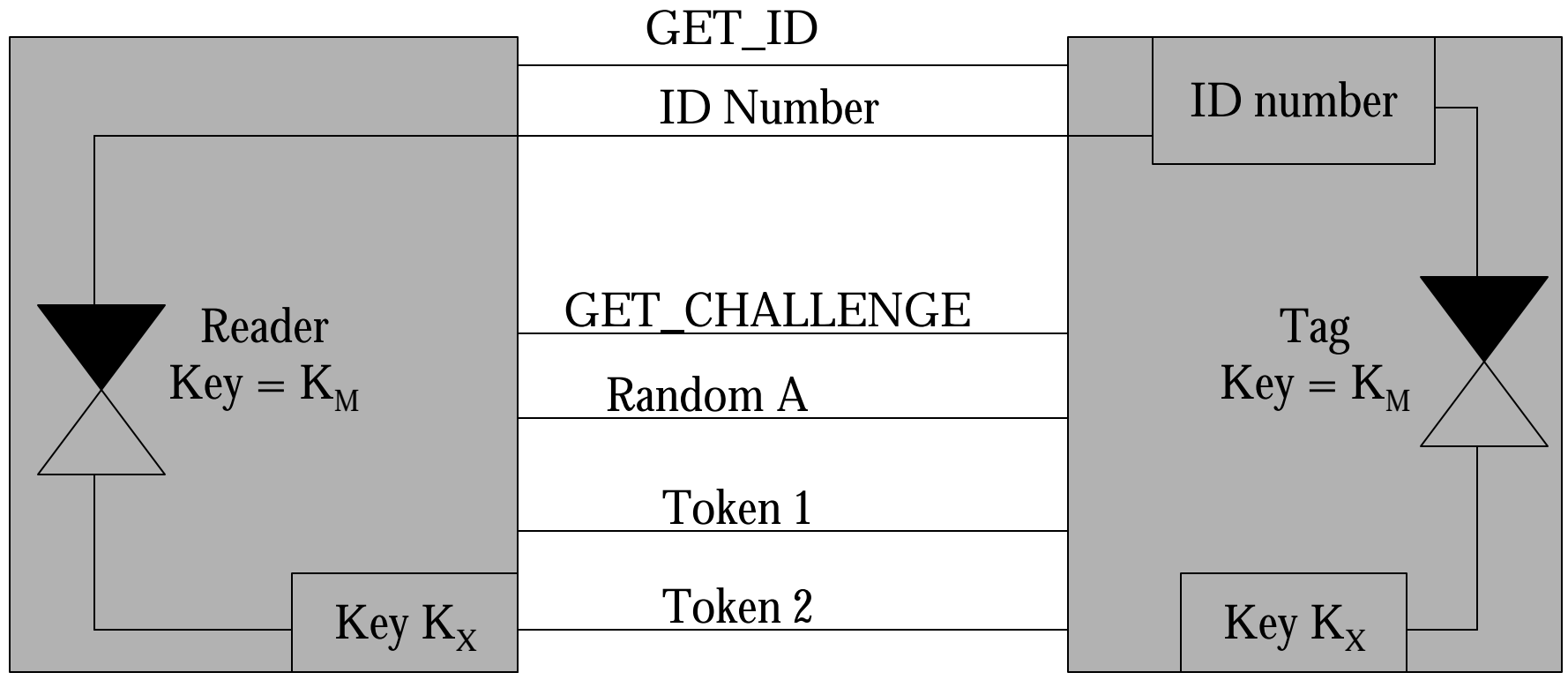
Tag Authenticity - approaches

- Track and trace
 - Challenge-response
 - Static authentication
 - Static authentication with public-key protocol
 - Pseudonym tag with mutual authentication
-

Shared key authentication

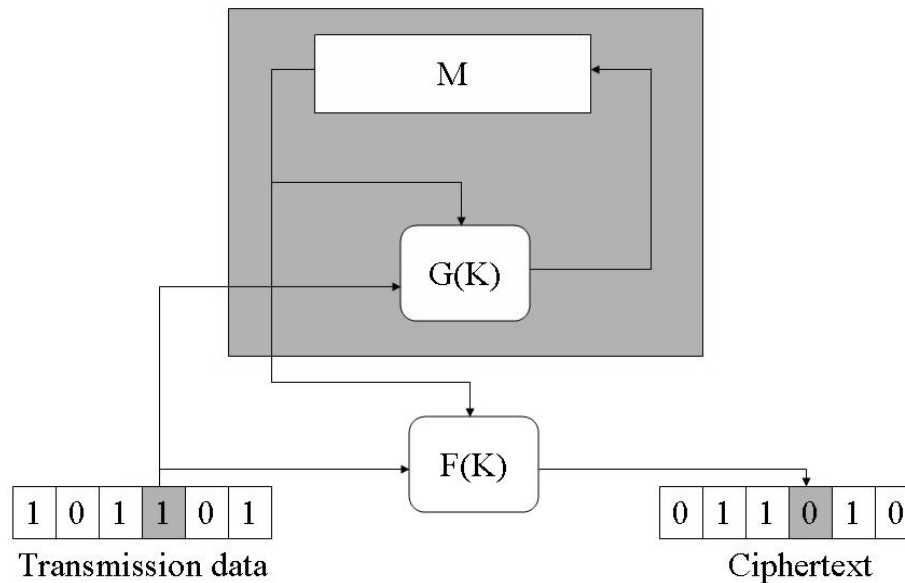


Derived key authentication



Data Encryption in RFiD systems

- Stream ciphers like the one below are used in RFiD



Reader and Database Security

- Standard security protocols
 - Basically, good distributed database / Web services security
-

RFiD based exploits

- Buffer overflows
 - Code Insertion
 - SQL injection

 - Based on the above, RFiD based worms and viruses can be developed by exploiting the middleware in various ways
-

RFiD based exploits cont.

- SQL Injection - if the middleware does not treat the data read from the tag correctly, it may be possible to trick the database into executing SQL code that is stored on the tag.
 - Normally, the tag's data should not be interpreted as code, but programming errors in the middleware may make it possible.
 - Many middleware systems use web-based components, for example to provide a user-interface, or to query databases in different parts of the world. These web-based components may also be vulnerable to attacks. The browser could be redirected to a malicious site.
 - The code that ties the RFID reader interface to the middleware is likely to be written in a low-level language such as C or C++. Any code written in such a language may be vulnerable to buffer overflows
-

RFiD based exploits cont.

- Viruses / worms are written as SQL quines into the tags – this helps replicate the viruses / worms
 - These worms download the actual malicious code from the internet
 - Web-based components may also be susceptible. Server-side includes may allow shell commands to be executed, which can be abused to download and execute the worm in the same way.
-

RFiD based exploits cont.

- Protection against the above outlined attacks is achieved by
 - Client-side scripting can be prevented by properly escaping data inserted into HTML pages
 - If the scripting language is not required, disabling it will avoid any chance of it being abused
 - SSI injection can also be avoided using proper escaping
 - Buffer overflows can be prevented by properly checking buffer bounds
-

References

- Simson Garfinkel, Beth Rosenberg, “RFID Applications, Security and Privacy”, Addison-Wesley
 - Klaus Finkenzeller, “RFID Handbook”, Wiley, Second Edition
 - www.rfidvirus.org
 - www.epcglobal.org
 - www.rsasecurity.com
 - Gopher search
-

Questions?

Thank You!
