CEFRIEL
FORGING INNOVATION
POLITECNICO DI MILANO

RFID: Security Briefings

Angelo P. E. Rosiello
angelo@rosiello.org

CEFRIEL
FORGING INNOVATION
POLITECNICO DI MILANO

Outline

- Introduction
- Auto-ID Leader Technologies
- Auto-ID Technologies: some practical instance
- The Business
- Components of an RFID System
- A First Taxonomy – Passive Tags
- A First Taxonomy – Semi Passive Tags
- A First Taxonomy – Active Tags
- How an RFID System work: an Overview
- Application Contests
- RFID and Security Contests
- Security Requirements
- Mutual Symmetrical Authentication
- Challenge Authentication: Hypothesis
- Challenge Authentication: the Procedure
- Challenge Authentication: Remarks
- Mutual Authentication Protocol: Possible Improvements
- Why Communications should be Encrypted?
- How to encrypt Transmissions
- Symmetric Ciphers: Which one? Why?
- Stream Ciphers: How Do they Work?
- “Modern” RFID Systems: are they safe?
- RFID and Privacy: New Proposals
- Very New Menaces
- RFID Viruses
- RFID Vendors Reaction
- Conclusions
- Bibliography

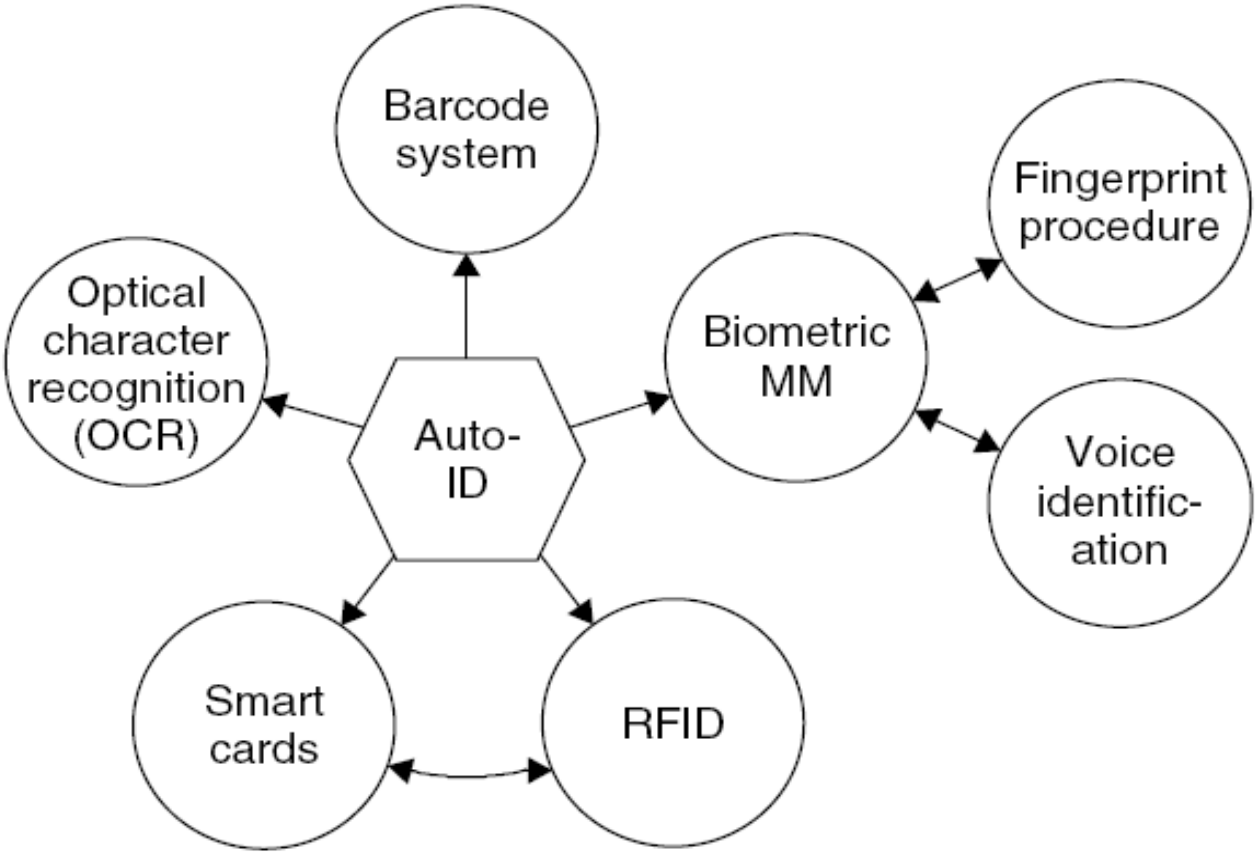
Introduction

- In the last years, the needs of developing new technologies to support automatic identification (Auto-ID) procedures for real world objects, strongly grew up.
- Modern enterprises must have at their disposal efficient and effective means to improve their performances and business. For example, important operations to be supported are:
  - items tracking
  - logistics management
  - Supply chain management
  - Identification of customers' preferences
  - etc.

Introduction

- Military research is really active in this area and the first technologies to support Auto-ID were proposed and used during second World War II.
- British soldiers seeking ways to identify friendly aircraft in World War II were given a newly developed radar transponder system called IFF - Identification Friend or Foe. It was a crude system, but it was a way to tap into technology to identify something at a distance.
- "If you go back and look at the history of patents for RFID — and it is long and storied — the proposals for applications such as baggage tagging, supply-chain management, all of that exists in patents that are 20-plus years old, all for using RFID or its precursor concepts" (Dan Engel)

Auto-ID Leader Technologies



Auto-ID Technologies: some practical instance

- Among the most common and used Auto-ID technologies we can identify *bar codes, which are become almost obsolete.*

Country identifier		Company identifier					Manufacturer's item number					CD
4	0	1	2	3	4	5	0	8	1	5	0	9
FRG		Company Name 1 Road Name 80001 Munich					Chocolate Rabbit 100 g					

Example of a bar code data structure

- Success Factor: costs.
- Major Limitations: they are not reprogrammable and memory capacity is very little.

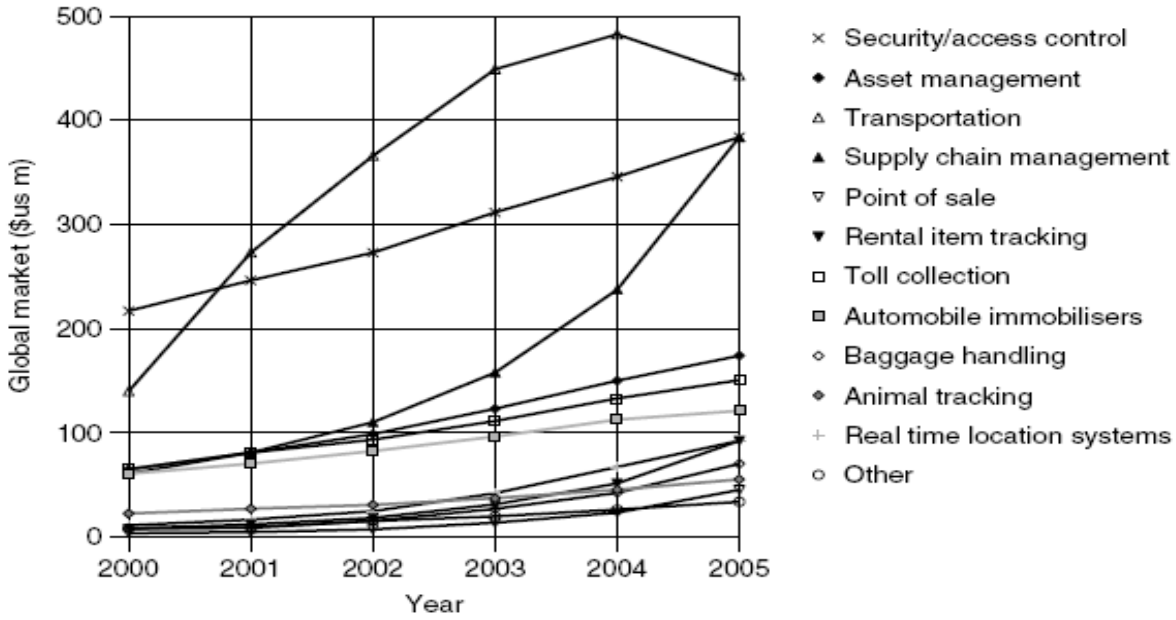
Auto-ID Technologies: some practical instance

- *Smartcards* (introduced in the first 1980 years) avoid many limitations imposed by *bar codes*, but it's still necessary a physical contact with the data reader, in order to extract and/or insert new data.

- RFID (Radio Frequency Identification) systems have a lot in common with smartcards, but not the same limitations!

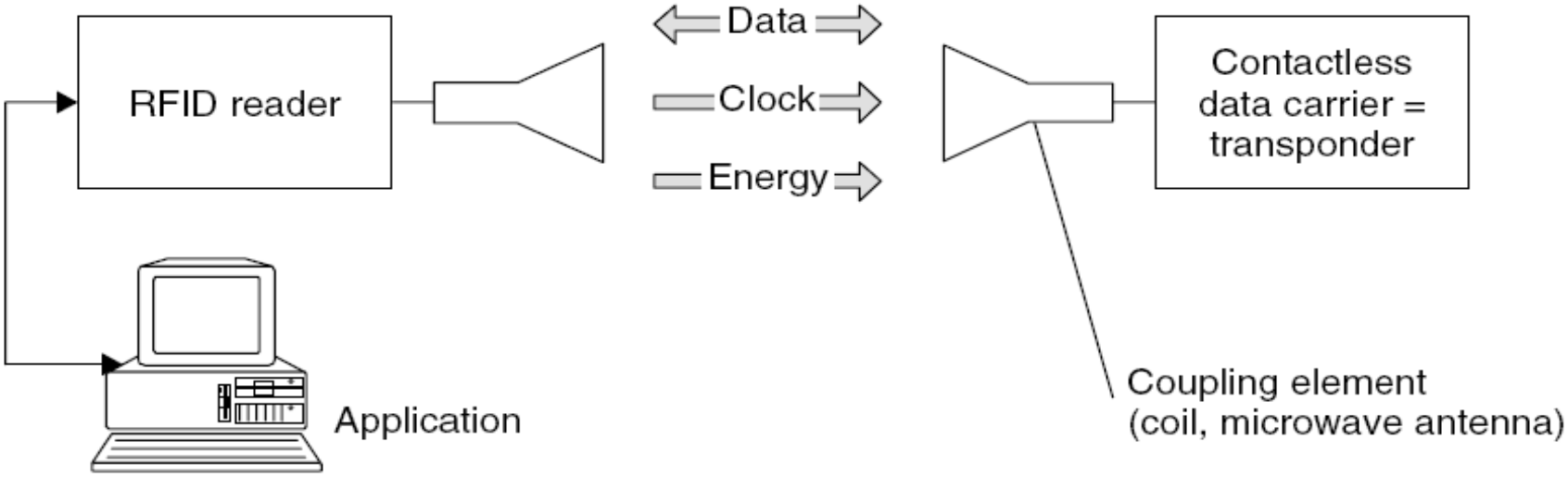
The Business Point of View

- RFID systems production business can't be neglected:
  - 2000 – revenue for RFID systems sold 900 M$
  - 2005 – ~2700 M$



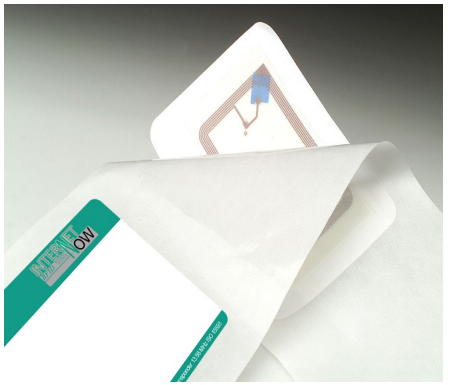
Components of an RFID System

- All RFID systems present two basic components:
  - Transponder: placed on (in) the object to be identified (tags).
  - Reader: strongly dependent on the design and the used implementation technology, its objective is to read and/or write data from/into the transponder.



A First Taxonomy - Passive Tags

- We can distinguish three main types of tags RFID: Passive, Semi Passive, Active.
- Passive RFID tags have no internal power supply. The minute electrical current induced in the antenna by the incoming radio frequency signal provides just enough power for the CMOS integrated circuit (IC) in the tag to power up and transmit a response. The tag chip can contain nonvolatile EEPROM for storing data.



A First Taxonomy - Passive Tags

- Lack of an onboard power supply means that the device can be quite small: commercially available products exist that can be embedded under the skin. As of 2006, the smallest such devices measured 0.15 mm × 0.15 mm, and are thinner than a sheet of paper (7.5 micrometers).
- The addition of the antenna creates a tag that varies from the size of postage stamp to the size of a post card. Passive tags have practical read distances ranging from about 2 mm (ISO 14443) up to a few meters (EPC and ISO 18000-6) depending on the chosen radio frequency and antenna design/size.
- Passive RFID tags do not require batteries, can be much smaller, and have an unlimited life span. Non-silicon tags made from polymer semiconductors are currently being developed by several companies globally, e.g. PolyIC and Philips. Polymer tags can be roll printable, like a magazine, and much less expensive than silicon-based tags.

A First Taxonomy - Semi Passive Tags

- Semi-passive RFID tags are very similar to passive tags except for the addition of a small battery. This battery allows the tag IC to be constantly powered, therefore semi-passive RFID tags are faster in response than passive, though less reliable and powerful than active tags.

A First Taxonomy - Active Tags

- Active RFID tags have their own internal power source which is used to power any ICs that generate the outgoing signal. Active tags are typically much more reliable (e.g. fewer errors) than passive tags due to the ability for active tags to conduct a "session" with a reader. Active tags, due to their onboard power supply, also transmit at higher power levels than passive tags, allowing them to be more effective in "RF challenged" environments like water, heavy metal (shipping containers, vehicles), or at longer distances. Many active tags have practical ranges of hundreds of meters, and a battery life of up to 10 years.
- Defense has successfully used active tags to reduce logistics costs and improve supply chain visibility for more than 15 years. As speaking, the smallest active tags are about the size of a coin and sell for a few dollars.

How an RFID System works: an Overview (1/2)

- The objective of an RFID system is to enable the exchange of information among mobile devices (tags) and one or more readers (tags reader) that will process them according to the needs of a particular application.
- As previously introduced, the use of RFID in tracking and access applications first appeared during 1932, to identify friendly and un-friendly planes.

How an RFID System works: an Overview (2/2)

- Usually, in a RFID system, objects to be identified are equipped with a tag. The tag contains a transponder with a digital memory chip. The interrogator, an antenna packaged with a transceiver and decoder, emits a signal activating the RFID tag so it can read and write data to it. When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's integrated circuit and the data is passed to the host computer.

Application Contests

- The Canadian Cattle Identification Agency uses RFIDs, as a replacement for bar-code tags, to track bovine's herd.
- High-frequency RFID tags are used in the libraries to track books.
- American Express Blue credit card includes an RFID tag.
- Sensor Networks.
- Toyota embeds RFIDs in its new vehicle models to substitute “old” keys (Lexus GS, 2006 - Toyota Camry, 2007).
- Passports.
- Human Implants (Kevin Warwick, 1998).
- etc...

CEFRIEL
FORGING INNOVATION
POLITECNICO DI MILANO

RFID and Security

RFID and Security Contests

- In the last months, the number of RFID systems used in security application contests, such as authentication systems, payment systems, etc., is fastly growing up.
- RFID systems in these delicate application contests require the existence of strong protection mechanisms, to defend devices from malevolent attacks.

Security Requirements (1/2)

- RFID systems must be immune or resistant to the following kind of attacks:
  - Unauthorized data read or manipulation.
  - Placement of a foreign device into the system's interrogation zone, in order to obtain unauthorized access or to exploit services.
  - Sniffing of the radio signal in order to replicate and/or modify the signal and transmitted data.

  "In a naive, RFID-enabled world, there's a risk that sensitive information will be secretly visible to anyone with a suitable scanner" (Burt Kaliski, RSA Laboratories).
- The choice of an RFID system must consider if security functions to protect the whole system have to be present or not, according to security needs.

Security Requirements (2/2)

- It seems quite evident that the adoption of security functions is not always a must but strongly depends on the application domain. For example, in fields such as industry automation, goods tracking, etc, the choice of including security mechanisms (e.g. cryptographic protocols) to stay safe from malevolent attacks may is an unjustified expense.
- Where specified security levels must be present by definition, e.g. passports, authentication procedures, etc..., if we don't invest in good security mechanisms, effects could be disastrous.

Mutual Symmetrical Authentication

- Key security aspect of RFID systems is the identification of legitimate entities.
- Before beginning any communication, both the reader and the transponder must verify their counterpart's identity, that is the reader must be sure to contact the wished transponder and vice-versa.
- Typically the protocol used to achieve mutual symmetrical authentication is the ISO-9798 2, based on the principle of “challenge-response”.

Challenge Authentication: Hypothesis

- When a transponder passes through the electromagnetic zone, it detects the reader's activation signal but there's no ex-ante method to know if the reader is the legitimate one or not, and also the reader can't know if the transponder is reliable, too. This is the very reason because a mechanism of mutual authentication is required.
- Actors of an RFID system must share a common but secret layer of knowledge. The common knowledge is a key K and a symmetrical cryptographic algorithm *ek.*
- *Let's make a thorough study of the problem...*

Challenge Authentication: the Procedure (1/2)

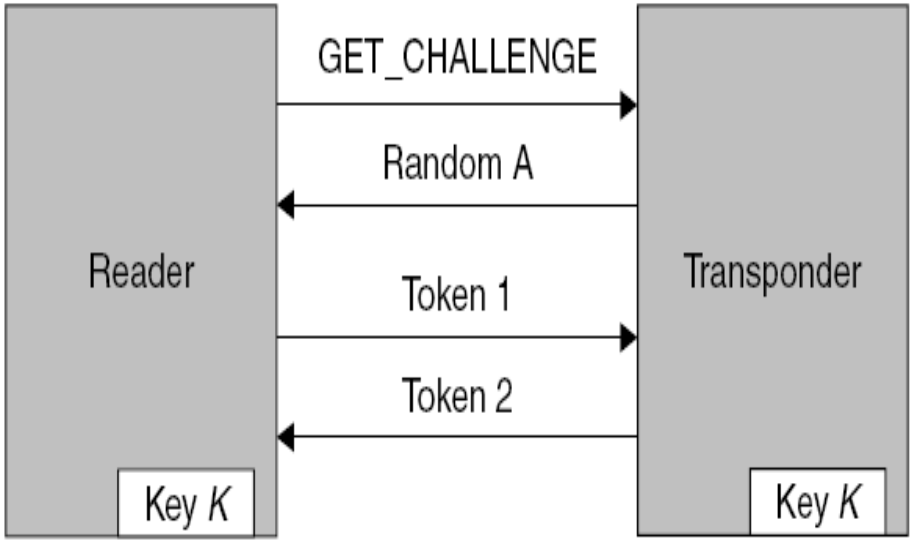
- The procedure starts after a "*GET_CHALLENGE*" command is sent by the reader to the transponder.
- The transponder receives the "*GET_CHALLENGE*" command, generates and sends a random number "*Ra*" *to the reader. The random number just sent represents the challenge for the reader.*
- Now, the reader has to do two actions:
  - *A random number "Rb" is generated and sent to the transponder.*
  - *The received number "Ra" and the generated one "Rb" are both encrypted using the shared key K and the algorithm ek, producing the data block "Token 1".*
- The transponder receives "Token 1" and decrypts it...

Challenge Authentication: the Procedure (2/2)

- After that “Token 1” gets decrypted, the transponder can verify the authenticity of “Ra”. The procedure returns two possible results:
  - *“Ra” doesn't correspond to the transponder computed number: the reader may is a fake and the procedure terminates.*
  - *“Ra” is correct, the procedure proceeds.*
- If the verification step was successful, the transponder generates another random number, i.e. Ra', which is concatenated with all the previous numbers (i.e. Ra and Rb) and encrypted.
- When the reader receives the encrypted message from the transponder, for first decrypts it and then check if “Rb” is correct.
- If all steps were successful the mutual authentication is complete and data can be exchanged, else anything is terminated.

Challenge Authentication: Remarks

- The strength of this authentication method is that the secret key K is never exchanged, but its implicit knowledge is proved.
- Random generated numbers may be a weakness point of the protocol because if predicted, replication attacks are feasible.
- There is no limitation about cryptographic algorithm to use. Obviously public and standardized algorithms are suggested.



Mutual Authentication Protocol: Possible Improvements

- During the description of the mutual authentication procedure, we supposed that all entities of the system had the same cryptographic key K, in order to encrypt messages. This can be a weakness point for the protocol, because if the key of a transponder is recovered, the whole system gets broken.
- To improve the security level of the system, it is possible to bind each transponder (x) with a private key Kx which depends on the master key of the reader and on the serial number of the device.
- During the authentication phase, the reader can compute the key Kx after receiving the serial number from the transponder. The other steps of the protocol are the same of the basic version.
- ***In this case, even if an attacker obtains the key Kx of the transponder x, he can't still decrypt data sent from the other transponders.***

Why Communications should be Encrypted?

- Feasible attacks that can be realized again a RFID system are mainly two:
  - Data Sniffing (passive).
  - Hijacking (active).
- To avoid these kind of attacks there's a large number of solution proposals in the literature. Cryptography is the core of these defensive techniques, some practical and very popular examples are:
  - SSL.
  - SSH.
  - WEP.
- Since RFID systems are vulnerable to the cited kind of attacks, the choice of cryptographic solutions to encrypt communications are a must.

How to encrypt Transmissions

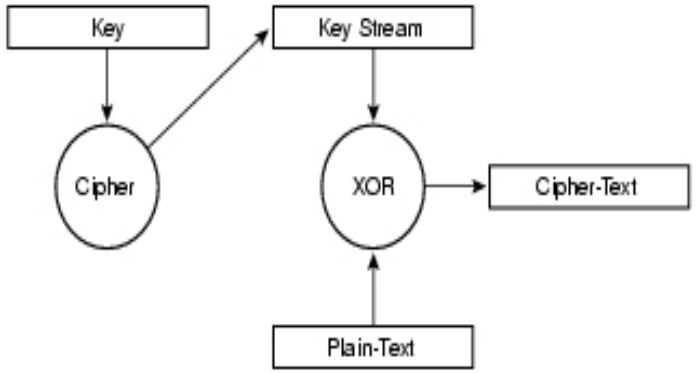
- Cryptography is the art of encrypting secret messages.
- If the messages exchanged in a RFID system are encrypted, there's no way for the attacker to extrapolate useful information, but:
  - The cryptosystem is not secure itself!
- There are two main classes of cryptographic methods:
  - Symmetric: the key K to encrypt and decrypt messages is the same (e.g. AES, DES, RC5, RC4, etc.).
  - Asymmetric: two different keys Kpub and Kpri exist, that execute one the inverse function of the other (e.g. RSA).
- Nowadays, RFID systems adopt almost exclusively symmetric algorithms, also because asymmetric solutions require much more computational and supply power.

Symmetric Ciphers: Which one? Why?

- Symmetric ciphers can be divided into two ulterior categories:
  - Block Ciphers.
  - Stream Ciphers.
- Block Ciphers (e.g. AES, DES) elaborate blocks of data (e.g. 512-bits) and for the numerous operations of transposition and permutation, they dissipate a lot of power.
- Stream Ciphers (e.g. RC4, A5/1, FISH, PANAMA, Helix, etc) process data bit-to-bit (at most byte-to-byte), and actually require less power for the computations. This is the very reason because RFID systems designers prefer stream ciphers (moreover they are also faster than block ciphers).

Stream Ciphers: How Do they Work?

- The core function of a stream cipher produces a sequence of random bits, said *keystream*, constantly depending on the secret key. Encryption is accomplished combining the keystream with the plain-text, usually with the bitwise XOR operation.
- The generation of the keystream can be independent of the plain-text and cipher-text, yielding what is termed a synchronous stream cipher, or it can depend on the data and its encryption, in which case the stream cipher is said to be self-synchronizing. Most stream cipher designs are for synchronous stream ciphers.



"Modern" RFID Systems: are they safe?

- A group of researchers from RSA Security and Johns Hopkins University (February 2005) broke one of the most common RFID systems in less than 15 minutes. The object of the attack was the *Registration and Identification System* from Texas Instruments, one of the major producers of RFID systems. Researchers assert that, via wireless, it was easy to "steal", from the tag present in the payment card, information of its owner. In this way it was possible to realize a clone of the victim's card, to fraud the system.
- **During the last months, many researches improved the security quality of RFID systems and also proposed new systems to guarantee a major level of privacy for consumers.**

RFID and Privacy: New Proposals

- Consumers will almost certainly wish to possess live RFID tags in many of their belongings for "smart" appliances, prescription refills, automated payment, store returns, and so forth. At the same time, they do not want their RFID tags to be scanned indiscriminately.
- During the last RSA Conference (February, 2006) about ICT security in San Francisco, RSA Security Inc. presented a prototype of the new RFID technology named “RSA Blocker Tag”, designed to protect users' privacy.
- One may think of a the RSA Blocker Tag as "spamming" any reader that attempts to scan tags without the right authorization. The RSA Blocker Tag manipulates the reading protocol with the aim of making the reader think that RFID tags representing all possible serial numbers are present. When a Blocker is in proximity to ordinary RFID tags, they benefit from its shielding behaviour.

Very New Menaces

- Some researchers from Vrije Universiteit of Amsterdam (Rieback, Crispo, Tanenbaum) are advising the community about viruses integrated into RFID tags, designed to identify and track objects.
- No RFID virus was still released but tags have suitable characteristics that could be used to exploit security vulnerabilities of back-end software systems (e.g. TinyDB).

The first RFID chip infected with a virus.

RFID Viruses

- SQL injection attacks or buffer overflows can be exploited to compromise RFID systems.
- Possible Scenario: some airports are planning to expedite baggage handling by attaching RFID-augmented labels to the suitcases as they are checked in. This makes the labels easier to read at greater distances than the current bar-coded baggage labels. Now consider a malicious traveler who attaches a tiny RFID tag, pre-initialized with a virus, to a random person's suitcase before he checks it in. When the baggage-handling system's RFID reader scans the suitcase to determine where to route it, the tag responds with the RFID virus, which could infect the airport's baggage database. Then, all RFID tags produced as new passengers check in later in the day may also be infected. If any of these infected bags transit a hub, they will be rescanned there, thus infecting a different airport. Within a day, hundreds of airport databases all over the world could be infected. An RFID virus could also carry a payload that did other damage to the database, for example, helping drug smugglers or terrorists hide their baggage from airline!

RFID Vendors Reaction

- Ninety-nine percent of security concerns around RFID technology are "solved problems," says Kevin Ashton, vice president of marketing at RFID vendor ThingMagic.
- Moreover Ashton asserts that RFID chips infected with viruses is not relevant phenomenon, because researchers assumed data could be treated as if it were code. As far as the answer to the question of RFID signals being intercepted by unauthorized readers, is to simply keep the RFID tagged data to a minimum and carefully defined by parameters. The "interesting and secret stuff" stays on the network. What should get more attention but doesn't, Ashton says, is the fact that RFID systems are being deployed in locations, such as warehouses, that to date have not had IT infrastructure in place, and determining who will control the RFID deployment and budget.

Conclusions

- RFID is an emerging (but not new) technology which will replace lots of the existing Auto-ID technologies.
- Security is a very important issue of RFID Systems and it must be kept in high consideration during the design phase of the whole system.
- In this presentation we could observe that security functions to be adopted in a system, strongly depend on the application contest. It means that the optimal solution doesn't exist, instead it consists in the right trade-off among costs and claimed security levels.
- Cryptography is widely used to achieve authentication of the system's entities and to satisfy confidentiality needs. Stream ciphers are prefered to block ciphers mainly for power reasons.
- New menaces came out during the last months, such as viruses or worms, but they still can't be considered as a serious present menace and new defense techniques may avoid them before their real spread.

Bibliography

- RFID HandBook 2nd edition, John Wiley & Sons.
- http://www.rfidvirus.org/index.html
- Applied Cryptography, 2nd edition – Bruce Schneier, John Wiley & Sons.
- Is Your Cat Infected with a Computer Virus? - Melanie R. Rieback Bruno Crispo Andrew S. Tanenbaum, Vrije Universiteit Amsterdam Computer Systems Group.
- http://www.nfc-forum.org/
- http://www.aimglobal.org/technologies/rfid/
- http://www.epcglobalinc.com/
- http://portal.etsi.org/radio/RadioFrequencyID/RFID.asp
- http://www.rfidgazette.org/