Radio-Frequency Identification - Overview

Lukas Grillmayer
Supervisor: Dipl.-Inf. Matthias Wachs
Seminar Future Internet, WS 2012/13
Chair for Network Architectures and Services
Department of Informatics, Technical University of Munich
Email: grillmay@in.tum.de

ABSTRACT
Radio-frequency identification (RFID) is a wireless technology for automatic identification using electromagnetic fields in the radio frequency spectrum. In addition to the easy deployment and decreasing prices for tags, this technology has many advantages to bar codes and other common identification methods, such as no required line of sight and the ability to read several tags simultaneously. Therefore it enjoys large popularity among large businesses and continues to spread in the consumer market. Common applications include the fields of electronic article surveillance, access control, tracking, and identification of objects and animals. This paper introduces RFID technology, analyzes modern applications, and tries to point out strengths and weaknesses of RFID systems.

Keywords
RFID, transponder, active / passive tag, Auto-ID, Smart Card, EPC, NFC

1. INTRODUCTION
During the last decades bar codes have probably been the most successful identification technology, as other procedures didn't yet exist or were too expensive to be deployed efficiently, although technologies like RFID have many advantages. RFID technology is cheap, fast, does not require a line of sight and supports simultaneous reading of several tags at once over distances ranging from few centimeters to hundreds of meters. Due to technological progress the technology behind RFID has improved, lowering the costs to reasonable levels allowing it to enter the mass market. Every RFID system consists of a reader, a transponder, and an application software. The transponder is a data-carrier which is commonly called tag. They come in various shapes and sizes, mostly in form of a so called smart cards or smart labels, which are sticky and can easily be attached to objects. Widespread applications can be found in the fields of anti-theft, access control, logistics, supply chain management, animal identification and tracking, and electronic payment systems, to name few examples for the countless uses of RFID.
In the next section the history of RFID technology is presented, followed by an introduction to the principles and components of RFID systems along with important standards, which specify the basics of RFID. Afterwards modern applications are analyzed before introducing possible risks and attack vectors which can result out of the use of RFID technology.

2. HISTORY
The invention of radar in the mid 1930s made it possible to detect aircraft from vast distances, but during World War II the issue of distinguishing friendly from enemy planes became a problem. For this purpose the Germans would fly upside-down on command before entering friendly airspace, altering the reflected radio signal to identify the aircraft as friendly [1]. One can call this the first passive RFID system, which was simplistic to spoof by Allied forces. This called for a more sophisticated methods of identification and as a result IFF (Identify Friend or Foe) systems were developed, for example the German FuG 25a "Erstling" manufactured by GEMA in 1941 which sent back a pre-defined signal to ground radar stations when asked for identification [2, 3]. This method of automatic identification via radio-frequency signals is one of the first active RFID systems. In 1948 Harry Stockman described in his publication "Communication by Means of Reflected Power" basic theoretical principles for passive RFID systems and suggested more active foundational research in this area [4]. Radio-frequency identification was invented [5].

More experimental work followed in the upcoming decades, such as Donald B. Harris' "Radio Transmission Systems with Modulatable Passive Responder" in 1960. Harris patented a wireless communication system similar to the military's "Walkie Talkie" systems with the main difference that only one station needs an external power source whereas the portable station draws the required energy to reply out of the received radio signals [6]. Another RFID-related development was Robert M. Richardson's invention "Remotely Actuated Radio Frequency Powered Devices" primarily focusing on efficient usage of radio frequency energy "approaching the theoretical maximum" [7].

As RFID technology was mostly used by the military, in the 1960s first companies recognized the advantages it brings for civilian commercial usage. One of the most widespread and well known inventions of this time were RFID based electronic article surveillance (EAS), to prevent theft and loss of merchandise, which was developed by Arthur Minasy later the founder of the company "Knogo" (1966). Also "Sensormatic Electronics Corporation" (1960) and "Checkpoint Systems, Inc." (1969) competed in this area of EAS systems, which mostly uses 1-bit passive tags and several readers called gates which form a detection zone. If a functional tag is detected in this area an alarm is triggered to signalize an unauthorized passing, whereas no radio signal

doi: 10.2312/NET-2013-02-1_04

can be received when the tag is either destroyed, deactivated or removed [8, 9, 10, 11].

In 1975 three scientists from the Los Alamos Scientific Laboratory published their work on "Short-Range Radio-Telemetry for Electronic Identification, Using Modulated RF Backscatter" and presented an innovative method of communication for passive RFID tags. They were developing a passive "electronic identification system for livestock", which reported the animals identification number as well as its body temperature over a distance of several meters between tag and reader [12]. During the 1970s further novel developments of RFID systems included also the fields of vehicle identification and access control systems [13, 14].

So far RFID technology was mostly a subject of research and development, whereas widespread commercial applications were yet to come in the following decades. Since the late 1980s several countries began to deploy electronic toll collection systems, first of all Norway in October 1987, soon followed by the United States, Italy, and France [15]. As there was only little competition in this market section prices for RFID systems were very high, hindering it from becoming a mainstream technology, although improvements were made considering the size, weight and range of tags. This enabled applications such as animal tracking with implanted tags under the skin, and container tracking which was a development of the Association of American Railroads and the Container Handling Cooperative Program [16].

The 1990s and 2000s are characterized by RFID technology becoming part of everyday life of consumers and the first establishment of industrial standards along with governmental regulations concerning the power and used frequencies of RFID systems. New applications developed in the 1990s included systems for electronic toll payment, ski passes, vehicle access and article tracking. The Auto-ID Center at the Massachusetts Institute of Technology was founded in 1999 supported by the EAN International (today known as GS1) and Uniform Code Council Inc. (UCC, today known as GS1 US) along with Procter & Gamble and Gillette in order to develop the Electronic Product Code (EPC) and standards for low-cost UHF RFID tags used in supply chain applications [17]. As the Auto-ID Center gained supporters and became a worldwide operating research facility, the need for global RFID standards was recognized and resulted among other developments in two air interface protocols (Class 0, Class 1) and the EPCglobal Network, a multicorporate network for real-time tag tracking via the Internet. Until the late 1990s most aspects of modern RFID technology were standardized. These standards applied to animal identification (ISO/IEC 11784, 11785 and 14223), contactless smart cards (based on ISO/IEC 7810: ISO/IEC 10536, 14443 and 156693), container identification (ISO 10374), anti-theft systems for goods (VDI 4470) and item management (ISO/IEC 18000, EPCglobal Network) [18]. All standards are subject to continuous revisions as technology progresses.

In 2003 the UCC and EAN International formed the nonprofit organization EPCglobal Inc. to commercialize the EPCglobal Network internationally. It kept developing new protocols parallel to the combined efforts of the International Standards Organization (ISO) and International Electrotechnical Commission (IEC). Although EPCglobal tried to create the ISO compatible Gen2 standard it took until 2006 before it was merged wth the ISO/IEC 18000 standards [19, 20]. In the meantime large organizations like Wal-Mart and the US Department of Defense set up mandates, which required many of their suppliers to apply RFID tags on their shipments. [16] In 2004 the US Food and Drug Administration (FDA) eased the way for human RFID implants containing a unique ID number, which lead to ethical discussions lasting to this present day [21]. Further current RFID applications will be discussed in the following section.

3. TECHNOLOGY AND STANDARDS

Every RFID System is formed out of a reader/writer, transponders, which are commonly called tags, and an application for further processing of the read data. For instance the application can be an access control system or a supply chain management system. In the following various classes and aspects of RFID systems are described, in order to develop a basic understanding of this technology.

3.1 Transponder / Tag

A tag or transponder contains always an antenna for receiving and sending signals and a silicon chip which holds (and processes) the data to be transmitted to the reader. Tags are usually of a flat appearance, often deployed on plastic foils or paper for smart labels, in plastic casings for access cards and car keys, or in a glass housing for the use as implant [18].

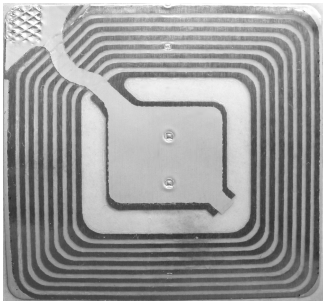

Figure 1: RFID sticker on a DVD for EAS [22]

As described earlier EPCglobal Network introduced classes to characterize the functionality of RFID tags. With the introduction of new classes more features were added to the previous classes.

Table 1: RFID transponder classes[23]

#	Layer Name	Added Functionality
1	Identity	passive identification tags
2	Higher Functionality	read/write memory
3	Semi-Passive	battery power for chip
4	Active AdHoc	communication with tags
5	Reader	can act as reader

Another class of transponders implentents the "Generation 2" (Gen2) standard which was introduced in 2004 and can be described as an improved class 1 tag with additional features as described below [18, 24].

doi: 10.2312/NET-2013-02-1_04

3.1.1 Class 1: Identity Tags

Class 1 tags are passive-backscatter tags, which have no power source, so they draw power from the reader's emitted radio signal in order to reply. Because only a fraction of the emitted power can be used, the reflected energy is very weak, which limits the maximum distance between a passive tag and reader to a few meters. Advantages are low production costs, their small size and very high durability, which allows commercial mainstream mass market deployment for example for electronic article surveillance [25].
Identity Tags are writable once and carry one 64-bit or 96-bit EPC identifier, one tag identifier for manufacturer identification and an implementation of a kill-command, which disables the tag permanently. Optional features include password protected access-control, user memory and the functionality of turning the tag temporarily on and off. This class of transponders operates at 860-930 MHz and 13.56 MHz [18, 26].
Please note that former class 0 and class 1 were merged to class 1 since both had the same functionality of being passive and writable only once [25].

3.1.2 Gen2 Tags

Gen2 tags have a dense reader mode to prevent multiple readers from interfering with each other, improved memory segmentation, barcode applications allowing identical electronic product codes (EPC) on several tags, and changed bit coding to improve detection rates. Another feature of Gen2-tags allows global usage as it meets European (860 MHz - 868 MHz) and North American (902 MHz - 928 MHz) radio frequency regulations and operates at any frequency between 860 MHz and 960 MHz. According to an RFID hardware manufacturer [27] ICs on Gen2 tags have 40-50 year data retention and support up to 100,000 write cycles. The tag's memory is segmented in reserved memory, for 96 bit EPC, 32-64 bit tag identifier, 32 bit kill password and 32 bit access password, and optional user memory ranging up to several kilo bit.

3.1.3 Class 2: Higher Functionality Tags

In addition to class 1, Higher Functionality Tags have an extended tag identifier, extended rewritable user memory up to 65kbit and authenticated access control. Further features of class 2 transponders are not yet specified in this standard [27].

3.1.4 Class 3: Semi-Passive Tags

These tags have a power source, usually in form of a battery, for supplying energy to the circuitry of the tag. It has to draw energy from the reader only for communication purposes, allowing longer ranges and more reliability concerning the successful transmission of data. The life time of class 3 tags is generally shorter than for entirely passive tags [25].

3.1.5 Class 4: Active AdHoc Tags

Active RFID tags are equipped with an autonomous transmitter so they need their power source for communication purposes as well. This enables long reading ranges up to several kilometers using the microwave band. The simultaneous reading of several hundred tags at once, high data transfer rates and the possibility to build complex systems by adding sensors made this technology especially attractive for container tracking, refrigerated transport and other fields of logistics [25]. Drawbacks are lifetime cycles of 5 - 10 years, mostly limited by the battery life, and high costs of about $10-$50 for one active RFID tag [28, 29, 30].
In addition to class 3, Active AdHoc Tags can communicate with other class 4 tags through the on-board transmitter. Therefore class 4 tags are able to initiate communication, whereas tags of class 3 and below can only answer to the reader which provides the power for communication [18, 27].

3.1.6 Class 5: Reader Tags

Class 5 supports all features of class 4 tags and has the ability to act as reader for passive and active tags of classes 1, 2, 3, and 5 [18].

3.1.7 Power Supply and Antenna Design

As mentioned before passive tags have no battery to power communication functionalities whereas active tags have an on-board power source. In the following, various methods to supply power to passive transponders and the resulting antenna design are described. Antennas of active tags may differ in size and shape, but the presented principles apply to active tags as well as to passive tags.

1-bit tags, which are mostly used in EAS, use fairly simple physical exploits as they only have to communicate their presence and no further information. In systems using radio frequency for tag detection the transponder has coils, which generate a current on the tag when it is located in the magnetic alternating field emitted by the reader (see Figure 1). This current causes a weakening of the magnetic field which can be meassured.
Tags in EAS systems operating at microwave range use a dipole antenna connected to a diode. When the tag is in the range of the reader, the emitted carrier frequency causes a flow of current in the diode which re-emits harmonics of the carrier wave, which can be measured. Similar systems work with subharmonics or even inharmonics of the carrier frequency.
A different approach is the use of acoustomagnetic systems, where tags are made of two special metal strips contained in a plastic housing. When placed in a magnetic alternating field one metal strip starts to vibrate and it keeps oscillating for a while when the magnetic field is turned off. This causes the tag to emit a weak, but measurable magnetic field for a short period of time.

Transponders supporting full- or half-duplex comunication use different principles than 1-bit tags since they need more energy to power their chip. Tags using inductive coupling draw power of the reader's emitted magnetic alternating field through the use of coils. The resulting current powers the chip and two parallel capacitors, which form the resonant frequency of the tag.
Electromagnetic backscatter coupling is used for long-range systems (> 1 m) operating at UHF frequencies. Long distances between reader and tag result in a high loss of energy of the emitted electromagnetic field, which has to be considered for the design of the tags dipole antenna.
Close coupling is used for ranges between 1mm and 1 cm, therefore the energy loss over distance is minimal. These tags are usually inserted in or placed onto the reader. The

doi: 10.2312/NET-2013-02-1_04

reader has coils on a ring-shaped or U-shaped core, whereas the transponder's coils can be placed coplanar. The energy transfer is similar to the principle of transformers.
At last tags for systems using electrical coupling have an antenna, which is made of two large conductive surfaces, each acting as an electrode. When the tag is placed in the electric field of the reader, there is a voltage between the electrodes, which can be transformed to a lower voltage to power the transponder's chip [18].

3.2 Reader

A Reader is responsible for the communication with tags and the RFID system's application software. It provides an electromagnetic field to activate the tag and initiates the communication process with one or more tags in range. This field is used by passive and semi-passive tags to power their communication ability as they do not have an onboard power source for this purpose. Readers handle the connection establishment, and anticollision and authentication procedures exclusively. In order to write data to a tag's read/write memory, special readers can also act as writers. Modern readers are able to connect directly to a network or the internet to communicate with the application software using IP, TCP, and UDP, or they are connected to a computer, which redirects or processes the gathered data via an USB or RS232 connection. There are handheld models and stationary readers of which latter ones might support multiple antennas or can be deployed in an array of readers forming a larger detection zone.
A current development is the integration of RFID technology in cell phones and tablets, enabling mobile devices to operate as reader and tag. These applications use the Near Field Communication (NFC) standard which relies on RFID technology [18].

3.3 Frequency

The name "radio-frequency identification" already indicates that RFID operates in parts of the radio frequency spectrum which ranges from about 3 kHz to 300 GHz, although mostly frequencies between 30 kHz and 6GHz are used in today's RFID applications. In the following, four frequency bands will be discussed as can be seen in table 2 in respect to ISO/IEC Standards, which will be presented later in this paper. Please note that the use of various frequencies and maximum signal strengths are heavily regulated by governments all over the world. Details to read ranges are exemplary as read ranges improve with technological progress and can be extended using more sophisticated technologies.

Table 2: Frequency Ranges used for RFID

Frequency	Abbr.	Designation
30 kHz - 300 kHz	LF	Low Frequency
3 MHz - 30 MHz	HF	High Frequency
300 MHz - 3 GHz	UHF	Ultra High Frequency
2 GHz - 30 GHz	-	Microwave

3.3.1 Low Frequency

Applications using LF operate usually below 135 kHz and are characterized by short reading ranges of < 0.5m and a low data transfer rate of <1 kbit/s. Performance issues arise when metal objects are disturbing the transmission. Typical applications of LF RFID systems are animal tracking and access control [25].

3.3.2 High Frequency

The very common RFID frequency of 13.56 MHz can be found in the HF band. With a read range of < 1.5m and decent data transfer rates of about 25 kbit/s it very suitable for the deployment of smart labels and product authentication. Once again it cannot penetrate metal [25].

3.3.3 Ultra High Frequency

UHF RFID systems use the following frequencies: 433.92 MHz and 860 MHz to 930 MHz. Data transfer rates are about 30 kbit/s. This band is supported by the Electronic Product Code which is currently used by Wal-Mart and the US Department of Defense in their supply chains. Read range is up to 100m for 433.92 MHz and between 0.5-5 m for 860-930MHz.Water and metal cannot be penetrated [25].

3.3.4 Microwave

Microwave systems operating with frequencies of 2.45 GHz or 5.8 GHz have a long read range of 10m and above, and a high data transfer rate of about 100 kbit/s. This technology is used in toll collection systems all over the world with the drawbacks of being more expensive than other systems and the lack of water and metal penetration.

LF and HF RFID systems can be counted to near field communication systems, using inductive coupling from a magnetic field, whereas UHF and microwave systems use far field communication with backscattering of radio waves [25].

3.4 Standards

As RFID technology began to spread rapidly all over the world, global standards needed to be accomplished in order to clearly define RFID technology as multiple standards serve as entry barrier. Standards were developed by several organizations such as the International Standardization Organization (ISO) in corporation with the International Electrotechnical Comission (IEC) called ISO/IEC, and as earlier introduced EPCglobal Network. Both developed their standards hoping for an adoption to a global standard, which was accomplished in 2006 [16]. In the following several important RFID standards are introduced.

3.4.1 ISO/IEC 14443 - Smart Cards

ISO/IEC 14443 "Identification cards - Contactless integrated circuit cards - Proximity cards" is a standard for contactless smart cards with a range of 7-15cm. This standard is commonly utilized in ticketing and payment systems later described in this paper [31].

ISO/IEC 14443 - Proximity-Coupling Smart Cards:
Part 1: Physical characteristics
Part 2: Radio frequency power and signal interface
Part 3: Initialization and anti-collision
Part 4: Transmission protocol

The first part describes the physical characteristics of the tag, such as standardized size and shape as well as material properties [18].
Part two specifies this type of tag to be passively powered

doi: 10.2312/NET-2013-02-1_04

at a frequency at 13.56 MHz and introduces two communication interfaces, which are not interchangeable during an ongoing transmission. Type A and Type B operate at the same subcarrier frequency of 847 kHz for tag-to-reader communication and have the same data transmission rate of 106 kbit/s for any directions of communication whereas they differ by used modulation and synchronization methods. Type A implements frame synchronization by detecting start-of-frame and end-of-frame marks, Type B relies on one start- and one stop-bit per byte [18].

Next "Initialization and Anticollision" introduces frame structures and anti-collision procedures for each type. Collisions occur when more than one tag tries to communicate with the reader at the same time.
When a type A card enters an active read range of a reader, it puts itself into the IDLE mode, not interrupting an ongoing communication. Now the reader can issue a REQA command (Request-A) which is replied by an ATQA block (answer to request) causing the card to switch to the state READY. The reader triggers the anti-collision algorithm based on a dynamic binary search tree by sending a SELECT command. After having chosen the tag for communication the reader issues a SELECT command with the target tag's serial number. The selected card switches into ACTIVE mode and is now ready for transmission.
Type B also switches into IDLE mode when entering an interrogation field waiting for a REQB (Request-B) command which triggers the anti-collision algorithm utilizing a dynamic slotted ALOHA procedure with parameters dictated by the reader. The REQB frame includes two parameters, one for choosing the card's application group for preselecting and one for communicating available slots. After a random waiting interval the card starts to transmit when a slot marker indicated the start of a new slot. The tag sends an ATQB (answer to request B) command, receives additional protocol parameters (ATTRIB), then switches into ACTIVE state and is now ready for transmitting. Readers can cut idle slots by issuing a new slot marker to save time [18].

Lastly transmission protocols are introduced for transmission error handling. ISO/IEC 14443-4 is based upon a standard for non-wireless contact smart cards (ISO/IEC 7816-3) which is an advantage for the implementation of dual interface smart cards as both protocols are compatible. Type A cards need additional information about protocol parameters, which Type B cards received with the ATTRIB command, FSDI (frame size device integer) which defines the maximum frame size and an optional CID (card identifier) for addressing an individual card in the interrogation zone. After ensuring the availability of the 14443-4 protocol data is sent using the following frame structure [18, 32]:

PCB	**[CID]**	**[NAD]**	**[INF/APDU]**	**CRC**
1 byte	1 byte	1 byte	N byte	2 bytes

Figure 2: Frame structure in ISO/IEC 14443

The PCB field (Protocol Control Byte) provides additional protocol parameters, NAD (Node ADress) is optional, and INF (Information) / APDU (Application Protocol Data Unit) is optional and forms the payload of the frame. Lastly CRC is used for error detection in the payload [18, 32].

3.4.2 ISO/IEC 18000 - Air Interface Standards

In 2004 a committee created by ISO and IEC released the so called RFID Air Interface family of standards: ISO/IEC 18000 Series, which standardized transponders and defined an "Air Interface" to be used for communication between tags and readers at various frequencies. This standard has been modified several times, adapting to the fast development progress of RFID technology.

ISO/IEC 18000 - RFID for Item Management:
Part 1: Generic parameters for Air Interfaces for globally accepted frequencies
Part 2: Air Interfaces below 135 kHz
Part 3: Air Interface at 13.56 MHz
Part 4: Air Interface at 2.45 GHz
Part 5: Air Interface at 5.8 GHz
Part 6: Air Interface at 860 MHz - 930 MHz
Part 7: Air Interface at 433.92 MHz

3.4.3 ISO/IEC 15691 and 15692

These standards define functionalities of readers and the communication interface between readers and applications. ISO/IEC 15691 defines commands, responses and error messages, which can be used for communication between the application host and the reader. For writing data from the reader to a tag, ISO/IEC 15692 defines memory mapping rules. This is necessary since the tag's memory is organized in blocks and segments so data can only be transferred in blocks. Therefore the reader preprocesses and segments the data according to ISO/IEC 15692 before sending it to the tag [18].

3.4.4 Electronic Product Code (EPC)

When applying RFID technology to countless products produced by thousands of companies it seemed important to introduce a numbering scheme to RFID tags to be able to track back where a certain product came from. Therefore the MIT Auto-ID Center developed the Electronic Product Code (EPC), a standard for numerous numbering schemes. An example would be the General Identifier (GID-96) which can be seen as an improvement to the existing barcode numbering scheme (UPC) which uniquely identified manufacturer and product. In addition to this functionality GID-96 can also identify every single article of each product group, so every item has its own unique number.

Header	**EPC Manager**	**Object Class**	**Serial No.**
8 bit	28 bit	24 bit	36 bit

Figure 3: General Identifier Format (GID-96)

Figure 3 illustrates the used numbering scheme: The header field describes the used scheme, for example for GID-96 this would be 0x35. The EPC Manager field is a registered number unique for every manufacturer, Object Class contains an identifier for the object class i.e. "Some-Brand's Cookies", and the Serial Number field gives every single unit of this object class a unique number, so in this example every package of cookies could be uniquely identified. Other common EPC numbering schemes are the serialized global

doi: 10.2312/NET-2013-02-1_04

trade item number (SGTIN), serial shipping container code (SSCC), serialized global location numer (SGLN) and the global individual asset identifier (GIAI) [33].

4. RFID APPLICATIONS

Modern RFID technology is already deployed in numerous fields: asset utilization, asset monitoring and maintenance, item flow control in processes, inventory audit, theft control, authentication, payment systems, etc. Currently production costs for low-cost passive RFID tags are about 5 cents, with continuing research further improvements in range, size, costs can be expected, as RFID experts dream of a 1 cent tag finally making the costs neglectable and allowing RFID to be deployed ubiquitously [34].

4.1 Electronic Passport

Since August 2006 all 24 EU members are required to integrate ISO/IEC 14443 conform RFID technology into the so called ePassport. The main purpose of this development is to improve passport security against forgery. A chip integrated into the data page or the cover stores personal information about the holder, such as name, date of birth, gender, biometric features of the face, and since 2008 fingerprints. This information uses about 32kByte of memory, which is a specified minimal requirement. The contents are secured against forgery by a digital signature which can be checked with a public code from the country's signing certification authority to ensure data integrity and authenticity. Due to a data transfer rate of 848 kBit/s at a read range of 10 cm this technology allows border controls at airports to process more travelers in less time. RFID technology is ideal for this purpose, as it is cheap, fast, easy to integrate into a passport, and makes forgery of passports more difficult. Several countires outside the EU use this technology as well, for example Japan, Singapore, and the US [18].

4.2 Credit Cards

In 2005 several major credit card organizations started to offer contactless credit card payment to their customers. Embedded passive RFID tags operating at a frequency of 13.56 MHz, allow the card holder to pay on the fly, by placing the credit-card-containing wallet close to the reader (max. 4 cm) which then requests the stored information required for a successful transaction. Worldwide established systems are called PayPass (MasterCard), ExpressPay (American Express), and payWave (Visa), and follow the ISO/IEC 14443 standard for identification cards, contactless integrated circuit cards and proximity cards [18]. RFID technology is well suited for the purpose of making transactions easier and faster. As this application is especially prone to attacks, payments neither requiring a signature nor a PIN are limited so small amounts such as $25 whereas larger values need to be authorized by the card-holder [31]. Possible attacks and securities issues as well as solutions to the problem of vulnerability of contactless credit cards are discussed later in this paper.

4.3 Access Control

One of the most popular applications of RFID technology is access control. Compared to other systems it has many advantages in addition to operating wirelessly, such as very high adaptability. Keys can easily be excluded from the system, permissions can be altered, temporary access can be granted, the system can be extended by additional cards and readers, etc. All of the mentioned changes can be made very fast and easily. Online systems are formed out of cheap tags which only carry a number, which can be received by a reader connected to a database via a network. The database contains permissions associated with tag numbers, telling a door to open or to remain closed. In offline systems the key contains the data needed for access. The stored data can be altered and in case of a lost key, every reader has to be informed about which key will be excluded.
RFID enabled electronic access control systems are very useful since a large number of people with different access authorizations can carry a single key without having to plan a complicated lock system before installing it. For example the cleaning personnel can receive keys which only open doors at nighthours or temporary workers can receive a time restricted key [18].

4.4 Prospects

Today and in the near future much more functionality will be transferred into mobile phones with internet access using NFC technology, enabling mobile devices to act as credit cards, tickets for public transportation or public events, access control cards, tracking device, etc. This is one of the developments contributing to the Internet of Things (IoT), described in the IoT action plan for Europe by the Commission of the European Communities [35]. As legal restrictions are starting to allow the deployment of RFID technology in humans, future applications will most certainly include the wide spread use of human implants for previously named applications and beyond [21].

5. RISKS AND ATTACK VECTORS

With RFID technology increasingly being deployed in security relevant applications such as anti-theft, access control, and electronic payment systems, it is prone to be attacked. In the following various attack vectors are presented along with possible countermeasures.

5.1 Basic / Physical Attacks

Attacks on RFID systems on the physical layer can be very simple. Since only a fully operable tag can be detected by a reader in range, removing the tag from the tagged object is sufficient to fool for example an EAS systems. Common countermeasures implemented in tags are acoustic alarms or the release of colour from inside the tag when someone tries to remove it improperly, which draws attention to a probable thief or permanently damages the object it was attached to. Tag destruction can be achieved through the application of too much mechanical force or for most RFID tags by applying a very strong electromagnetic field, which can destroy an essential part of the tag. Since most transponders are very fragile, they must be protected by a more robust design or by placing it inside the tagged object. The proper way to permanently disable a transponder is to issue the kill-command which is specified by EPCglobal. The unautherized execution of the kill command can be prevented by implementing a sufficiently strong password protection, which is required for Gen2-tags.
Temporarily disabling tags can be achieved as easily as by

doi: 10.2312/NET-2013-02-1_04

shielding the tag with common aluminum foil. As mentioned before electromagnetic waves cannot efficiently penetrate metal, therefore the tag cannot communicate with the reader. Attackers can also jam the frequency range, which is used by tag and reader by applying a signal in the same frequency range. This interferes with communication signals and as a result the reader receives only noise. The described effects can also be caused by unintentionally placing the tag in a shielded area or by a noisy environment. Detection of disabled tags by an RFID system is impossible, therefore other means of security, such as video cameras or locked doors should be used additionally in order to prevent physical attacks [36].

5.2 Eavesdropping

The interception of communication (eavesdropping) is one of the most popular attacks on wireless systems. Data is intercepted at some point in the range of tag and reader, an area which can range from few square centimeters up to several hundred square meters, which can even be significantly extended by using more sensitive antennas such as beam antennas. Detection of useful data from vast distances depends on many environmental factors like the presence of metal objects or water can weaken and block the sent signals [18].
After successful interception, the received information can also be used in more sophisticated attacks such as cloning and replay attacks. Car theft can be an application for replay attacks, which can be stolen by replaying the signals, intercepted when the car owner opened or closed the car using a remote wireless key using RFID technology [37].
An exemplary countermeasure is the limitation of signal strength and use of shielding or directional transmission to restrict the reading range to the actually needed area. The deployment of multi-channel communication and communication protocols with strong security policies can prevent replay attacks but realizing secure protection against eavesdropping itself is very difficult if not impossible [18].

5.3 Cloning

Cloning is the task of creating a replica of the original object. This method has been used for decades to duplicate credit and debit cards in the area of credit card fraud for decades as criminals copied the stored information of a credit card and applied the data to a different card which contains all needed data to withdraw money from the victim's account. The original card usually leaves the hand of the card owner and disappears into a machine involved in a financial transaction or a waiter takes the card away to the cashier. In the meantime the card's information can be copied and the regular transaction takes place as expected, arousing no suspicion by the card owner. This acquisition of data always needed mechanical contact with a reader which can possibly be out of sight. As major credit card organizations deployed wireless technology in credit and debit cards, one of the benefits seemed to be that the card never left the owner's hand, was always in sight and could not be mishandled by a corrupt cashier, supposedly increasing the safety concerning credit card fraud. Au contraire this new technology offers a new interface to retrieve information in a split second without somebody possibly noticing it as these cards broadcast their information in every direction through the air to a reader up to 4 cm away when a request was received. Richard Vanderhoof from Smart Card Alliance stated he does not see an increased risk in this use of RFID technology [38].
In June 2012 "Report München" a German television show aired a report about how easily this information can be extracted. They developed an application for a NFC enabled smart-phone and were able to retrieve several sets of credit card information in public by holding the mobile device close to pedestrians' wallets, unnoticed. It is to note that no encryption or password protection was used [39].
Similar methods can be used to clone other RFID tags, like access cards, price tags, etc and to apply the gathered data to similar tags with read/write memory. The usage of cloned tags may be undetectable as for the reader there is no difference in the cloned tag compared to the original.
Ways to avoid tag cloning on the physical layer in advance are the disabling or destruction of the transponder, or to shield the tag by wrapping it into aluminum foil. More applicable is the inclusion of security means in the backend, such as the storage of already read serial numbers as some tags might only be read once, or by disallowing the simultaneous use of supposedly unique tags in two different locations. Common ways to protect data from being accessed without authorization are the use of passwords and encryption on the tag, thus causing a tag's price to increase as usually more hardware is needed [38].

5.4 Virus Attacks

Most RFID are connected to rather complex backend systems, processing the data received through an RFID transmission. In general the communicated tag content contains a unique serial number for identification and some further information about the object. As modern reusable tags have data storage capacities exceeding several kilobytes of read/write memory this information can be altered or completely new tags are introduced to an existing RFID system. Additional or wrong data can be written on the tag causing unintended data to be sent to the backend system which now can perform differently than expected from the initial legit data processing. If this attack scenario has not been accounted for in the development of the affected backend system, additionally received and executed commands have the potential to harm the entire system as the attacker now has control over some system components. Databases could be copied, altered, or deleted (i.e. SQL-injection), web-based components could download hazardous files from the internet containing malware (for example by using enabled JavaScript in Browsers) and even files could possibly be removed or altered (code insertion) causing the entire system to fail.
Virus attacks can be prevented by a well designed system, which does not allow unintended behavior. For example to prevent SQL-injection in databases, developers can use predefined statements, telling the system exactly which kind of data to expect and clearly define how to use it in the next query. As this form of defense does not require additional hardware in tags or readers it does not contribute noticeable to additional costs for an RFID system [38].

5.5 Privacy

With RFID technology spreading rapidly into many aspects of every day life, RFID systems are able to collect enormous amounts of data. As it is a wireless technology the data can be read unnoticed, no contact is necessary and common tags

doi: 10.2312/NET-2013-02-1_04

cannot log who tried to access which information. Countless items are already enabled to act as RFID tag, for example passports, credit cards, ID-cards, customer loyalty cards, library books, event tickets, bank notes, and even regular grocery purchases may contain RFID tags. If the data on those transponders is unsecured or the used security measures are easy to breach, it can be read by anyone in range. Possible privacy violations are apparent in the following example: Someone shops in a large grocery store, which uses RFID everywhere. Customer loyalty cards enable the store to create movement profiles of every single customer and associate items to a person, which tells the store preferences and habits. Even if that person carries other companies' RFID enabled products, this store is able to tell where else this person goes for shopping and what was bought. Bank notes acting as tags could reveal a customers financial situation to anyone in range. Out of collected data one can most certainly conclude information which one never agreed on sharing, which is a privacy violation.
One can avoid privacy issues by designing RFID systems properly with tags supporting password protection and encryption as well as by limiting the read range of reader and tags to the necessary distance not allowing someone to access stored information unauthorized [40].

6. CONCLUSION

RFID technology connects objects with associated data, in other words the real world with the virtual world. Therefore it can contribute vastly to the development of the Internet of Things. Although RFID makes many aspects of life easier and more comfortable, there are always risks involved which should not be underestimated. With a proper system design one can try to use this technology for the better and take advantage of the great opportunities RFID technology provides. With decreasing prices for tags and rapidly developing applications RFID is becoming more and more ubiquitous, it will soon be impossible to imagine a life without RFID.

7. REFERENCES

[1] Andy Jones: *Proceedings of the 3rd European Conference on Information Warfare and Security*, page 81, Academic Conferences Limited, 2004

[2] TM E 11-219 Directory of German Radar Equipment: *Airborne Radar: FuG 25 Airborne IFF Transmitter-Receiver*, April 20, 1945

[3] Jerry Scutts: *German Night Fighter Aces of Word War 2*, page 84, Osprey Publishing, Oxford, GB, 1998

[4] Harry Stockman: *Procedings of the I.R.E. - Communication by Means of Reflected Power*, pages 1196-1204, The Institute of Radio Engineers Inc., NY, USA, October 1948

[5] Jeremy Landt: *The History of RFID*, AUTO-ID Labs at MIT, November 2005

[6] Donald Harris: *Radio Transmission Systems with Modulatable Passive Responder*, United States Patent Office, No. 2927321, March 1, 1960

[7] Robert M. Richardson: *Remotely Actuated Radio Frequency Powered Devices*, United States Patent Office, No. 3098971, 1963

[8] Justin Patton: *RFID as electronic article surveillance: Feasibility assessment*, University of Arkansans, AR, USA, December 2008

[9] Daniel F. Cuff: *BUSINESS PEOPLE; An Anti-Theft Specialist Bolsters Its Top Ranks*, New York Times, NY, USA, November 8, 1990, `http://www.nytimes.com/1990/11/08/business/business-people-an-anti-theft-specialist-bolsters-its-top-ranks.html/`

[10] Bloomberg Businessweek: *Company Overview of Sensormatic Electronics, LLC*, `http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=302947/`

[11] Bloomberg Businessweek: *Checkpoint Systems Inc (CKP:New York)*, `http://investing.businessweek.com/research/stocks/snapshot/snapshot.asp?ticker=CKP/`

[12] Alfred R. Koelle, Seven W. Depp, Robert W. Freyman: *Short-Range Radio-Telemtry for Electronic Identification, Using Modulated RF Backscatter*, Los Alamos Scientific Laboratory, University of California, Los Alamos, NM, USA, Febuary 10, 1975

[13] Cardullo et al: *Transponder Apparatus and System*, United States Patent Office, No. 3713148, 1973

[14] Charles A. Walton: *Electronic Identification and Recognition System*, United States Patent Office, No. 3816709, 1973

[15] Timothy D. Hau: *Congestion Charging Mechanisms for Roads: An Evaluation of Current Practice*, The World Bank, Washington DC, USA, December 1992

[16] V. Daniel Hunt, Albert Puglia, Mike Puglia: *RFID: A Guide to Radio Frequency Identification*, John Wiley & Sons, 2007

[17] EPCglobal Inc.: *GS1 EPCglobal - Frequently Asked Questions*, January 2007, `http://www.gs1.org/docs/epcglobal/ Frequently_Asked_Questions.pdf`

[18] Dr. Klaus Finkenzeller: *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near Field Communication*, Wiley, 2010

[19] Mark Roberti: *The History of RFID*, RFID Journal, `http://www.rfidjournal.com/article/view/1338/`

[20] *A Summary of RFID Standards*, RFID Journal, `http://www.rfidjournal.com/article/view/1335/`

[21] Thomas C. Greene: *Feds approve human RFID implants*, The Register, GB, October 14, 2004, `http://www.theregister.co.uk/2004/10/14/ human_rfid_implants/`

[22] Image of an RFID sticker on a DVD for EAS, photo by Lukas Grillmayer

[23] Jongwoo Sung, Daeyoung Kim: *Sensor Profile Requirements for Sensor Network Capability Information in the EPCglobal Network*, Auto ID Labs, Korea Advanced Institute of Science and Technology, March 2009

[24] Bill Glover, Bhatt Himanshu: *RFID Essentials*, O'Reilly Media Inc., 2006

[25] Gaynor Backhouse: *RFID: Frequencies, standards, adoption and innovation*, JISC Tech Watch, May 2006

[26] *EPCglobal Tag Class Definitions*, November 2007, `http://www.gs1.org/docs/epcglobal/ TagClass-Definitions\_1\_0-whitepaper-20071101.pdf`

doi: 10.2312/NET-2013-02-1_04

[27] Sky RFID Inc.: *RFID Gen 2 - What is it? - Smart RFID!*, http://www.skyrfid.com/RFID_Gen_2_What_is_it.php
[28] *RFID System Components and Costs*, RFID Journal, http://www.rfidjournal.com/article/ article-view/1336/1/129/
[29] *What is the Lifespan of an Active Tag*, RFID Journal, http://www.rfidjournal.com/article/view/4673/
[30] *NephSystem Technologies*, http://www.nephsystem.com/
[31] Visa Inc.: *Visa payWave - FAQ*, http://usa.visa.com/merchants/payment_ technologies/paywave_faq.html/
[32] *ISO/IEC 14443-4: Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission protocol*, 2008
[33] GS1 EPCglobal: *GS1 EPC Tag Data Standard 1.6*, September, 2011
[34] Mark Roberti: *A 5-Cent Brakethrough*, RFID-Journal, May 1, 2006, http://www.rfidjournal.com/article/ article-view/2295/1/128/
[35] Commision of the European Communities: *Internet of Things - An action plan for Europe*, Brussels, June 18, 2009
[36] Aikaterini Mitrokotsa, Melanie R. Rieback and Andrew S. Tanenbaum: *Classification of RFID Attacks*, http://www.cs.vu.nl/~ast/publications/iwrt-2008.pdf
[37] Aurélien Francillon, Boris Danev, Srdjan Capkun: *Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars*, ETH Zurich, Switherland
[38] Frank Thornton, John Kleinschmidt: *RFID security*, Syngress Pub., Rocklannd, MA, USA, 2006
[39] Ronald Eikenberg: *Kreditkartenklau per Smartphone*, June 6, 2012, Heise Online, http://www.heise.de/newsticker/meldung/ Kreditkartenklau-per-Smartphone-1611874.html
[40] Dirk Henrici: *RFID Security and Privacy*, Springer, May 2008

doi: 10.2312/NET-2013-02-1_04