BULETINUL Universităţii Petrol – Gaze din Ploieşti	Vol. LXI No. 3/2009	87 - 92	Seria Tehnică

Considerations about RFID Systems Vulnerabilities

Nicolae Paraschiv[*], Toader Melinte[**], Emil Pricop[*]

[*] Petroleum – Gas University of Ploieşti, 39 Bucureşti Blvd., Ploieşti, ROMÂNIA
e-mail: nparaschiv@upg-ploiesti.ro, emil.pricop@gmail.com

[**] S.C. SEEKTRON S.R.L., Şos. Vestului, nr.33, Ploieşti, ROMÂNIA
e-mail: office@seektron.ro

Abstract

RFID is a novel technology for automatic object identification, marking and tracking. It is very important to ensure the security of RFID systems, since many organizations have already included such devices in many applications: ticketing, goods tracking, hospital and medication management and even banknotes tracking and anti-counterfeiting. In this paper we will explain the threats on RFID systems such as specific viruses and weak privacy and data security strategies. We will analyze the risks introduced by those systems and then we will present some methods for securing RFID applications. Our research result will be a security guideline for application designers, developers and system administrators.

Key words: *RFID, security, virus, cryptography, privacy.*

Introduction

Radio Frequency Identification (RFID) is a novel technology for automatic object (goods, products, animals and even people) identification, marking and tracking. If you search the term RFID in Google you find about 30.000.000 results, giving us the right to say that the technology is becoming more popular each and every day. This fact might be caused by the marvelous performances and the large number of RFID applications. Basically speaking the RFID systems are similar to the widespread barcode identification systems, being regarded as an evolution.

The consumer RFID systems contain mainly three components: the reader and the transponder, also named tag, and a backend database. The tag has two sections: one for radio communication and a memory used for storing data and custom fields. There are mainly two categories of RFID tags: active and passive. The active tags are writeable and readable and have an internal power source (a battery), so the lifetime of an active tag is limited. The passive tags obtain the energy from the magnetic field of the reader. These types of tags are smaller, cheaper and could be used an unlimited time. The functionality of RFID passive tags is very simple: when a tag is in the nearby of a reader, it detects the radio signals generated by the reader and starts to transmit the data stored in the memory. The radio signal generated by the reader offers the power needed to function and the synchronization data for communication between the two entities [1].

Technical aspects of RFID systems

RFID systems use wireless radio communication technology to uniquely identify tagged objects. The three basic components of a RFID system, as shown in figure 1, are:
- a tag or a transponder, composed by a chip, an antenna and optionally a battery;
- a reader, also called interrogator, which is composed of an antenna and electronic modules;
- a computer or a controller that usually run database and middleware software.

The tag and the reader communicate using radio waves. Tags can hold many kinds of information about the objects they mark, including serial numbers, time stamps, and configuration instructions. When the reader receives data from card it transmits to the middleware via network protocols such as RS-232, RS-485 standard IP network or even the Internet. Using Internet connected devices users could create a global distributed system for product tracking and inventory. In this case there are special security issues related to Internet communication and centralized database protection schemas.

The tags consist of an electronic chips and an antenna encapsulated in a package forming a single piece of material. The chip contains a memory that is usually read-only. The active RFID tags contain an internal power source, so they can communicate with less powerful readers and have a longer work distance. The active tags have a larger memory of about 128 KB and often are writeable. Passive tags does not have an internal power source, they get the power needed to transmit data from the signal sent by the reader. They have usually a smaller memory, a short transmission distance and a cheap price.

Basically speaking the RFID reader must read data from the tag and send it to another device controller, PC or database server. For building secure systems the readers must implement anti-collision measures, so they could communicate with many tags simultaneous, authenticate tags and encrypt data. There are three types of anti-collision methods: spatial, frequency and time domain. All are used to implement a transmit order for the tags being in the nearby of the reader. Tag authentication and data encryption are basic methods for ensuring data privacy and integrity. The algorithms in use nowadays are not very complex; they mainly use symmetrical encryption keys.

The brain of any RFID system is the device called controller. Physically it could be a PC which runs a specific application, database server or an embedded system specially designed for RFID application. The controller manages the information gathered in the field by the readers; it could track the movement of objects, debit an account in a point-of-sale application or keep inventory in a supermarket. In many applications the controller is connected directly with the enterprise network, resulting in special security requirements.

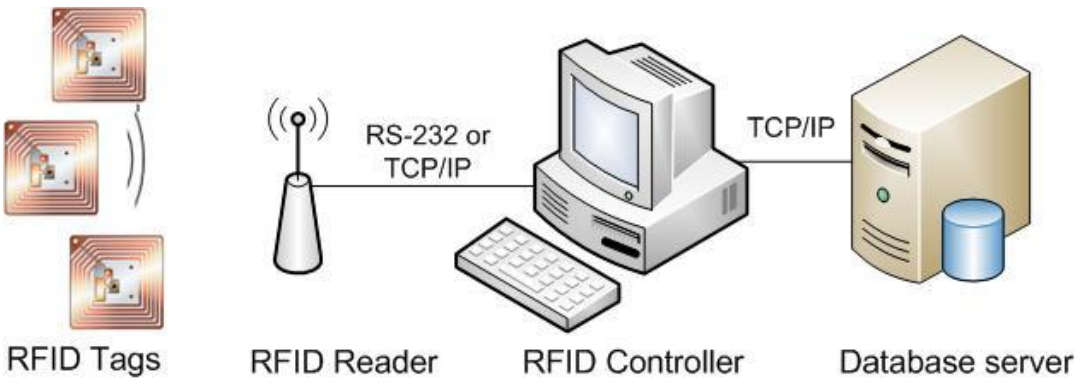

Fig. 1. The general architecture of a RFID system.

RFID systems use diverse radio frequency bands for communication between the tag and the reader. Low frequency bands are 125-134 KHz and 13.56 MHz. The tags on High Frequency (13.56 MHz) have been standardized by Philips and are also known as Mifare tags. Ultra high frequency (UHF) bands used by RFID are 860-960 MHz and microwave bands at 2,4 GHz and above. The read range varies from 2 centimeters, in case of low frequency passive tags, to 2-5 meters when using microwave active RFID tags. The data rate is usually in order of Kbits/s [3].

The risks associated with RFID systems

A topic that has been ignored for a long time by researchers is the security of the RFID systems. Nowadays, the number of threats and attacks is increasing because the technology (equipments, software and documentation) is available for public and the bad intentioned people try to find ways for stealing data, denial of service and even taking over the systems. So, it is a very important task to ensure the systems security, since many organizations have already included radio identification devices in many applications: ticketing, goods tracking, hospital and medication management and even banknotes tracking and anti-counterfeiting.

We should effectively manage the risks of RFID systems in order for their implementations to be efficient and successful. This technology is a complex one, combining different computing and communication technologies. The mainly risks associated to RFID systems are: business process risk, business intelligence risk, privacy risk and intrusion risk [2].

Business process risk represents the risk of service interruption in RFID-enabled process. For example a warehouse that identifies the goods only by RFID tags cannot process orders or track the goods if the RFID system fails.

Business intelligence risk represents the risk of unauthorized access to RFID data. An adversary could use collected data against the organization, for example they could detour a shipment when they get positive reading of RFID tag.

Privacy risk seems to be the most discussed one. Do our society risk becoming a surveillance security by using RFID systems? The public is generally concerned with the protection of their personal information. Citizen right groups in many countries fear that RFID tags on consumer goods might be misused. They suppose that secretly scanned tags enable companies to make profiles of behavior and movement, profiles that could be used by supermarkets to know everything about their customers and to optimize their marketing strategies. The fear is not underlain because in the most applications in use today personal data is not employed at all. But if personal data is stored on a RFID chip, such as loyalty or credit cards, the national and international data protection laws and directives must apply. A 2008 report by the Federal German Government says that RFID technology does not require further legislation for handling personal data, other than that applied for other technology [3].

Intrusion risk is not so evident. RFID technology could represent a treat for database systems and networked or collocated systems. For example if a bad intentioned user has access to an IP enabled RFID reader which was not configured properly, he could get access to the whole enterprise network.

Common attacks and countermeasures

The authors of this paper are experienced researchers in communications and data security fields. In this paper the authors will present the common attack types and some recommendation for preventing or decrease the vulnerabilities of RFID systems, based on their practical and research experience.

One common attack type is sniffing. It consists of an unauthorized RFID reader that could read virtually any type of tag in its nearby. The obtained data may be used for spoofing attacks. Bad intentioned people can write properly formatted data on RFID transponders and use them to compromise the systems. Research about spoofing attacks has been made at Johns Hopkins University and RSA Security. The researchers cloned a transponder with sniffed data and then they used the tag to buy combustibles in a gas station. The countermeasures for these kinds of attacks are tag authentication and data encryption [2, 4].

Attackers may build devices that can retransmit captured data or RFID queries. Using these devices they can do so called replay attacks, fooling digital passport readers, contactless payment systems or access control stations. Challenge-response authentication algorithms must be implemented in order to prevent this type of attack.

The most dangerous attacks are RFID-based exploits of middleware database system. This may consist of buffer overflows, code insertion and SQL-injection, leaving a door open for hackers, worms and viruses. Even if a RFID tag has only 1 KB of memory it could be use with ingenuity to launch an attack with sufficient power to compromise the database, the computer or even the entire network.

Buffer overflows are the most common vulnerabilities found in software. They have played an important role in the apparition of various computer worms such as Code Red and SQL Slammer. Buffer overflows usually appears when using programming languages like C or C++ with functions that are not memory-safe such as strcpy, strlen, strcat or functions with many pointers. The buffer overflow appears when the input data is longer than the allocated buffer memory. This data overwrite the program control data which is adjacent to the buffers and cause the programs execute random code. RFID tags can exploit buffer overflows to compromise the middleware system (controller); an attacker could use an active tag or a specially designed transponder simulating device with much memory to blow the middleware's buffers.

Another type of attack against the middleware system is code insertion. Malicious code could by injected using scripting languages such as VBScript, JavaScript, Perl and HTML. RFID tags could contain data written in a scripting language that could affect the security of middleware system, if the software can interpret the languages.

A special type of code insertion attack is represented by SQL injection. This type of attack may tricks the database server into running malicious SQL code. The first object of the attacker is to discover the database structure. Using this information the attacker could retrieve, modify or delete data. Even if RFID tags contain a small quantity of data, they could be used to harm the backend database with small injected commands that could even stop the SQL server.

Another important threat in the security of the RFID systems is represented by RFID worms. They spread from a tag to another if the tags are writeable or when a tag is written from a computer or a database infected with the malicious piece of software. The tag is functioning properly but the data from it, when introduced in the backend database, could action modifying data, launching a large number of processes, downloading other malicious software or leaving a backdoor open for a hacker to connect to the enterprise network. These actions are also called worm's payload.

The RFID viruses can spread by themselves, the attack vector being just one infected RFID tag. This threat is applicable more likely in case of reusable RFID tags, which can be written and read many times. The virus uses SQL injection to attack the middleware systems. When the tag data is read the code is executed unintentionally by the database engine. We assume that the virus copies itself to all the data in a row of a table in the database. When a new tag is emitted, it will contain the virus body taken from the database, and then this newly-infected tag will spread the virus to infect other tags and possibly other middleware components. The virus presented is not so stealth, but its developer could use SQL stored procedures, leaving the tables in the

database unmodified at least at the first view. Let suppose that together with the self-spreading mechanisms the virus may have a payload that modify some data in the database or leave a port open on the server.

The threats of worms and viruses could be eliminated by following some simple countermeasures. First of all the programs and scripts must be developed permanently checking the bounds in the case of C and C++ programming languages and with compiler's bounds-checking option enabled in case of Visual Basic, Java or C#. Also it is very important to audit the software development process. To avoid code injection the inputs must be verified to contain only valid characters and it is recommended to disable back-end scripting languages. That include turning off client-side languages like JavaScript, VBScript, ActiveX, Flash and the server-side ones such as Server-Side Includes and CGI. Another good security measure is to limit the rights of the database connected user. For example tables that contain data that do not modify must be set read-only. Also it is recommended to disable the execution of multiple SQL statements in a single query.

The RFID middleware server could be isolated from the enterprise network using the DMZ, Demilitarized Zone, which is a critical component of the security system. It is composed by hardened servers with latest software patches. These servers could be accessed from the Internet directly. A usage scenario could be that DMZ server has Terminal Services running for Remote Access and the user could connect form Internet to the DMZ server and from the terminal to a computer situated in internal protected network zone [5].

Conclusions

The RFID systems could be affected by many security threats. In this paper we have shown the common attack types: sniffing, identity spoofing and replay-attacks. There were presented new security risks such as RFID spreading worms and viruses that could affect the RFID middleware component which is the brain of the whole system. We have proposed a hierarchy of security measures that must be taken by the developers and the implementers of RFID in order to ensure the security of their applications: code bounds checking, data encryption and tag authentication, correct users permission on middleware database and isolation of internet connected radio identification systems in the DMZ. RFID systems became connected to the enterprise network and a security breach in this zone could lead to an unsecure and vulnerable company network. Many organizations have already included radio identification devices in many applications such as ticketing, goods tracking, hospital and medication management and even banknotes tracking and anti-counterfeiting. That is the reason why any breach in RFID security is not permitted.

References

1. Finkenzeller, K. – *RFID Handbook: fundamentals and applications in contactless smart cards and identification, 2nd ed.* John Wiley & Sons Ltd., West Sussex, 2003.
2. Ahson, S., Ilyas M. – *RFID Handbook. Applications, Technology, Security and Privacy*, CRC Press LLC, 2008.
3. Hunt, D., Puglia, A., Puglia, M., – *RFID – A guide to radio frequency identification.* Wiley-Interscience, 2007
4. *** – *The Quintessence of RFID Technology*. Issue 03 – 2008-2009, EBV Elektronik GmbH &Co. KG, Poing, Germany.

5. * * * – *Securing Process Control Network External Communications*. PCN Data Honeywell – Whitepaper, 2007.

Consideraţii privind vulnerabilităţile sistemelor RFID

Rezumat

RFID, identificarea prin radio-frecvenţă, este o tehnologie relativ nouă care este utilizată la marcarea, identificarea şi urmărirea obiectelor. Numărul aplicaţiilor bazate pe RFID s-a diversificat în ultima perioadă, multe organizaţii utilizând identificarea prin radio-frecvenţă în sisteme de eliberare a biletelor, de urmărire şi identificare a pacienţilor şi medicamentelor în spitale şi chiar în soluţii de protecţie împotriva falsificării bancnotelor. În această lucrare vom analiza riscurile şi ameninţările la care sunt supuse aceste sisteme din punct de vedere al securităţii informaţiei. Dorim ca rezultatele cercetărilor prezentate în această lucrare să reprezinte un ghid pentru proiectanţii şi implementatorii de sisteme RFID.