Implementing high-level Counterfeit Security using RFID and PKI[1]

Andreas Wallstabe B.Sc. in Computer Science and Prof. Dr. Hartmut Pohl, Information Security, Department of Computer Science, University of Applied Sciences Bonn-Rhein-Sieg, St. Augustin Germany

Abstract

Radio Frequency Identification (RFID) systems have become popular mostly for automated identification and supply chain applications. To implement counterfeit security, RFID- and Public Key (PK) technology are combined. RFID tags authenticate themselves by responding to a challenge of a reader/writer device. For this an asymmetric encryption algorithm (RSA) is implemented and executed on the tag. Thereby a high level of counterfeit security is reached. Using a private/public key pair makes this method very flexible for validation by the distributor or the customer. The asymmetric encryption algorithm is running on a low cost tag providing security even for products with a low value. For high level security, drugs are used as example products.

1. Introduction

Today 5 - 7% of the international trade is counterfeited [11]. This corresponds to a value of about 534 billion $ US in 2004 [21]. 10% of the world wide trade of drugs are counterfeited [19]. In 2005 the value of counterfeited drugs was about 35 billion $ US [20]. Hence the pharmaceutic industry has a tremendous financial loss because of counterfeited products. The reputation and the existence of the pharmaceutic industry are threatened too. Much more relevant is the health of the customer witch is in a serious danger by consuming counterfeited products: Not only by having a lower efficiency of the active substance, the counterfeited products can be harmful or deathly. Today the automated identification of objects with electromagnetic fields is the major purpose of the RFID (Radio Frequency Identification) technology. RFID systems basically consist of transponders (tags), readers/writers (scanners) and application systems for back office processing of the acquired data. There is a large variety of different RFID systems: they may use low, high or ultra high frequencies, the tag may emit only a fixed identifier or possess significant memory and processing capabilities. Tags may incorporate no security features at all or realise effective security protocols similar to smartcards. Most tags are passively powered by the radio field emitted by the reader but there are also active tags with a separate power supply. The tag design is also little uniform: there are e.g. tiny tags with a size of several millimetres, very thin “smart labels” or standard ID-1 cards [6, 12].

A high level of counterfeit security can be implemented by RFID-technology. For this, a tag is attached to every single item. The tag consists of a processor, memory and an antenna. It runs program-driven and stores data which can be read and written contact-less. For such a security level, a non detachable connection of the product with the tag is needed. The tag must not be unnoticed removed or replaced. The RFID-techno-logy is combined with a public key infrastructure (PKI) to raise the counterfeit security. For the implementation of the PKI every tag gets its own key pair. The private key is stored on the tag and must be protected of unauthorised access. Using the private key and an asymmetric encryption algorithm the tag authenticates itself. For this the transponder digitally signs a response with its private key and sends it back to the challenger. The public key needs to be distributed as part of a certificate in a public directory, so everybody can identify and authenticate the tag.

2. Materials and Methods

To verify the identity of a product, it is necessary to make a product anti-counterfeit. There are three authentication categories [10]. Overt authentication features are visible to everybody, they can be verified without any reading or sensing device. Covert authentication features are not directly visible to everybody, an additional reading or sensing device is necessary to verify them. The security level is higher than using overt authentication features [14]. Forensic authentication features are extremely hidden; often based on

[1] The work is part of he Research Project NEGSIT – Next Generation Services in Heterogeneous Network Infrastructures of the School of Communication Systems and Networks (SoCSandNets), Bonn-Rhein-Sieg

"need to know". The analysing techniques for verification are very specialised and only known by some specialists inside the providing company. Forensic authentication features provides the highest level of counterfeit security.
The implemented anti-counterfeit method is a mixture of the covert and forensic authentication features. The verification is as easy as with the covert authentication features but provides a security level as high as provided with the forensic authentication features.
There are many aspects to be considered while implementing anti-counterfeiting with RFID and PKI: The tag itself, the data communication, the RFID reader/ writer, the involved applications, databases and the people implementing and using this protection. In this case the view is limited to the tag itself and the communication with the reader/writer.
Counterfeit security is realised as follows: A tag is attached to the item. It has to be realised a non detachable connection of the item with the tag. The tag must not be removed unnoticed or replaced. E.g. a tag inside a glass packing of drugs. This tag has the ability to authenticate itself. On the tag an asymmetric encryption algorithm is implemented (RSA). The tag is able to sign a message with its private key of an asymmetric algorithm. For authentication purposes an arbitrary message as a challenge is sent to the tag. After reception the tag signs this message using its private key and sends it back (response). Now the signed message can be verified with the public key of the tag and the tag is authenticated.
Using asymmetric encryption the communication between the tag and the reader is overt but can not be used by an attacker. A simple replay of the signed answer of the tag is not possible, because the challenging message is never the same and so the answer (signed challenge with the private key of the tag) is never the same.
For this the RSA algorithm can be viewed as secure. No backdoor is known yet. In Germany the digital signature has a similar status like the autograph signature since 2001 [9]. This makes the high level of counterfeit security and flexibility clear. Everybody can verify a signature. This is realised by providing the public key in a public directory.
The residual risk of the asymmetric algorithm depends on the key. On the one hand it is the key length [4] and on the other hand it is the possibility of a non accessible storage for the key on the tag.
The length of the key to protect a product with a value of about 10,000 $ US should be 768 bit [22]. With the actual price of computing power (August 2006) hacking of a 768 bit RSA key within one year would cost about 10 million Euro. This is only an actual estimation. Because of the steady rising computing power this estimation should be reviewed regularly to be trustworthy.
The second remaining risk is the storage of the private key inside the tag. There are possibilities to read out data of a microcontroller's memory. Today this requires very special knowledge, very high technical equipment and a detailed knowledge of the application itself. These aspects reduce the probability of an attack to a minimum [15]. Additionally special hardware and software defence mechanisms are available. On the hardware side dummy structures, bus and memory scrambling, protection layers and voltage, current and frequency monitoring are possible. On the software side checksums, self tests and encapsuling are possible.
Both residual risks have one thing common: If one key is hacked or read out, only one item can be cloned. Several items or the whole series of items cannot be counterfeited. Thus the counterfeiting effort must be worth one or a very small number of items. This is an advantage in contrast to a symmetric encryption where the key would be the same for many or all the product items.

3. Hardware and Software

The asymmetric encryption algorithm was implemented on an ATAM893 4 bit microcontroller of ATMEL with 4kByte EEPROM and 1kBit RAM [1]. The ATAM893 has been chosen because it is multi-programmable and the ROM version of it is cheap. In combination with the transponder interface IC U3280M of ATMEL the tag functionality can be realised [2]. After connecting each other the Read/Write Device TMEB-8702 of ATMEL can be used to communicate with the tag [3]. The use of this hardware is model like. The implementation is not bound to it. It can be used for any other microcontroller with tag functionality.
For the software development the MARC4 Starterkit TMEB893 of ATMEL was used. It uses the programming language qForth, a 4-bit version of the FORTH-83 standard [7, 5]. Both, the architecture of the ATAM893 microcontroller and qForth are stack oriented. There are no resources or libraries for encryption algorithms known in qForth. They had to be created by the author. Because of the very limited resources of the microcontroller it was necessary to create utilities even for simple tasks like a multiplication with a result higher than 4-bit. This makes the software development very complex. A RSA signature algorithm was realised with a key length of 8-bit as a prototype. With the available resources of the ATAM893 a key length up to 256-bit should be possible. To realise a key length of 768-bit 36kByte of memory are needed [22].
The realised RSA signing algorithm was tested in an emulation environment and on the hardware of the ATAM893. An arbitrary challenge was sent to a port of the microcontroller and it responds with the signed

challenge on the other port. The ATAM893 it is now able to authenticate itself with a RSA signing algorithm.

4. Related work

There is related work providing counterfeit security by RFID and PKI. Texas Instruments and VeriSign have developed a model where both technologies are combined for counterfeit security [16, 17, 18]. There is also a patent discussing counterfeit security is using RFID combined with PKI technology [8]. But in both cases the tag is only used as a storage media. There is no “intelligence” on the RFID tag. The tag does not execute any encryption algorithm. Therefore the tag is very easy to clone, because the information is readable for everybody.
There is one tag available which is able to execute an encryption algorithm: the Phillips Mifare ProX P8RF5016 [13]. But this tag is too expensive (about 20 $ US compared to 2.60 $ US for the used ATAM893) to use it for anti-counterfeiting by today.

5. Future work

Future work will be an extension of the key length for the RSA signing algorithm, either on the ATAM893 or another Tag. The used hardware resources must be very close to the requirements of the security level to make the hardware as cheap as possible even if the effort on development time is getting much higher. In contrast to a very high number of used tags the development costs are pretty small.
Other future work will be to connect a certain tag with an item in a safe way.

6. Conclusion

With the combination of the RFID and PKI-technology and the additional execution of encryption on the tag itself, the counterfeit security is higher than using other current technologies which combine RFID and PK-technology. Without shifting the encryption from the background system to the tag itself, the tag would remain a simple storage media, which could be replaced by barcode or other similar media and counterfeited easily. These media are not protected against cloning because of the unprotected readability of the information. Even with a password protection, the product at all is in danger by compromising the password and the implementation of authentication mechanisms would be very difficult because of the needed knowledge of the password. With the represented implementation of the PKI the authentication can be verified by everybody. Through the shift of the encryption into the tag the product stays secure with the help of logic and plausibility controls. Even by compromising the secret information of one tag only a single item can be cloned and not all the items of the product series. With an additional support of logic controls the single item can only be cloned once. By now this is also the residual risk: It is the unauthorised access to the secret information. Therefore the risk depends on the ability to protect information stored on the tag.
It is possible to combine such a high counterfeit security level with the high flexibility of authentication by the customer and supplier only by the intelligent combination of the RFID and PKI technology.

7. References

[1] Atmel (ed.): ATAM893-D, http://www.atmel.com/dyn/resources/prod_documents/doc4680.pdf, San Jose 2005

[2] Atmel (ed.): U3280M, http://www.atmel.com/dyn/resources/prod_documents/doc4688.pdf, San Jose 2005

[3] Atmel (ed.): TMEB8704 RFID Application Kit, http://atmel.com/dyn/resources/prod_documents/doc4781.pdf, San Jose 2005

[4] Beutelspacher, A. Schwenk, J. Wolfenstetter, K.: Moderne Verfahren der Kryptographie, Von RSA zu Zero-Knowledge, 5. Auflage, Wiesbaden 2004

[5] Brodie, L.: Programmieren in FORTH, München 1984

[6] Finkenzeller, K.: RFID-Handbook, Fundamentals and Applications in Contactless Smart Cards and Identification, München 2003

[7] Hahnen, M: Easy Programming in qForth, http://www.atmel.com/journal/documents/issue5/pg46_48_Atmel_5_CodePatch_A.pdf, San Jose 2006

[8] Heinicke, D.: Produktsicherungssystem und Verfahren hierfür, http://www.wipo.int/pctdb/en/wo.jsp?IA=EP2004001002&DISPLAY=STATUS, Berlin 2005

[9] Heise Online (ed.): Digitale Unterschrift: fast wie eigenhändig, http://www.heise.de/newsticker/meldung/19796, Hannover 2001

[10] ICC Counterfeiting Intelligence Bureau (ed.): The International Anti-Counterfeiting Directory 2005, http://www.icc-ccs.org/pdfs/IACD2005.pdf, Essex 2005

[11] ICC Counterfeiting Intelligence Bureau (ed.): The International Anti-Counterfeiting Directory 2006, http://www.icc-ccs.org/pdfs/IACD2006.pdf, Essex 2006

[12] Knospe, H.; Pohl, H.: RFID Security. Information Security Technical Report: 9, 4, 39 - 50, 2004

[13] Philips (ed.): Mifare pro X P8RF5016 Secure Dual Interface Smart Card IC http://www.semiconductors.philips.com/acrobat_download/other/identification/sfs051814.pdf, Eindhoven 2003

[14] Pohl, H.; Jung, N.; Roth, T.: Bewertung des Sicherheitsniveaus einiger Mechanismen zur Vertraulichkeit, Verfügbarkeit und Pseudonymität von Transpondern (RFID). In: Hollstein, T.; Wernle, M.E.; Wissendheit, U.: 2. Workshop RFID: Intelligente Funketiketten – Chancen und Herausforderungen. Erlangen 4./5. Juli 2006 VDE/ITG Darmstadt 2006

[15] Rankl, W.; Effing, W.: Handbuch der Chipkarten: Aufbau – Funktionsweise – Einsatz von Smart-Cards, 3. Auflage, München 1999

[16] RFID Journal (ed.): TI, VeriSign Devise Drug-Protection Plan, http://www.rfidjournal.com/ article/articleview/1628/1/1/, Melville 2005

[17] RFID Productnews (ed.): Authenticated RFID-The Next Level of Protection for Pharmaceutical Product Verification, http://www.rfidproductnews.com/issues/2005.09/feature/02.php, Malvern 2005

[18] TI – Texas Instruments (ed.): Securing the Pharmaceutical Supply Chain with RFID and Public-key infrastructure (PKI) Technologies, http://www.ti.com/rfid/docs/manuals/whtPapers/wp-Securing_Pharma_Supply_Chain_w_RFID_and_PKI_final.pdf, Dallas 2005

[19] WHO Regional Office for the Western Pacific (ed.): Counterfeit Medicines: Some Frequently Asked Questions -May 2005, http://www.wpro.who.int/media_centre/fact_sheets/fs_20050506.htm, Manila 2005

[20] WHO Media centre (ed.): Counterfeit medicines, http://www.who.int/mediacentre/factsheets/fs275/en/, Washington D.C. 2006

[21] WTO (ed.): World Trade Developments in 2004 and Prospects for 2005, http://www.wto.org/english/res_e/statis_e/its2005_e/its05_general_overview_e.pdf, Geneva 2004

[22] Wallstabe, A.: Fälschungssicherheit durch den Einsatz von Radio Frequency Identification (RFID) und Public Key Infrastructures (PKI) am Beispiel von Medikamenten, Bachelor Thesis, Department of Computer Science, University of Applied Sciences Bonn-Rhein-Sieg, St. Augustin 2006

Authors Biographies:

Andreas Wallstabe is a M.Sc. in Autonoumous Systems Student at the University of Applied Sciences Bonn-Rhein-Sieg, St. Augustin, Germany, where he received his B.Sc. degree in Computer Science in 2006. He got the “Evidian-Pohl-Preis für Informationssicherheits 2006” (Award for Information Security)

E-Mail:
Andreas.Wallstabe(at)smail.inf.fh-bonn-rhein-sieg.de

Hartmut Pohl is a Professor for Information Security at the Faculty for Computer Science at the University of Applied Sciences Bonn-Rhein-Sieg, St. Augustin, Germany

E-Mail:
Hartmut.Pohl(at)fh-bonn-rhein-sieg.de