ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

University of St.Gallen

AUTO–ID LABS

Product Specific Security Features Based on RFID Technology

Zoltán Nochta, Thorsten Staake, Elgar Fleisch

Auto-ID Labs White Paper WP-BIZAPP-028

Zoltán Nochta
Project Manager
SAP AG

Thorsten Staake
Senior Researcher
University of St.Gallen

Elgar Fleisch
Research Director
Co-Chair of Auto-ID Labs
University of St.Gallen and ETH Zurich

Contact:

Institute for Technology Management
University of St. Gallen
Dufourstrasse 40 a
9000 St. Gallen
Switzerland

Phone: +41 71 224 72 47
Fax: +41 71 224 73 01

Email: Thorsten.Staake@unisg.ch
Internet: www.autoidlabs.org

Business Processes & Applications

Abstract

In today's business, there is a growing problem of product counterfeiting and piracy. Criminals have considerable expertise and resources that enable them to produce and sell counterfeits of products. The proposed solution aims at providing unique and secure authentication mechanisms of a given item, in order to distinguish between genuine products and counterfeits. As underlying technology, the approach utilizes RFID technology: Transponders hold unique and cryptographically secured data that uniquely binds a given product to a given tag, and thus makes duplication or re-application of tags difficult.

1. Introduction

Counterfeiting and piracy of products have evolved constantly with emerging trends and technology. For 2004, the International Chamber of Commerce estimated that tampered and counterfeit products account for some seven percent of world trade, which is said to amount to a market volume of 500 billion US dollars [1]. The development of trade with counterfeit goods is shown in Figure 1.

The problem is not specific for certain products or markets. Alongside the music, software and luxury goods industries, counterfeit products are increasingly finding their way into other sectors, such as pharmaceuticals, automobile spare parts or toys. Referring to the International Chamber of Commerce, "…counterfeiting and piracy are growing exponentially in terms of volume, sophistication, range of goods, and countries affected - this has significant negative economic and social impact for governments, consumers and businesses, and an international multisectoral response is required" [2].

Companies, as well as enforcement agencies, are becoming increasingly aware of the problems resulting from counterfeiting. The market for product security and brand protection technologies belongs to the fastest-growing industry sectors.

In this paper, we propose a security solution based on Radio Frequency Identification (RFID) technology, which is applicable for passive, low-cost transponders that contain item-specific information to avert cloning attacks. Moreover, the approach could be easily integrated in the emerging EPC Network. Section 2 discusses properties of existing and emerging security techniques, making shortcomings and requirements more explicit. In Section 3 the proposed solution is outlined, and Section 4 closes with concluding remarks.

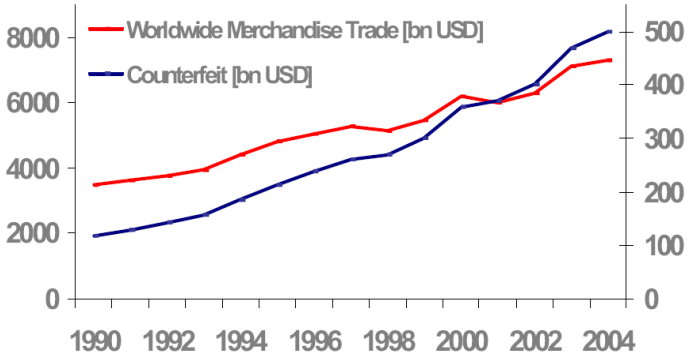

Figure 1. Development of Trade with Counterfeit Goods [3] [4] [1]

2. Existing and Emerging Security Techniques

Product security mechanisms to prevent unauthorized production most often rest on applying features to or using inherent properties of objects, with the features or properties being relatively cheap to produce for the rights holder, but are - or at least should be - unreasonably expensive to copy, to reproduce or to remove and reapply for illicit actors.

A very large number of different product authentication techniques exist, designed for various application areas, all with specific characteristics and different cost for applying and testing. A complete overview would be beyond the scope of this paper. However, selected features will be introduced in the following subsection, allowing for a comparison with upcoming techniques based on RFID technology.

2.1. Established Security Features

Established security features are often classified concerning the cost per feature, the cost per check, their visibility for external parties (overt vs. covert features), the readability (human-readable vs. machine-readable), as well as the underlying technology. Among the technologies, optical and chemical / biological techniques are frequently applied.

Optical anti-counterfeiting technologies are widely in use. Prominent examples are watermarks, micro printings and holograms. In the past, the use of holograms has been successful for a number of reasons: holograms have a strong visual appeal, and replicating them was possible only with a high investment. However, today equipment to manufacture holograms is cheap, and holograms constitute no great barrier for counterfeiters. Moreover, due to their extensive use, customers pay less attention to holograms than in the past. There

is a large range of other optical anti-counterfeiting devices, including retro-reflective materials and optically variable thin films and inks.

Biological and chemical technologies are becoming increasingly attractive as anti-counterfeiting measures, mostly due to the improved understanding of the unique characteristics of proteins, enzymes and DNA and the ability to test these characteristics. One method, for example, uses specific antibodies to detect antigens or marker chemicals. Engineers add the marker chemicals in low concentrations to products such as pharmaceuticals or liquor. Specific antibodies contained in test kits detect the markers in the original products.

Besides the type of technology used, the most important issue is to distinguish between markings of the packing and the marking of the product itself. Strictly speaking, the first solution only allows for an authentication of the package, and one can only infer the authenticity of the product. However, marking the packing most often comes with low costs for both the security feature and the product check. Therefore, package marking is frequently applied to products for which security is less relevant; examples are fast moving consumer goods or apparel. Biochemical solutions are often used to mark the product itself. Here, the application of the marker mostly comes with low costs, but the testing often is cost intense and may even require disassembling or destruction of the product. Another disadvantage of biochemical markers is that in many cases, test kits can only detect the presence of the substance but not its concentration. This enables illicit actors to use the sub-stance contained in an original product and dilute and disperse it to counterfeit goods. The use of unique product characteristics overcomes this disadvantage. However, here the cost per test is often prohibitively high, such that the solution is not applicable for low-cost goods.

However, besides the shortcomings mentioned above, a major drawback of the established techniques is their static property: Once they are applied and the product is no longer under the control of the manufacturer or rights holder, the feature cannot be changed. In this regard, the electronic protection techniques can be used to overcome this shortcoming.

2.2. Approaches Based on RFID

Microelectronics receives growing acceptance as anti-counterfeiting devices. Solutions range from identification technologies based on a simple, unique number to sophisticated digital signatures providing a very high degree of security. Devices can be implemented covertly or overtly, may or may not be accessible to the user, are nondestructive and suited for automated checks. A drawback is the high price, but experts expect less expensive devices in the near future [5].

The use of RFID as an authentication technology is discussed in various publications [6, 7, 8, 9]. Two approaches can be distinguished: The first relies on unique numbers which are used to generate inherently dynamic track & trace profile of individual goods, in order to derive a product history. The pharmaceutical industry is likely to introduce a product pedigree solution based on RFID technology due to a number of emerging laws and regulations aiming at a more secure supply with drugs. The advantage of RFID over other “number-carriers”, such

as bar codes, is the reduced time and associated cost savings due to an efficient bulk-reading capability. However, a drawback of the solution is the low resistance against cloning attacks, i.e. the duplication of transponders. Therefore, the product history must be regarded as plausibility check only.

The second approach uses cryptographic features to avert cloning attacks. The functionality – and complexity – is similar to smart cards; a good summary can be found in [10]. The solutions mostly rest on symmetric or public key challenge response authentication principles, which leads to a much larger chip size and thus to higher costs compared to "basic" RFID or Electronic Product Code (EPC) tags. Moreover, the energy consumption is much higher, and the communication between tag and reader involves larger amounts of data to be sent. For passive tags, this has serious implications on the maximum distance between tag and reader as well as on the number of tags which can be read in bulk mode.

Both solutions are very promising - the scalable level of security, the possibility to automate the verification process and thus the possibility to conduct a large number of tests as well as the dynamic property are important advantages over established security features. However, two drawbacks exist: First, the solution based on extended tags with security features comes with high fixed costs, and second, it is still the tag which is authenticated and not the product. The approach presented in the following section addresses this issue.

3. A Solution Based on Signed Product Characteristics

3.1. Adding Object Specific Data on the Tag

In Figure 2 the main components of a schematic architecture are shown. The system allows setting up a se-cure and authentic binding between a product and a passive RFID tag residing on that product. This task is done by the component called Branding Machine.

The Branding Machine is mainly responsible for computing and writing of the unique and secure Product Validation Data to the Tag. The component called Product Verifier is able to determine whether the Product Validation Data delivered by an RFID tag is authentic and thus indicates the tagged product's authenticity. The Product Verifier will have different modules, such as an RFID Reader, a Crypto Engine, and a Communication Interface.

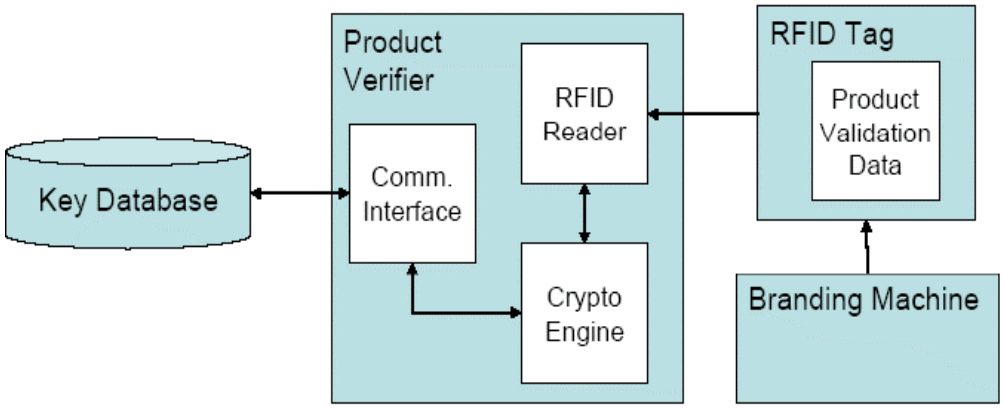

Figure 2. Architecture Overview

The RFID Reader component requests the RFID Tag for the product validation data stored on that Tag. The Crypto Engine is responsible to check the authenticity of the Product Validation Data read by the RFID Reader and also to determine whether the Product Validation Data has been altered by an impostor which would be an indicator for a faked product. The Communication Interface can be used to determine authentic cryptographic keys from the (optional) component called Key Database. The usage of the Key Database can be eliminated by storing known verification keys either on Tags or on Product Verifiers.

3.2. Specification of the Components

Product Validation Data: The Product Validation Data contains the following data sections each with different data elements:

Product Validation Data : = {

Unique Product Identifier,

Unique Tag Identifier,

Signature Method,

Signature Value,

Validation Key }

Unique Product Identifier: In this section, a bit sequence that uniquely characterizes the given product, will be stored. Typically, this information is determined by the product's vendor. Depending on the specific type of product, different physical, chemical, etc. properties that can be verified, i.e. detected or measured, by a (human or machine) observer could be

relevant. Example properties that - either altogether or in a subset - can uniquely characterize a product with a certain high probability are weight, electric resistance, geometrics, a serial number printed on the product itself or its packaging, etc. This data will typically be written on the Tag by the product's vendor before product delivery, for example during packaging. It is also possible to place a reference here, such as an URI that specifies a dataset stored on a remote database. This may help to save Tag resources, but will make product validation dependent on the availability of that external storage.

Unique Tag Identifier: The RFID Tag will store a unique read-only number in order to distinguish between RFID Tags during product validation.

Signature Method: In this section a bit sequence identifies the combination of cryptographic methods that were used by computing Signature Value. This information will be used by the Product Verifier to apply the correct cryptographic functions during product validation.

Signature Value: Signature Value will be computed preferably by the product vendor by combining a cryptographic hash function h with a public-key encryption method SPr, such that

Signature Value = SPr(h(Unique Product Identifier, Unique Tag Identifier, Signature Method,Validation Key)).

Here, SPr indicates the usage of the vendor's private key (a.k.a. signing-key) when computing Signature Value. Note that the private key must be exclusively known to the entity (e.g. product vendor) that computes Signature Value. During product validation, the corresponding public-key called Validation Key will be used to check the validity of Signature Value. Commonly known methods that can be utilized here, e.g. MD5, SHA-1, SHA-512, or Whirlpool.

Validation Key Identifier: Validation Key Identifier is a unique reference, e.g. a URI, to the authentic public-key of the entity that computed Signature Value which is stored on the given Tag. Preferably, public keys are stored in the (online) Key Database that can guarantee their authenticity. To ensure this, a trusted certification authority can be utilized that provides secure bindings between public-keys and their holders by issuing certificates. In this case, the Key Database would store such certificates. It is also possible to store the Validation Key, i.e. public-key directly on the Tag.

4. Conclusion

In this paper, we proposed an anti-counterfeiting security solution based on RFID and EPC technology, which is applicable for passive, low-cost transponders. The exceptional feature of the approach is that the tags contain verifiable, item-specific information. Thus, a tag which is applied to a product is tightly bonded to that item, providing a measure to avert cloning attacks. The solution is also adaptable for offline checks if no network connection is available. However, the applicability of the proposed solution depends very much on the availability of unique, product specific properties which are easy to observe.

References

[1] International Chamber of Commerce, the fight against piracy and counterfeiting of intellectual property, prepared by the Commission on Intellectual Property, 35th ICC World Congress, Marrakech, June 2004.

[2] International Chamber of Commerce, Current and emerging intellectual property issues for business, Sixth edition 2005, www.iccwbo.org/iproadmap, September 2005.

[3] Kommission der Europäischen Gemeinschaft, Folgemaßnahmen zum Grünbuch über die Bekämpfung von Nachahmungen und Produkt- und Dienstleistungspiraterie im Binnenmarkt, KOM(2000)789, November 2000.

[4] World Trade Organization (1986-1994) Agreement Establishing the World Trade Organization, Annex 1C, Agreement on Trade-Related Aspects of Intellectual Property Rights, www.wto.org/english/docs_e/legal_e/27-trips.pdf.

[5] S. Sarma, S. Weis, D. Engels, RFID systems and security and privacy implications, Cryptographic Hardware and Embedded Systems - CHES, August 2002.

[6] T. Staake, F. Thiesse, E. Fleisch, Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting, ACM Symposium on Applied Computing ’05, March 2005.

[7] T. Dimitriou, A Lightweight RFID Protocol to protect against Traceability and Cloning attacks, SecureComm, September 2005.

[8] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim. Mutual authentication protocol for low-cost RFID, Ecrypt Workshop, July 2005.

[9] A. Juels, Strengthening EPC Tags Against Cloning, Working Document RSA Laboratories, www.rsasecurity.com, March 2005.

[10] P. Hartel, P. Paradinas, J.Quisquater, Arithmetic Coprocessorsfor Public-key Cryptography: The State of the Art, Proc. of CARDIS’96, September 1996.