AUTO–ID LABS

Features, Identity, Tracing, and Cryptography in Product Authentication

Mikko Lehtonen, Nina Oertel, Harald Vogt

Auto-ID Labs White Paper WP-BIZAPP-040

Mikko Lehtonen
Senior Researcher
ETH Zurich

Nina Oertel
Research Associate
SAP Research

Harald Vogt
Senior Researcher
SAP Research

Contact:

Auto-ID Labs ETH Zurich/St.Gallen
Swiss Federal Institute of Technology (ETH) Zurich Department of Management, Technology and Economics
Kreuzplatz 5
8032 Zurich
Switzerland

Phone: +41 44 632 86 24
Fax: +41 44 632 10 45

E-Mail: mlehtonen@ethz.ch
Internet: www.autoidlabs.org

SAP Research, CEC Karlsruhe
E-Mail: {nina.oertel, harald.vogt}@sap.com

Business Processes & Applications

Index

Abstract

Product authentication is needed in anti-counterfeiting to distinguish genuine products from counterfeit ones. In spite of the current availability of sophisticated techniques and solution concepts for product authentication, secure authentication of different kinds of physical products remains an unsolved problem in practice. This paper presents a systematic overview of product authentication techniques. Our goal is to identify and analyze fundamental approaches for product authentication, investigate the available and emerging technologies and to evaluate them. The results are used to derive a set of decision variables, or constraints, that need to be taken into consideration when choosing which approach is most suitable to authenticate a given product.

1. Introduction

The increasing complexity and dynamics of global markets offer enormous possibilities for counterfeiting, grey marketing, and tampering of branded and high-valued goods. Basically all areas are affected by this development, including the pharmaceutical, aircraft, automobile, tools, and luxury goods industries. Besides the economic damage, often the security of consumers and patients are at risk. High profits and low risks for such wrongdoing are countered by jurisdictional, educational, and technical means. Obviously, the high demand for faked goods results in a large supply, against which these measures are mostly ineffective. However, in many cases ensuring the quality of goods is of critical importance.

In this paper, we discuss the fundamental properties of techniques for product authentication. A large number of products and services are being offered today, including widely used security marks like holograms as well as emerging authentication approaches that are based on innovative technologies such as Radio-Frequency IDentification (RFID). A classification and systematic evaluation of these authentication approaches is largely lacking. We therefore evaluate the basic principles for product security, their incarnations in certain technical implementations, and their suitability in different application areas.

2. Relation to Existing Theories and Work

Authentication is recognized as one of the general security services together with confidentiality, integrity, non-repudiation, and availability. Authentication of physical and logical entities is crucial for the security of various systems, from ATMs to e-mails, and thus well established in the domain of system and network security [8], as well as biometrics.

Authentication of physical products, however, is only scarcely addressed within the scientific community and the domain is dominated by commercial solution providers. Scientific literature in the domain of radio-frequency identification (RFID), however, does address product authentication [10], [23], but does not address general approaches. [24] describes general approaches to object authentication, claiming that authentication can be based on something an object knows, something it has, or something it is, but also on something an object does or based on where it is. [12] touches briefly on the differences between traditional authentication approaches and trace-based systems.

3. Authentication Approaches

In this section we identify and discuss distinct approaches and technologies for product authentication, based on the state of the art.

3.1. Authentication based on features

The identity of a physical object is uniquely determined by a set of distinctive properties. It may not be possible to, at any given time, conclusively determine the current “value” of such properties, which may be due to the unavailability of the right tools. As an example, consider two “identically” produced bottles of wine. With the naked eye, it may not be possible to reliably distinguish them, but it is inevitable that there are small differences between them, such as the amount of wine, the shape of the bottles, and the structure of the paper from which the labels are made. These differences can all be spotted if the right tools are available.

When a product is to be authenticated based on its natural properties, the first step is to look for common features of genuine products. We assume that an expert who knows the original product or has access to its specification can identify most fake products this way. Consumers and other non-trained persons can be offered photographs of the distinctive properties of genuine products in order to enable them to spot counterfeits. If the product passes this first test, then one can verify if it has the security features that genuine products must be equipped with, or go through laboratory tests to make the decisions more reliable. If the product does not have the required security features, it is definitely not genuine. In some rare cases, for example for some accurate imitations of brake-pads, the only way to verify their authenticity is to really use the product and see if it sustains stress as an original, or breaks because of lesser quality. This simple example shows the delicacy of product authentication: a fake item may be easy to spot, but it is hard to establish the authenticity of a genuine product conclusively. A secure way to authenticate products based on their natural properties is the so called Laser Surface Authentication (LSA). It is based on the fact that each surface has a unique pattern of how it reflects laser light. [19]. With a special laser scanning process, it is possible to measure the surface structure of an object so closely that

a unique fingerprint is captured, which can be stored in a database for the later comparison with products claiming to be genuine.

Measuring imminent features of products, however, may be too complicated (e.g. requiring line-of-sight) or may only work in certain environments. A simpler method is to add an artificial feature, which can be verified easily, to an item. Here, the problem is that artificial features are man-made, and it is generally possible to clone them. Such features include, e.g., holograms, watermarks, security threads, chemical and DNA markers, micro printing or printing with inks only visible in ultraviolet light. Products can also be authenticated by injecting microscopic taggants to them whose existence can be optically verified [16]. These features offer a secure authentication, if it is difficult for counterfeiters to equip the fake products with the same security features. The difficulty in reproducing a feature might have different reasons, among them:

- the cost for reproducing the feature or for attaching it to a product,
- no access to the material needed for imitating the feature,
- no access to the production facilities needed (e.g., for manufacturing RFID tags),
- no knowledge about the (complex) production process or the materials needed,
- no knowledge about the presence of a feature (covert and forensic features),
- intrinsically not reproducible features, i.e. features that are produced based on a random process, which can be verified but not reproduced voluntarily.

Since holograms were historically hard to copy, they were used to provide cloning resistance to products. Today, however, equipment to manufacture holograms is relatively accessible, and holograms that are used as security labels incorporate unique serial numbers (e.g., [25]) or polarize the reflected light (e.g., [13]). Another currently used technology to authenticate products is the Copy Detection Pattern (CDP) that can be printed on paper or carton package, labels or documents, and that can be verified by optical reading [2]. A CDP is hard to copy and thus protects the product from cloning.

The domain of document authentication uses very advanced methods mostly because of the security requirements of banknotes and passports. Many features of these documents themselves are used in authentication, such as the material of the paper, visible printings, the serial numbers and other data they carry. In addition, they have many hidden security features such as invisible printings, watermarks, special materials, but information about their existence is not publicly available and thus out of the scope of this work.

Also barcodes and RFID labels can serve as security features. They can be quickly scanned, even without line of sight, and they return a unique number (identifier) that correspond the identity of the product where the feature is attached to. The identifier can be easily mapped to a database where all objects are registered, thus offering additional possibilities to authenticate a product besides the mere presence of the feature. These methods will be described in the next two subsections.

3.2. Tracing

Products can be authenticated based on tracing information [18] and product pedigree [26] that allow a plausibility check. These systems gather and verify knowledge about the locations of the original products. In case of the pedigree, also information about the sender and receiver of an item are known and can be verified. An important prerequisite of these approaches is to have unique identifiers on each product, which can be achieved by putting an RFID tag on it, or by printing a 2D barcode or an alphanumeric code on the product.

Tracing can be used in the following way to establish the authenticity of an item. Note that there is always a background system involved, which keeps records about the whereabouts of an item.

- As a rudimentary authentication, the system can verify whether the identifier an object claims to have was indeed issued at manufacturing time. In order for this check to be useful, the following two conditions must be met to minimize successful number guessing by counterfeiters: the unique identifiers must be assigned randomly, and the number of potential identifiers must be significantly larger than the number of identifiers issued.
- If the supposed location of the item is known in the background system, the actual location can be verified against the supposed one. This will also contribute to detection of grey marketing activities.
- If the history of the item is known, i.e. where it has been in the past, at what time and in which transactions it was involved, this history can be checked against valid traces. Only if the history is plausible the item will be accepted as genuine.

Duplicated tags may often be detected by the background system, given that the information of the movement of individual items is made centrally available. The latter two abovementioned plausibility checks can detect duplicated tags in certain scenarios. Automated detection of cloned tags in a RFID-enabled access control application using intrusion detection mechanisms has been addressed in [17]. This approach presents the state-of-the-art in cloned RFID tag detection and it is based on detection of statistical anomalies vis-à-vis the established normal behavior profile. However, it suffers from a relatively high rate of false positives making it infeasible for many real world applications.

In tracing based authentication it is crucial that the association between an item and a serial number is established in a secure way. Otherwise, the result of the authentication process would provide no information at all about the item under consideration. How this binding between identifier and product can be achieved is described in Section 4.

3.3. Cryptographic support

A secret key embedded within an RFID tag can serve as an authenticating feature. Of course, the key must be protected against unauthorized access, such as side-channel attacks. Cryptographic functionality should only be accessible through a well-defined

interface, which typically offers entity authentication features through a challenge-response protocol. But it is usually not possible to directly access the key value, not even after successful user authentication to the tag. A recent example is new electronic passports, which use RFID tags for authentication [6]. Such passports are also a good example of security and privacy issues being raised by the widespread use of RFID [7].

Several protocols have been designed for authenticating RFID tags; a survey can be found in [10]. The general property of these protocols is that a reader device verifies if a tag knows a certain secret key. The secret key is never transmitted in clear text over the radio-frequency interface which can be eavesdropped. Knowledge of the key is typically verified through a challenge-response protocol. Such a protocol may be based on (i) public-key cryptography. Due to advances in elliptic curve cryptography (ECC), public-key cryptography is becoming more and more feasible in serialized RFID tags. ECC allows for less computationally intense encryption for resource-limited devices, and it is expected to have an important role in securing mobile internet devices [29]. To illustrate the effect of this increased computational efficiency, ECC has enabled implementing the world's smallest SSL Web Server in shape and size of a quarter dollar coin [30]. Wokenstorfer [28] has shown that ECC could be implemented by respecting the strict power and area constraints of RFID tags. Batina et al. [1] show how secure identification protocols based on elliptic curves are implemented on a constrained device such as an RFID-Tag requiring between 8500 and 14000 gates, depending on the implementation characteristics. Tuyls et al. [27] claim that at least the complexity of 12,000 logic gates is required for implementing these approaches, which is a significant overhead even for high-end tags. Also, (ii) a hash-function may be used to authenticate RFID tags [4]. This approach has lower resource requirements than public-key encryption. Alternatively, (iii) symmetric-key encryption seems to be viable for RFID, as demonstrated by [5], which presented an AES implementation with approximately 3,400 gates. The disadvantage of symmetric-key versus public-key cryptography is more sensitive key management. Most of these approaches are, however, still not feasible for low-cost, high-volume RFID tags due to cost and size constraints, and the increased reading time.

Another way to implement a secret key on the RFID tag is to use a Physical Unclonable Function (PUF). The PUF is a one way function that allows for the calculation of unique responses using only some hundreds of logical gates without any costly cryptographic primitives [20]. In order to make the use of eavesdropped responses infeasible, several challenge-response pairs should be stored in a database. A model of PUF in transponder authentication is presented in Fig. 1. One possible candidate for a PUF is proposed in [9] where the idea is to exploit the statistical delay variations of wires and transistors across integrated circuits (ICs) to implement unique secret key on each tag. The evaluation in [9] indicates that there exists significant delay variation of wires and transistors across ICs implementing this circuit, and that the idea of leveraging this variation to uniquely identify and authenticate an IC seems promising. However, there are open issues that should be addressed for PUFs to be deployed in real applications.

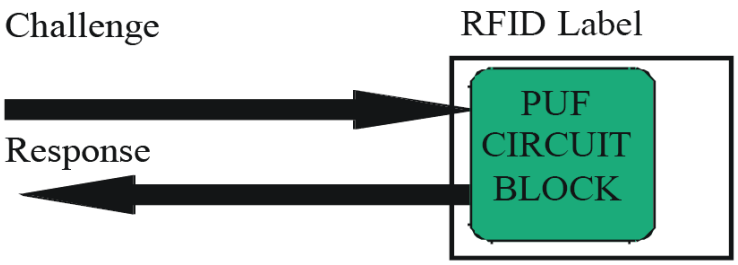

Fig 1. A model of a PUF based Class I / Class II RFID label [20].

Regardless of the exact implementation of the tag authentication protocol, one major challenge with RFID tags is that the tag itself is authenticated and not the product. Therefore, as in the case of product tracing, a strong binding between the tag and the product has to be established.

4. Complementary Concepts

As outlined above, plain authentication of the security feature is sometimes not sufficient for secure product authentication. Authentication has to be complemented by additional safeguards, so that the authentication methods cannot be tricked or circumvented easily. For example, it is useless to employ copy protected RFID tags if they can be ripped off and reused on other (counterfeit) products easily. Therefore, we will briefly discuss three complementary concepts to product authentication:

- Methods for ensuring the binding between product and identifier
- Methods for preventing the copying of identifiers
- Sealing of packages to prevent product tampering

The binding (inseparability) between a tag and a product can be achieved either based on mechanical principles or it can be ensured virtually by personalizing the tag. One proposed approach to bind the tag to the paper document it authenticates is to make use of optical memory device that is integrated on the document [11].Mechanical binding includes the use of RFID tags that lose their functionality if they are ripped off a product. This principle can be applied for example in spray perfume bottles where the tag resides between the bottle top and the glass bottle. Removing the bottle top detaches a wire from the tag's antenna, disabling the tag [22]. RFID tags can also be integrated inside solid metal objects such as rings. In this case, using optimized protocol, optimized reader signal processing, and magnetic induction in 125 kHz (LF) band, a reading (and writing) distance of about 1 cm can be achieved, from which about 1 mm through metal [22]. Using similar techniques, RFID tags can also be integrated in blister packages that are commonly used for example in pharmaceutical industry. A tag residing between two aluminium foils inside the blister can be read from up to about 5 cm distance, from a stack of blisters [22]. Integration of RFID tags inside the electronic passports also presents secure tag-product bindings.

The personalization of tags requires that product-specific information is stored on the tag [14]. This information should be as unique to the item as possible. One possible choice would be the LSA fingerprint described above in subsection 3.1. By comparing the measured property of the product to be checked to the data stored on the tag, it can be verified whether the tag belongs indeed to the product. Note that not only RFID tags are able to store this product specific data, but also 2D barcodes and similar optical identifiers can store additional object information.

How it can be ensured that identifiers are not copied depends on the type of tag used. In the case of RFID tags, cryptographic approaches are well suited to prevent copying. In the case of visual identifiers like barcodes, it is possible to superimpose the line pattern with a CDP, thus rendering the barcode hard to clone. Alphanumeric identifiers and barcodes can also be combined with traditional security features like holograms to protect them against copying. This combination approach is also demonstrated by [25].

Anti-tampering measures have to be considered if the tag is not applied directly to the product, but to its packaging. In this case, binding mechanisms will only ensure that the tag stays with the packaging, but it must furthermore be ensured that the product stays with the packaging. Therefore, the packaging must be sealed appropriately. Mechanical seals are one option, but RFID tags and sensor networks can also be employed for this purpose. For example, RFID is used in electronic seals to guarantee the integrity of containers in transatlantic traffic [21]. RFID tags are also useful by providing immediate notification, e.g. [3], or by recording the tampering event (e.g. by rendering the tag unreadable [15]).

5. Findings

We have identified four fundamental approaches to product authentication:

- Authentication based on properties that are inherent to the product itself, such as a unique design, weight, or certain materials. True uniqueness is often only determined if the inspection procedure captures highly precise details, such as the optically captured, random alignment of paper fabric, or surface details measured by a laser scanner. Such details provide identity for an object.
- Authentication based on security features that are incorporated into a product, for example by the application of an invisible ink or a security tag.
- Historical data about an object provides valuable information about its origin, former use, and operation and storage conditions. Besides its usefulness for product authentication, such tracing information is a precondition for making sound decisions about the future application of an object.
- Cryptography is a commonly used tool for the remote authentication of entities. The same principle can be useful for product authentication. A prerequisite is the presence of a computational unit, which can perform cryptographic operations, and the protection of the

secret key against unauthorized use. This approach is conceptually similar to incorporation of security features but very different in the way it's implemented.

Every authentication process, including human-to-human authentication, relies on the observation of effects that are caused by certain properties. The apparatus that actually performs the observational process could, in principle, be fooled by a clever adversary. In order to provide high level of security, the threshold for such activities must be set sufficiently high so that they become unattractive. There is a compromise involved between the cost for the verification apparatus and process, and the cost for faking the authenticity of a product.

Based on this study, it is too early to conclude which approaches are the most suitable for which kinds of products. To assess which technology or approach to choose for a given product, the following main constraints need to be taken into consideration:

- Intended use-case for product authentication: Depending on who is to authenticate the products and what is the environment, there are different constraints regarding the time and effort for the check, required equipment, and expertise. Therefore different techniques and approaches are needed for, e.g., private investigators, customs officers, warehouse employees, sales clerks, and consumers.
- Desired level of security: There is no such thing as perfect security and therefore, in theory, all product authentication approaches can be broken. The level of security of an approach is defined by the amount of effort needed to break or bypass it. For unprotected products, all product authentication techniques present a substantial increase in the level of protection, but in the long term the level of security needs to match the value of the product it protects.
- Cost of the solution: In anti-counterfeiting, the cost to protect a product is often a critical factor when choosing a product authentication technology and it should not exceed the expected benefits. Today there are no formal ways to estimate the benefits of different product authentication approaches in order to enable a cost-benefit analysis that could justify the cost of a solution.
- Physical constraints of the product: None of the techniques might be feasible due to physical constraints of the product. Finding natural features that are suitable for authentication is very challenging for example for pharmaceutical products. Some products like certain luxury goods require invisible integration of the security feature, making clearly visible security features infeasible. Also the environmental constraints due to the product's life-cycle, such as robustness to extreme temperatures and lifetime of the security feature, need to be taken into account.

The formulation of guidelines for choosing suitable product authentication approaches for different products while taking into account the main constraints that are outlined above is subject to future work.

6. Conclusions

In this paper, we have presented an overview of existing ways to authenticate products. The number of available techniques is high and the authentication process can be based on various things. Mitigating the cloning attack is often the first priority in most approaches, but it is equally important to provide a binding between the security feature and the product. Current ways to authenticate products require expertise, specialized equipment, or even both. Furthermore, some product authentication approaches require access to information that companies are not willing to share, such as the trace of a product or the existence of hidden security features. Product authentication is therefore currently rather inaccessible to ordinary consumers, even though their involvement could be of great benefit in anti-counterfeiting.

Acknowledgement

This work has been partly funded by the European Commission through IST Project SToP: Stop Tampering of Products (Ref. IST- 034144). The authors wish to acknowledge the Commission, Eric Gout, and Thomas Kelepouris for their support and comments.

References

[1] Batina, L.; Guajardo, J.; Kerins, T.; Mentens, N.; Tuyls, P.; Verbauwhede, I.: An Elliptic Curve Processor Suitable For RFID-Tags. Cryptology ePrint Archive, Report 2006/227. http://eprint.iacr.org/, 2006.

[2] Busch, C.; Schmucker, M.; Vorbrüggen, J.: Product and Brand Protection. In CG Topics 1/2004. Available at http://www.inigraphics.net/press/topics/2004/issue1/1_04a11.pdf (31.1.2007).

[3] Collins, J.: African Beef Gets Tracked. RFID Journal, 10 December 2004.

[4] Engberg, S.; Harning, M.; Damsgaard-Jensen, C.: Zero-knowledge device authentication: Privacy & security enhanced RFID preserving business value and consumer convenience. In Conference on Privacy, Security and Trust – PST, New Brunswick, Canada, October 2004.

[5] Feldhofer, M.; Aigner, M.; Dominikus, S.: An Application of RFID Tags using Secure Symmetric Authentication. In Proceedings of 1st International Workshop on Privacy and Trust in Pervasive and Ubiquitous Computing - SecPerU 2005, in conjunction with IEEE ICPS'2005, pp. 43–49, ISBN 960-531-179-8, Santorini Island, Greece, July 14, 2005.

[6] ICAO: PKI for Machine Readable Travel Documents offering ICC Read-Only Access. Technical Report, version 1.1, October 2004.

[7] Juels, A.; Molnar, D.; Wagner, D.: Security and Privacy Issues in E-passports. In Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm, Athens, Greece, September 2005. IEEE.

[8] Kurose, F.; Ross, K.: Security in Computer Networks, p. 620, 2003.

[9] Lee, J.; Lim, D.; Gassend, B.; Suh, G.E.; Dijk, M.; Devadas, S. :A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications. In Symposium on VLSI circuits, 2004, pp 176—179.

[10] Lehtonen, M.,;Staake, T.; Michahelles, F.; Fleisch, E.: From Identification to Authentication – A Review of RFID Product Authentication Techniques. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006. (a)

[11] Lehtonen, M.,;Staake, T.; Michahelles, F.; Fleisch, E.: Strengthening the Security of Machine Readable Documents by Combining RFID and Optical Memory Devices. In Conference on Ambient Intelligence Developments - AmI.D, Sophia-Antipolis, France, September 2006. (b)

[12] Lei, P. Claret-Tournier, F. Chatwin, C. and Young, R.: A Secure Mobile Track and Trace System for Anti-counterfeiting. In Proceedings of the 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service, 2005.

[13] NHK Spring Co. Ltd.: Security Technologies & Solutions. http://www.nhkspg.co.jp/eng/prod/info_01.html, 2007

[14] Nochta, Z.; Staake, T., Fleisch, E.: Product Specific Security Features Based on RFID Technology. Proceedings of the International Symposium on Applications and the Internet, Workshops. IEEE Computer Society, 2006.

[15] O'Connor, M. C.: Packaging Maker Offering Tamper-Evident RFID Film. RFID Journal, 2007.

[16] Microtrace: Microtaggant, http://www.microtracesolutions.com/taggant.htm, 2007.

[17] Mirowski , L .: Detecting Clone Radio Frequency Identification Tags. Bachelor's Thesis, School of Computing, University of Tasmania, November 2006.

[18] PackAgent: http://www.packagent.com/, 2007.

[19] Protexxion: http://www.bayertechnology.com/eng/press/79_6540.php, 2007.

[20] Ranasinghe, D.; Engels, D.; Cole, P.: Security and privacy: Modest proposals for low-cost RFID systems. Presentation at the Auto-ID Labs Research Workshop, Zurich, Switzerland, September 2004.

[21] RFID Journal: E-Seals Smooth Border Crossings. News Aticle, September 3, 2002. http://www.rfidjournal.com/article/articleview/62/1/1/ (12.6.2006).

[22] SpaceCode: Private communication, 2007.

[23] Staake, T.; Thiesse, F.; Fleisch, E.: Extending the EPC Network - The Potential of RFID in Anti-Counterfeiting. In Proceedings of the 2005 ACM symposium on Applied computing (pp. 1607 - 1612). New York (NY): ACM Press.

[24] Stajano, F.:Security for Ubiquitous Computing, John Wiley & Sons, 2003.

[25] Tesa: Holospot http://www.tesa-scribos.com/security-technologies/tesa-holospot.htm, 2007.

[26] Texas Instruments and VeriSign Inc.: Securing the pharmaceutical supply chain with RFID and public-key infrastructure technologies. Whitepaper, 2005. http://www.ti.com/rfid/docs/manuals/whtPapers/wp-Securing_Pharma_Supply_Chain_w_RFID_and_PKI_final.pdf (1.4.2006).

[27] Tuyls, P.; Batina, L.: RFID-tags for Anti-Counterfeiting. In D. Pointcheval, editor, In Topics in Cryptology - CT-RSA - The Cryptographers' Track at the RSA Conference, number 115-131 in lecture Notes in Computer Science, page 3860, San Jose, USA, February 13-17 2006. Springer Verlag.

[28] Wokenstorfer J.: Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags?, Workshop on RFID and Lightweight Crypto, July 14-15th, 2005. IAIK, Graz University of Technology, Graz, Austria.

[29] Sun: Elliptic Curve Cryptography: The Next Generation of Internet Security. Whitepaper. http://research.sun.com/projects/crypto/ECC-Whitepaper.pdf (17.8.2007)

[30] Morgan, T. P.: Sun Creates World's Smallest SSL Web Server. Computerwire, news article 14 January 2005. http://www.computerwire.com/industries/research/?pid=C55355B9-B6CD-42EC-80BC-ACFDA6F2CDD3 (17.8.2007)