Synchronized Secrets Approach for RFID-enabled Anti-Counterfeiting

A. Ilic, M. Lehtonen, F. Michahelles, E. Fleisch

ETH Zurich, Information Management, CH-8092 Zurich, Switzerland
{ailic,mlehtonen,fmichahelles,efleisch}@ethz.ch

Abstract. In today's global marketplace, brand owners need techniques for guaranteeing the authenticity of their products. By linking physical products with digital identities through RFID, secure and automatic authentication checks can be used to prevent counterfeit products from entering the licit distribution channel. However, cryptographic RFID tags seem still too expensive to be used on a broad scale. In this demo, we want to show how standard low-cost RFID tags can be used for anti-counterfeiting in a non-conventional but efficient way. We use a method that detects desynchronization when cloned tags are introduced in a protected channel and thus helps to prevent the further distribution of the counterfeit products.

Keywords: anti-counterfeiting, RFID, clone detection, synchronized secrets

1 Introduction: The Challenge of Anti-Counterfeiting

Product counterfeiting is an ever increasing problem that affects trademark and brand owners, governments, as well as consumers [1]. Though some aspects of the problem are often considered relatively harmless by the public, such as purchasing of fake designer handbags from street vendors, the intellectual property rights and investments of licit businesses must be protected. Furthermore, in more dangerous forms of product counterfeiting, the fake products are injected into the licit distribution channel and sold as genuine articles [2]. While potentially risking the health and safety of consumers, in this way the counterfeiters can sell their articles in higher price for higher profits. As a result, the licit supply chains need to be protected from counterfeit products. The emerging electronic pedigree in the pharmaceutical industry (e.g. [3]) is a prominent example of measures towards this objective.

Radio-frequency identification (RFID) is an emerging Automatic Identification technology. RFID systems comprise tags that are attached to products, interrogators that read and write data on tags, and back-end systems that store and share data. RFID has recognized potential in anti-counterfeiting [4]. Probably the most common approach to authenticate an RFID-tagged product is to cryptographically authenticate the transponder. However, cryptographic tags have cost and performance disadvantages due to their additional hardware and processing time requirements. In addition, cryptographic RFID tags remain computationally limited and are vulnerable to different tag cloning attacks, such as, cryptanalysis and reverse-engineering [5] and side-channel attacks [6]. As a result, cryptographic tags do not seem to deliver best possible trade-offs between cost, security, and performance today.

In our approach, we do not attempt to prevent tag cloning but instead we try to detect the cloned tags. Our approach is less expensive than cryptographic tag authentication in terms of tag price and tag processing time, and it provides a high level of security where the genuine products are repeatedly read in a high rate. The limitation of our approach is that in certain conditions the system will trigger a false alarm for the genuine product and thus another level of inspection is needed to ascertain the product's origins. However, we make use of the fact that RFID tags will be deployed anyway and our approach can be implemented with minimal hardware overhead that is some bytes of rewritable memory.

2 Demo

Our application scenario is the following: A manufacturer of pharmaceutical products inserts tags to individual articles at the manufacturing site. These products are distributed through multiple steps to a hospital or a pharmacy and they are authenticated throughout the supply chain to detect counterfeit products (cf. Fig. 1).

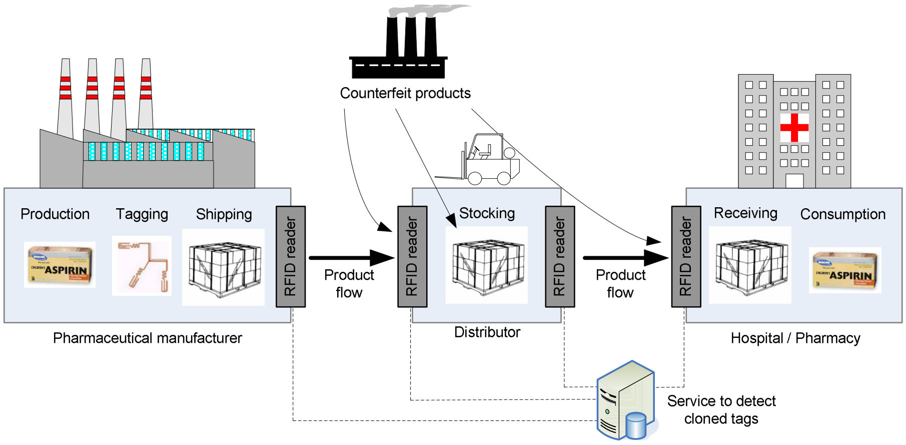


Fig. 1. Simplified view of an RFID-enabled pharmaceutical supply chain

In our demo scenario we relate to the practical context of the EU-funded project BRIDGE and show a part of an actual pharmaceutical supply chain. In this demo, the IoT conference visitors will see two Supply Chain Stations representing a pharmaceutical wholesaler and a retailer. As a Supply Chain Station we refer to the combination of a computer running the clone detection client, and an attached RFID reader (cf. Fig. 2). In addition, we set up a Supply Chain Station representing a malicious supplier that is able to clone tags and affix them to counterfeit products that are injected in the previously described two-stage supply chain.

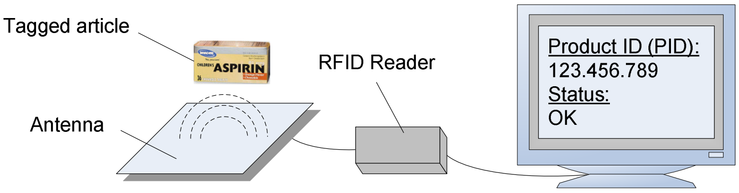
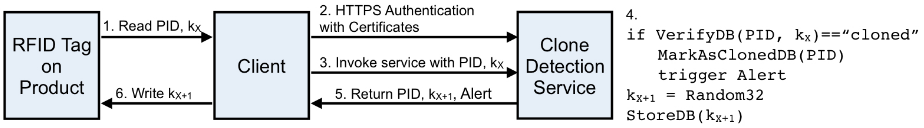


Fig. 2. Illustration of the hardware set-up of one Supply Chain Station

3 System

Our system bases on a web service for clone detection through synchronized secrets (e.g. [8]). We assume that all genuine articles are equipped with an RFID tag, which is checked at least once at every stage of the supply chain. A counterfeiter is therefore forced to equip also fake products with RFID tags. Following the Service-oriented Architecture paradigm, our solution provides a service to verify and update the synchronized secrets of tags. The same secret k_X is stored on both the tag's memory and the backend database. On every web service invocation, a new random secret k_{X+1} is generated and updated in both, the backend database and the tag's memory. If a genuine tag's identifier (PID) and synchronized secret are copied to a fake tag which is affixed to a counterfeit article, and the counterfeit article is injected into the supply chain, the backend will detect a desynchronization, i.e. a tag with invalid secret, as soon as both the genuine and counterfeit article are read. The backend service triggers an alarm upon desynchronization and a further verification, based on other authentication techniques, can be conducted to ascertain which article is the cloned one. A sequential illustration of the clone detection protocol flow, with pseudo code for the most relevant backend steps, is depicted on Fig. 3.


RFID Tag on Product
1. Read PID, k_X
6. Write k_{X+1}
Client
2. HTTPS Authentication with Certificates
3. Invoke service with PID, k_X
5. Return PID, k_{X+1}, Alert
Clone Detection Service

```
4.
if VerifyDB(PID, $k_X$)==“cloned”
    MarkAsClonedDB(PID)
    trigger Alert
$k_{X+1}$ = Random32
StoreDB($k_{X+1}$)
```

Fig. 3. Illustration of the clone detection protocol flow with pseudo code in the backend

The backend web service is implemented in PHP using a relational MySQL database to keep track of the synchronized secrets. The communication interface bases on XML_RPC and uses https as an encrypted transportation protocol. To demonstrate the clone-detection in practice, we implemented a user interface in Java that represents an organization's software that invokes the back end web service. To communicate with RFID readers and RFID tags, the client uses the open source EPC Network implementation Accada [7]. Each time a tag is read (by an RFID reader), the client invokes the web service's clone detection method, which verifies the synchronized secret through a lookup in the backend database. If clones are detected the user receives a visual alert together with the information about the other suspicious products and their last reading locations (if known). Also, as it is not safe to say whether the product with the desynchronized secret is the fake one, the database marks the product ID number as "cloned". Next time a product with marked ID number is read, the user will receive automatically a warning that the product might be subject to counterfeiting.

4 Conclusions

Our demo presents a simple but effective method for detecting cloned RFID tags in an anti-counterfeiting application. In contrast to cryptographic RFID tags, our approach is more cost-effective as it can be deployed with low-cost tags. Our clone detection protocol bases on a desynchronization detection mechanism that triggers an alert when a cloned product is injected into the licit supply chain. The limitation of the presented approach is that it alone cannot prove which of the suspicious products is the counterfeit one and which is the genuine one. We demonstrate, however, that in practice already the awareness of counterfeits and the knowledge about their most recent locations can be used to effectively deter counterfeiting.

Acknowledgements. This work is partly funded by the European Commission within the Sixth Framework Programme (2002-2006) projects BRIDGE (Building Radio frequency IDentification solutions for the Global Environment), IP Nr. IST-FP6-033546, and SToP (Stop Tampering of Products), Nr. IST-FP6-034144.

References

1. Organization for Economic Co-operation and Development (OECD): The Economic Impact of Counterfeiting. (1998)
2. Lehtonen, M., Al-Kassab, J., Graf von Reischach, F., Kasten, O., and Michahelles, F.: Problem-Analysis Report on Counterfeiting and Illicit Trade. Deliverable D5.1 of EU-BRIDGE Project, July 2007.
3. EPCglobal Inc.: Pedigree Ratified Standard. Version 1.0, January 5th, 2007. Available: http://www.epcglobalinc.org/standards/pedigree/pedigree_1_0-standard-20070105.pdf
4. U.S. Food and Drug Administration (FDA): Combating Counterfeit Drugs. February 2004. Available: http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html
5. Bono, S., Green, M., Stubblefield, A., Juels, A., Rubin, A., Szydlo, M.: Security analysis of a cryptographically enabled RFID device. 14th USENIX Security Symposium (2005).
6. RFIDJournal: EPC Tags Subject to Phone Attacks. News Article, February 24, 2006. Available: http://www.rfidjournal.com/article/articleview/2167/1/1/
7. Floerkemeier, C., Roduner, C., and Lampe, M.: RFID Application Development With the Accada Middleware Platform. IEEE Systems Journal, Volume 1, Issue 2 (2007)
8. Ilic, A., Michahelles, F., and Fleisch. The Dual Ownership Model: Using Organizational Relationships for Access Control in Safety Supply Chains. IEEE International Symposium on Ubisafe Computing (UbiSafe-07), Niagara Falls, Ontario, Canada (2007)