A Framework for Assessing RFID System Security and Privacy Risks

This framework for evaluating security and privacy risks in RFID systems focuses on key application domains, assessing risk levels for each on the basis of RFID-specific criteria.

Paweł Rotter
Joint Research Centre of the European Commission

Radio Frequency Identification systems use radio waves sent between tags and readers to automatically identify physical objects.[1] Passive tags, which have no battery and simply use the energy of a reader's emitted radio waves, are so small as to be almost invisible: tags that are 0.4 × 0.4 millimeter are currently on the market. RFID is becoming quite popular in logistics and the supply chain,[2] where vendors use it as a kind of improved bar code. Unlike printed bar codes, for example, RFID tags don't require line-of-sight readings. RFID also enables multiple scanning—readers can scan an entire truckload or shopping basket at once, which allows for further automation in many industry processes. Also, bar codes replicate only an ID number, while RFID tags can contain other information, such as product details. When combined with sensors, RFID tags can store the history of storing conditions, mechanical shocks, and so on. Increasingly, developers are commercializing RFID technology beyond logistics and the supply chain, offering applications for various domains, including medicine and agriculture.[3,4] They're also using RFID in applications that can identify people (e-passports) and in access-control systems.

Clearly, RFID is a powerful technology with numerous application possibilities. It's also a technology that raises serious privacy and security risks. Several RFID features make it particularly vulnerable among information systems, including

- the wireless transmission between the tag and reader;
- the tag's low computational power, which is often insufficient for strong security measures; and
- the tag's small size, which means that people can carry one without their consent or even knowledge.

Here, I offer an overview of the main RFID privacy and security threats and countermeasures, focusing on those that are exclusive to this technology. I then propose a framework for evaluating domain risks using three criteria: the system's deployment range, the link between the RFID tag and identity-related data, and the domain's security demands.

Threats to RFID systems

Like all information systems, RFID-based

Published by the IEEE CS ■ 1536-1268/08/$25.00 © 2008 IEEE

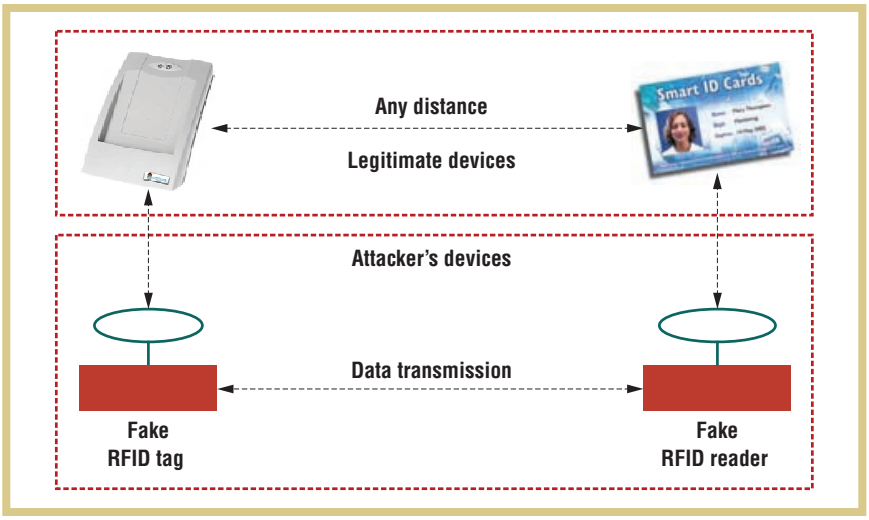

Figure 1. Relay-attack scheme. Attackers establish a communications channel between the reader and tag and thereby authenticate themselves in the target system.

systems are subject to generic attacks that threaten system security and user privacy. However, there are also many attacks that specifically target RFID system technologies.

Eavesdropping

In eavesdropping, hackers secretly monitor data sent from an RFID tag to a reader, or vice versa, via the air interface (the communication channel between the reader and tag). Because eavesdropping is passive—that is, the attacker doesn't emit any signal—it's highly difficult to detect. The most common countermeasures are to encrypt the data (so eavesdropping hackers can't understand the signal) and to use a metal screen to shield the tag and reader during information exchange (such as at border checkpoints). It's also important to limit the distance between the tag and reader by using the standard with the smallest communication range sufficient for a given application. However, developers must also bear in mind that, using a nonstandard reader, hackers can extend a standard communication range several times.[5]

Relay attacks

As figure 1 shows, in a relay attack, attackers create a connection between a legitimate reader and a victim's legitimate tag.[5] From the RFID system's viewpoint, the communication looks as if the legitimate tag and the reader are close to each other, when in fact they're communicating through the (usually wireless) communication channel that the attackers have established. Attackers can thereby authenticate themselves in access-control or payment systems. Researchers have proven that it's possible to successfully execute a relay attack against an ISO-14443A-compliant RFID system.[6]

Because attackers only transmit information—without needing to understand it—the authentication protocol (such as challenge-response) doesn't protect against this kind of attack. Developers can counter this threat—and the following four—by using short-range tags and by shielding the tags (such as keeping them in bags made of aluminum foil) while not in use. There's also a specific relay-attack countermeasure, the distance bounding protocol,[7] which uses response time to estimate the distance between the reader and tag.

Unauthorized tag reading

Attackers can use a fake reader to read tag information. They can extend a fake reader's range by several times that of the standard communication distance.[5,8] Moreover, it's relatively cheap to build an extended range reader.

A specific countermeasure against unauthorized tag reading is reader authentication. Another is initialization of transmission after the user activates the tag (by pressing a button, for example), so the possibility of unauthorized reading is limited to moments when the user demands a legitimate communication. Developers can also reduce risk by moving sensitive information to a protected database in the system's back end, as in VeriMed (see www.verimedinfo.com), a medical information system. Developers can address concerns about the unauthorized reading of a shopping bag's RFID-tagged contents using the "kill" command, which permanently disables the tag (and is obligatory in standard EPCGlobal Class 2). Researchers have also proposed a tag designed to let users physically destroy it.[9]

Tag cloning

In tag cloning, attackers make a duplicate RFID tag, which might either be quite similar in size or much larger than the original but have the same functionality. Attackers can use duplicates to access a restricted area, abuse private data, or make an electronic transaction on the victim's behalf.

Tag authentication prevents cloning; if developers use a challenge-response protocol, the information that attackers can obtain through the air interface (such as by eavesdropping) is insufficient to duplicate the tag. Also, developers can apply appropriate measures at the circuit manufacturing stage to protect tags from duplication by reverse engineering.

People tracking

In people tracking, attackers follow tag carriers' movements using various techniques, including placing fake readers in doors or deploying eavesdropping devices near legitimate readers.

Several countermeasures that I've already discussed also work with track-

TABLE 1
Threats and their relationship to vulnerabilities in RFID systems components.

	Tag	Air interface	Reader	Network	Back end
Eavesdropping	•	•		•	
Relay attack		•			
Unauthorized tag reading	•	•	•		
Tag cloning	•	•			
People tracking	•	•			
Replay attack	•	•			
Tag content changes	•				
Malware	•		•		•
RFID system breakdown				•	•
Tag destruction	•				
Blocking		•			
Jamming		•			
Back-end attacks				•	•

ing, including using low-range tags or shielding tags, authenticating readers, and disabling tags when they're not in use. In the future, however, people will carry many RFID tags, so it might be highly useful to develop a personal device to control access to them, possibly integrated into mobile phones or PDAs.[10] Developers can implement other countermeasures at the tag-design stage, including pseudonyms (changing identifiers) or tag-reader distance estimators based on the signal-to-noise ratio.[11]

Replay attacks

In replay attacks, attackers abuse authorized tag carriers' identities by repeating their authentication sequences. To do this, attackers might use a clone of a legitimate tag or resend the eavesdropped signal from a PC equipped with an appropriate card and antenna.

To perform replay attacks, attackers must obtain information sent by the tag during normal communication. Here, countering eavesdropping and unauthorized tag reading offers a first line of defense. A specific replay-attack countermeasure is to authenticate tags using, for example, the challenge-response protocol. In this case, the tag calculates its authentication code based on the challenge the reader sends. In a well-designed protocol, attackers can't deduce the key required to calculate a response from information exchanged through the air interface.

Tag content changes

If a tag is writeable, attackers can change its content, distorting item attributes or leading the access-control system to falsely reject an authorized person. Furthermore, they can insert malware—such as modified tag data that the reader interprets as a command—into writeable tags using, for example, SQL injection.[12]

In some writeable tags, developers can protect memory content by temporarily or permanently disabling writing capability (using, for example, the standard EPCGlobal Class 2 Gen 2 tag's "lock" and "permalock" functions). Also, developers can implement the readers so as to prevent them from interpreting a tag's data as a command.

Physical tag destruction

The easiest and cheapest way to disrupt RFID systems is to physically destroy the tags—heat them in a microwave, hit them with a hammer, and so on. This issue is especially relevant for applications that use RFID tags not just for identification purposes, but also to protect items against theft. Also, people concerned with privacy might destroy the RFID tags in their e-passports, which are still valid even if the RFID tag doesn't work.[13]

Blocking and jamming

Attackers perform a blocking attack using a blocker tag, which simulates the existence of numerous tags and thus causes a denial of service as the reader endlessly interrogates the nonexistent tags. However, blocking can be useful—as originally proposed, it serves to protect consumer privacy.[14] In jamming, attackers paralyze RFID system communications by generating a radio noise at the same frequency as that of the system. Blocker tags and jamming devices are easy to detect and localize, and developers can even implement appropriate warning functionalities into the system.

Overall threat analysis

Table 1 summarizes the threats and indicates the system component involved in the attack. As the table shows, few threats are related to the back end or the network; such threats are more typical for information systems in general. (For an

TABLE 2
RFID system threats and their potential consequences.

Threat \ Consequence	Relay attack*	Tag cloning*	Tracking*	Replay attack*	Tag content changes	RFID system breakdown	Back-end attacks	Malware*	Unauthorized access to secret/private data	Spoofing access-control systems	Material damages	Theft of goods
Eavesdropping		×	•	•					×	•	•	•
Relay attack										×	×	×
Unauthorized tag reading	×	×	×	•	•				×	•	•	•
Tag cloning				×						×	•	•
Tracking									×			
Replay attack									×	×	•	•
Tag content changes						•	•	×	•	×	×	×
RFID system breakdown										×	×	×
Malware					×	×	×			•	×	×
Blocking						×				•	×	×
Physical tag destruction											×	×
Jamming						×				•	×	×
Back-end attacks					•	×		×	×	×	×	×

An "×" indicates direct relationship between the threat and its consequence; "•" indicates an indirect relationship. An "*" indicates consequences that are also threats.

overview of risks and countermeasures for back-end attacks, see the overview by Susan Hansche and colleagues.[15]) Most threats exploit vulnerabilities of the air interface and the tag and are therefore specific to RFID systems.

Table 2 presents the threats' potential consequences. Most of the consequences (those marked with an asterisk) also occur as threats and might negatively impact the system even if they're not perceived as a problem. For example, eavesdropping might enable tag cloning, which could then result in a replay attack; the final consequence could be unauthorized access to a restricted area. As these relations imply, a single system vulnerability can threaten security and privacy in areas that are only indirectly related.

Framework for evaluating risks

Figure 2 shows the privacy and security taxonomy of RFID applications. I evaluate risks on the basis of three criteria: system deployment range (horizontal axis in figure 2), the link between the tag and identity-related data (vertical axis), and the domain's security demands (box color). The most critical applications are the red boxes in the figure's top-right area.

System deployment range

Here, I consider three basic types of RFID systems: those with local, restricted operations; those distributed within a single organization; and those distributed across different organizations. In locally operated systems—such as those used in some manufacturing processes or local access-control applications—the readers and back-end system use a local network to exchange information in a restricted area. Rather than exchanging information over a network, it's also possible to connect an RFID reader to a single computer that contains the whole back end (database and software). Although this solution has a limited scope, it might be sufficient, for example, in some manufacturing-process stages, such as element recognition in automatic assembly.

The second system type is distributed in space but controlled by a single organization or by a network of cooperating institutions. Typical examples include public transportation, administrative processes, some industry applications, and some access control systems. It's more difficult to secure these systems than locally operated ones because data is transmitted between physically separated sites and thus is more vulnerable.

The third type is systems that operate over large physical areas and across organizations (and often, platforms). Here, I distinguish between two different system types depending on where the information is stored: in a central database or on RFID chips. If a system uses a central database, it's accessible through a global network. This is the case for applications like Object Name Service,[16] livestock

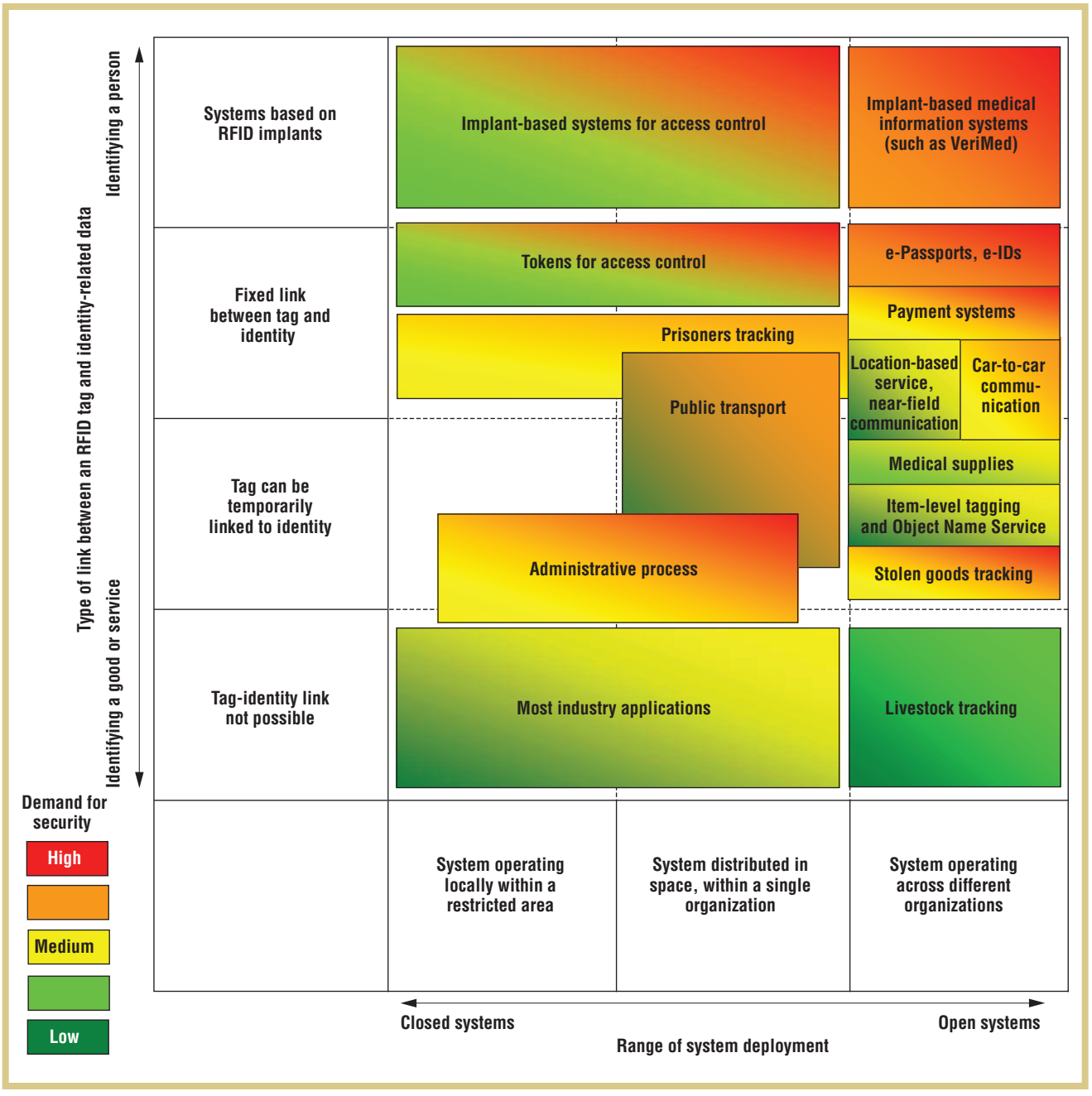

Figure 2. Privacy and security risk assessment taxonomy. E-passports and implant-based access-control and medical information systems are particularly vulnerable application areas.

tracking, and medical care systems such as VeriMed. This category also includes many emerging applications, such as location-based services and stolen-goods tracking systems. An example of systems that operate without a central database and keep data on tokens is e-passports, which store the owner's identity data on memory chips. From a privacy and security viewpoint, avoiding a central database might seem like an advantage; attackers can crack it and eavesdrop on transferred data. On the other hand, for token-based solutions, attackers might retrieve the token's data through the air interface (by eavesdropping a fake reader access) or through reverse engineering.

Links between the tag and identity-related data

Privacy risks exist only in systems that establish a link between the RFID tag and a specific person's identity. In this category, I consider four classes of RFID systems. In the first class, tags contain information about physical objects that are unrelated to people and

can't be linked to them. Examples here include most industrial applications and livestock tracking systems.

In the second class, a tag might be temporarily linked to an identity. Examples include

- item-level tagging in retail (tagged goods purchased in a shop might be used to track people),
- administrative processes (document tagging in an administrative circuit),
- medical supplies (drug labeling), and
- stolen-goods tracking.

Applications using anonymous tokens—such as single-use tickets in public transportation—also belong to this group. From a privacy viewpoint, an anonymous token is no different than any other item: it has no direct link to the carrier's personal identification data. However, if a person carries a whole set of anonymous tags, it can create a "signature" that—if periodically updated—can be permanently used to identify the person, despite the temporary character of the link between a single tag and its owner.

Systems in the third class establish a fixed link between a tag and the owner's identity. Such tags are built into personal tokens, which are directly linked to personal data. Examples here include e-passports and payment systems (such as SpeedPass[1]). Many future applications will also likely fall into this category, including credit card systems, location-based services, mobile phones equipped with near-field communication, and smartcards for access control.

In the fourth class, RFID implants, RFID tags are inserted directly into the human body. Many people have already voluntarily had RFID tags implanted, including for healthcare purposes (as in VeriMed, which offers instant patient identification and medical-records access), for controlling company premises (the VeriGuard system), and even for fun (as in Barcelona's Baja Beach Club). Such systems have a high privacy risk, especially because most existing implants have weak (if any) security measures.[17]

Demand for security

Security demands depend mostly on two factors:

- The size of the potential damage, which might include loss of money, loss of customers, or disclosure of privacy-sensitive information.
- The attackers' motivation level—that is, how much attackers stand to gain if they're successful.

Because these factors often correlate, I aggregate them into a single criterion. However, the factors aren't always linked: in medical information systems, for example, incorrect treatment can cause serious damage, but potential attackers have far less incentive here than they do with payment systems or e-passports.

Vulnerable application domains

Given these risk evaluations, I've identified three application areas that are particularly vulnerable to privacy and security threats: implant-based medical information systems, implant-based access-control systems, and e-passports (see figure 2).

Implant-based medical information systems

VeriMed, which is apparently enjoying rapid adoption by many hospitals, is the first commercial system of this type. VeriMed uses VeriChip RFID implants (www.verichipcorp.com) and gives each patient a unique ID number. When the reader is close to patients, it detects their ID numbers and lets physicians access patients' medical records through a password-protected website. The advantage of such systems is that medical professionals can easily and immediately retrieve vital information from practically everywhere, even when patients are unconscious.

This is a critical system type for several reasons:

- Implants are permanently and physically linked to people, making them sensitive from a privacy perspective.
- VeriMed and all future systems of this type must operate globally; anyone interested in cracking such a system can simply buy a tag and analyze it. People have already done this with VeriChip implants and offer detailed information on the Web about how to crack them (http://cq.cx/verichip.pl).
- Because it's globally accessible, the database—which contains sensitive data—is more vulnerable to unauthorized access.
- Health information is sensitive. Leaking such information to third parties could damage the targeted person's reputation. Malicious modification of health information could lead to incorrect medical treatment and, in the worst case, to the person's death.

Developers can increase implant-based medical information systems' security by encrypting the information an implanted tag transmits and by authenticating the reader. Furthermore, developers can secure the system's back end through strong authentication of the people with database access. For example, to do this, they could use two-way authentication: a password and a token that has a digital signature.

RFID implants also raise concerns beyond those related to privacy and security. Potential developers must consider such factors as low social acceptance, ethical issues, and possible

adverse medical effects, which have yet to be well researched.[18]

Implant-based access-control systems

An RFID tag inserted into a human body can offer authorized access to restricted areas (home or workplace, for example) or devices (a computer or a car). VeriGuard (www.verichipcorp.com/content/solutions/accesscontrol), is the first commercial system of this type, and, like the VeriMed system, is based on VeriChip implants.

Access-control using RFID implants entails a special risk for three reasons:

- As with medical implants, the system is privacy sensitive because the implant is permanently and physically linked to a person.
- It offers potentially high attacker motivation.
- Depending on the application, damages could be quite large in a successful attack.

These implant-based access-control systems are still in the early development stages. Currently, VeriGuard's security measures are weak for two reasons: authentication is based on an ID number that the implant sends in unencrypted form, and the system's VeriChip implant is easy to clone.[17] Some individuals have had RFID tags implanted that were originally manufactured for industry or supply chain purposes and include cryptosecurity features.[19] Nevertheless, implants shouldn't be used for applications with high security demands—even if they have built-in strong authentication algorithms—because there's a risk of coercive attack and potential damage to the victim's body.[17]

Even without strong security features, developers can use implants as an element of access-control systems in a safe way, increasing the overall system's security and efficiency. Combined in multimodal systems, they protect against both password spying and token stealing. In systems with password- and token-based authentication, implants also offer an additional modality that can prevent people from giving unauthorized privileges to colleagues. In a secure environment, organizations could use implants for continuous presence detection, immediately blocking access (to a control board or computer, for example) when the authorized person walks away. The authorized person could then re-establish access through other, more secure authentication methods. In any case, when organizations require strong security, they should use implants only as an additional authentication technique.

E-passports

Many countries—including the US and all European Union members—recently introduced e-passports containing RFID chips. When interrogated by the reader, these chips transmit personal and biometric data; in the latter case, the data is only a digital photo of the owner but in the near future, countries are planning to use fingerprints and possibly iris data.

Personal and biometric data are particularly sensitive. Also, attackers might be highly motivated to copy e-passports or use their data for identity theft. The consequences of an attack could be serious, including personal and biometric data theft, tracking of the e-passport's owner, illegal border crossings or even detonating a bomb designed for a specific country of origin or for a specific individual, based on information emitted by the chip in his or her passport.[20] E-passports' standard security mechanisms (Basic Access Control) use 128-bit key; although the US National Institute of Standards and Technology recommends 112 bit as safe till 2015, the e-passport key is calculated based on information that's accessible in the machine-readable zone. This information, even if it's unknown to attackers, has limited entropy. Given the interrelationship of some data, we can decrease total key entropy to a mere 41 bits, which is definitely insufficient (researchers have calculated an example for the Dutch passport).[21] Moreover, attackers can track the e-passport's owner even without knowing the key using the information exchanged between the RFID tag and reader before reader authentication. Attackers could do this, for example, using tag identifiers that are a part of the anticollision protocol.[21]

Developers can increase RFID passport security using asymmetric cryptography (Extended Access Control). Although some countries use this, it's not mandatory according to International Civil Aviation Organization standards. A simple yet efficient protection is to use a cover made of antiskimming material. As researchers have recently stressed,[22] we need an integrated approach to e-passport security at the international level. Making security measures such as Extended Access Control obligatory and defining detailed standards for security solutions would make passports much safer, regardless of the issuing country.

Of the three application areas I consider particularly sensitive, two are based on RFID implants, which have considerable potential. However, the implant approach also raises several technical, medical, and social concerns that must be solved if this approach is to be more widely adopted.[18] The third application area—e-passports—is part of an ongoing public consultation in the European Union (see www.rfidconsultation.eu).

The focus of this discussion is RFID application areas; however, a specific system's vulnerability depends on its implementation and the applied countermeasures. Developers can build an RFID system with a satisfactory security level even in a high-risk application area. To do so, however, they must pay special attention to the implementation of proportional security measures.

Also, as we move forward, we must reenforce our efforts to achieve effective RFID security and privacy technologies with efforts aimed at creating user trust and awareness.[3] Even a secure system will fail if users think it lacks sufficient security and privacy protections.

ACKNOWLEDGMENTS

Thanks to Ioannis Maghiros from the European Commission, DG Joint Research Centre–IPTS for many helpful comments and suggestions, and to Patricia Farrer from DG JRC – IPTS for help in preparing this article. The views expressed in this article are those of the author, and in no way represent the European Commission's official position.

REFERENCES

1. S. Garfinkel and B. Rosenberg, *RFID: Applications, Security, and Privacy*, Addison-Wesley, 2005.
2. I. Bose and R. Pal, "Auto-ID: Managing Anything, Anywhere, Anytime in the Supply Chain," *Comm. ACM*, vol. 48, no. 8, 2005, pp. 100–106.
3. I. Maghiros, P. Rotter, and M. Van Lieshout, eds., *RFID Technologies: Emerging Issues, Challenges, and Policy Options*, tech. report 22770 EN, European Commission Joint Research Centre's Inst. for Prospective Technological Studies, 2007.
4. B. Nath, F. Reynolds, and R. Want, "RFID Technology and Applications," *IEEE Pervasive Computing*, vol. 5, no. 1, 2006, pp. 22–24.
5. Z. Kfir and A. Wool, "Picking Virtual Pockets Using Relay Attacks On Contactless Smartcard Systems," *Proc. 1st Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks* (Securecomm 05), IEEE CS Press, 2005, pp. 47–58.
6. G. Hancke, *A Practical Relay Attack On ISO 14443 Proximity Cards*, Univ. Cambridge Computer Lab, 2005, www.cl.cam.ac.uk/ ~gh275/relay.pdf.
7. G. Hancke and M. Kuhn, "An RFID Distance Bounding Protocol," *Proc. 1st Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks* (Securecomm 05), IEEE CS Press, 2005, pp. 67–73.
8. I. Kirschenbaum and A. Wool, *How to Build a Low-Cost, Extended-Range RFID Skimmer*, Int'l Assoc. Cryptology Research, 2006, http://eprint.iacr.org/2006/054.
9. G. Karjoth and P. Moskowitz, "Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced," *Proc. Workshop on Privacy in the Electronic Society*, ACM Press, 2005, pp. 27–30.
10. M. Rieback, B. Crispo, and A. Tanenbaum, "RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management," *Proc. Australasian Conf. Information Security and Privacy* (ACISP 05), LNCS 3574, Springer, 2005, pp. 184–194.
11. S. Garfinkel, A. Juels, and R. Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions," *IEEE Security and Privacy*, vol. 3, no. 3, 2005, pp. 34–43.
12. M. Rieback, B. Crispo, and A. Tanenbaum, "Is Your Cat Infected With A Computer Virus?" *Proc. Int'l Conf. Pervasive Computing and Comm.* (Percom 06), IEEE CS Press, 2006, pp. 169–179.
13. J. Wortham "How To: Disable Your Passport's RFID Chip," *Wired*, vol. 15, no. 1, 2007, www.wired.com/wired/archive/15.01/start.html?pg=9.
14. A. Juels, R. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *Proc. Int'l Conf. on Computer and Comm. Security*, ACM Press, 2003, pp. 103–111.
15. S. Hansche, J. Berti, and C. Hare, *Official (ISC)2 Guide to the CISSP Exam*, Auerbach Publications, 2004.
16. B. Fabian, O. Günther, and S. Spiekermann, "Security Analysis of the Object Name Service," *Proc. Workshop Security, Privacy, and Trust in Pervasive and Ubiquitous Comp.*, 2005, http://lasecwww.epfl.ch/~gavoine/download/papers/FabianGS-2005-sptpuc.pdf.
17. J. Halamka et al., "The Security Implications of VeriChip Cloning," *J. American Medical Informatics Assoc.*, vol. 13, no. 6, 2006, pp. 601–607.
18. P. Rotter, B. Daskala, and R. Compañó, "RFID Implants: Opportunities and Challenges in the Identification and Authentication of People," forthcoming, *IEEE Technology and Society*, 2008.
19. A. Graasfata, *RFID Toys*, Wiley, 2006.
20. A. Juels, D. Molnar, and D. Wagner, "Security and Privacy Issues in E-Passports," *Proc. 1st Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks* (Securecomm 05), IEEE CS Press, 2005, pp. 74–88.
21. J.H. Hoepman et al., "Crossing Borders: Security and Privacy Issues of the European E-Passport," *Advances in Information and Computer Security*, LNCS 4266, Springer, 2006, pp. 152–167.
22. M. Snijder, *Security and Privacy in Large-Scale Biometric Systems*, report, European Commission Joint Research Centre's Inst. for Prospective Technological Studies, 2007, http://is.jrc.es/documents/SecurityPrivacyFinalReport.pdf.

the AUTHORS

Paweł Rotter is a researcher at the Institute for Prospective Technological Studies (IPTS), Joint Research Centre of the European Commission in Seville. He is currently on leave from the Department of Automatics at AGH-University of Science and Technology, Krakow, where he is an assistant professor. His current research projects focus on privacy and security aspects of RFID and biometrics. He has a PhD in computer science from AGH-University of Science and Technology. Contact him at rotter@agh.edu.pl.