Institute of Information Systems

University of Bern

Working Paper No 198

RFID Security Risks in Supply Chains: More Than Privacy

Simon Rihs

2007 08

The Working Papers of the Institute of Information Systems are intermediate results from current research projects and should initiate scientific discussion; criticism of the content is desired and welcome. All rights reserved.

Address: Engehaldenstrasse 8, CH-3012 Bern, Switzerland
Phone: +41 (0)31 631 87 39
E-Mail: simon.rihs@iwi.unibe.ch

source: https://doi.org/10.7892/boris.58046 | downloaded: 19.4.2024

Abstract

The use of Radio Frequency IDentification (RFID) in supply chains has received a lot of attention from academia and practitioners in the recent past. Due to important gains in efficiency and visibility in the supply chain, a widespread adaptation is expected to make RFID tags ubiquitous in the future. Thus far, the main criticism of RFID revolves around privacy problems.

In this paper we show that other security issues besides consumer privacy may arise, particularly in a supply chain. Analysed situations include open and closed loop RFID setups and the impact of different attacks on these setups. Building on this, we propose a RFID attack risk classification. Furthermore, we discuss the practical implications of these risks on supply chain operations.

1 Introduction

Radio Frequency IDentificaton (RFID) is a technology which allows contactless access to data on a transponder (also called tag or chip). Already in the late forties of the last century RFID was used to identify friendly aircraft. In 1948, Stockman [1] described the base of RFID in his seminal article “Communication by Means of Reflected Power”. Ongoing miniaturization and advancements in technology have lead to smaller and cheaper tags, which have made widespread use of RFID possible in supply chains. For a historic overview of the development of RFID technology see [2].

The benefits of RFID in supply chains are well documented. Large retailers, e.g. Wal-Mart and the Metro Group as well as large consumer goods producers like Procter & Gamble and Unilever, are amongst the early adaptors of the technology. Defence Departments also expect significant efficiency gains and cost reduction for their Military Logistics Operations. Better stock keeping, reduced shrinkage, improved tracking, better information flows along the supply chain and a higher service level are some of the benefits attributed to the introduction of RFID [3].

RFID is sometimes presented as a more sophisticated barcode or simply as the natural evolution from a paper-based to an electronic auto-ID technology. This analogy is dangerous, as it could result in inadequate risk management of RFID projects and systems. If not addressed, the specific nature of RFID, namely the wireless interface and the small computational footprint, might lead to security problems. The risks of RFID implemen-

tations are often solely seen as a consumer privacy problem, which can be dealt with at the point of sale by deactivating the tags. However, RFID specific security risks such as information leakage and data inconsistency arise along the entire supply chain. Ignoring the RFID specific risks in a supply chain environment can become quite costly. A preliminary consideration of the security risks is a prerequisite to achieve a successful RFID implementation. Rather surprisingly, the security implications of RFID projects for the supply chain are rarely addressed in a structured manner, but, if at all, on an ad hoc basis.

The remainder of the paper is organized as follows. First, we give a brief introduction to Supply Chain Management (SCM) and RFID, as well as to RFID specific supply chain setups. We explore the possible relations between benign and malicious RFID-readers as well as genuine and forged tags. Furthermore, we outline a number of possible attacks on the settings discussed and their respective impact on the supply chain operations. The implementation difficulty and the benefits for the attacker build the base for the RFID risk classification. Finally we derive practical recommendations regarding risk management in RFID supported supply chains.

2 Literature review

SCM is a concept according to which companies in different tiers of a value creating chain collaborate in order to be more competitive. The collaboration may include sharing of sales and planning information and is typically supported by information systems [4]. In this paper, we only consider a very simple, two stage supply chain, consisting of a wholesaler with a warehouse and a retailer with a single store. The reduction of the supply chain to such a simplistic model is adequate, since conclusions about possible attacks and risks with this model can be generalized.

A RFID system consists of one or more readers, and one or more tags. The term reader may be confusing since it is sending data as well. A backend information system connected to the readers is needed to link the information on the tags to databases. The Electronic Product Code (EPC) tags for instance only store a static identifier on the tag, information with little value without an information system [5].

The RFID system in a supply chain can either be designed as an open or closed loop. In a closed loop setup, the tags do not leave the store, warehouse or production site with the

product, whereas in an open loop the tag remains attached and is shared between the members of the supply chain. So far, due to cost constraints, tags are typically attached to transport containers or palettes, not the individual product itself. This will change in the near future, when falling tag prices could make item level tagging profitable [6].

In an RFID environment, one can distinguish between malicious and benign readers or tags. A malicious reader or tag is used by an attacker to attack the system, whereas the benign readers and tags are targets of those attacks. This leads to four possible settings of tag-reader interaction [Figure (i)].

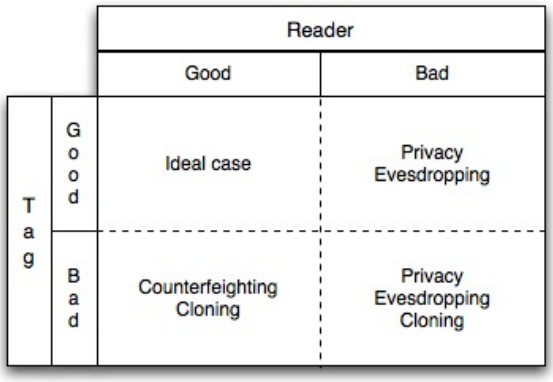

Figure (i) Interaction between benign and malicious readers and tags [7].

It is important to note that attacks can also occur outside of intended RFID communication channels, e.g. by destroying tags or attacking the backend infrastructure. However, there is far more experience on securing databases and infrastructure than RFID. The main focus of this paper is on RFID specific attacks and we assume backend system security as given.

Classifications of attacks against an RFID enabled supply chain may be established with different criteria. In [8] the following risks to a business operating RFID Systems are distinguished: Business Process Risk, Business Intelligence Risk, Privacy Risk, and Externality Risk. In [9] possible attacks on a supply chain were analysed and classified according to the type of risk. The authors distinguish between the consumer and supplier of tagged goods. The consumer of tags endures privacy risks and risks to physical security, whereas the supplier has to face risks of shrinkage, data loss and data integrity. Forgery as well as unauthorized reads and writes affect both. Three layers of RFID privacy, the physical layer, the protocol layer and the application layer are described in [10]. Possible attacks on RFID supply chains could also be classified along those layers. Another

possible and related classification distinguishes the attack vector and the target of the attack.

Furthermore, RFID specific risks could be classified by intent (malicious / accidents) as well as other classifications used in security literature (for a list of possible attack classifications c.f. [11]). RFID privacy attack trees that can be used to analyse weaknesses in the defence of a system were designed and analysed in [12].

While there is thriving research about possible attacks on RFID systems, there have been only few authors addressing these attacks from a supply chain point of view. In this paper, we will discuss the risks of different attacks on supply chains.

3 Attacks and classification

3.1 Analysed attacks

In this paper we followed a qualitative research approach. Due to the rather small number of fully RFID enabled supply chains and even fewer publicly known attacks, quantitative data is sparse and may not be generalizable. Therefore we chose an analytic-deductive design. Furthermore, we assume an economic behavioural model for attackers.

The attacks chosen for analysis have either already been proven feasible or are likely candidates for successful implementations against supply chain operations. The following attacks will be analysed regarding their impact on a supply chain:

- An *Electro Magnetic Pulse* (EMP) seems an unlikely candidate, since it is generally associated with nuclear attacks. However, it was demonstrated that it was possible to destroy an RFID tag in vicinity merely with the discharge from a capacitor found in a disposable camera [13]. Although the strength of electromagnetic pulses diminishes by the square with the distance from the emitter, which greatly reduces the scalability of this attack, it still seems possible to build a RFID zapper to take out a small area, e.g. a smart shelf.

- *Channel flooding* or *jamming* results in a Denial of Service (DoS) attack on the communication between readers and tags. During channel flooding a malicious reader

constantly sends out fake replies to communication requests by legitimate readers, which makes normal reader tag communication impossible. Jamming attacks are less sophisticated and are characterized by an emitter that sends noise in the relevant frequencies to disrupt communication. Channel flooding or jamming is used in some privacy protection technologies, as a countermeasure to data access by unauthorized readers (e.g. [14,15]).

- An *Injection Attack* is marked by either the replacement of a legitimate tag, the addition of a malicious tag into a system or the injection of information into a backend system via a RFID vector. It was shown in a proof of concept that a maliciously crafted RFID tag might introduce destructive code such as a SQL injection, a virus and a buffer overflow into the backend database [16]. Assuming the underlying applications and databases are hardened against malformed data, the risk of active code injection should disappear over time. However, false information in a well formatted way will remain a problem unless a tag to reader authentication is in place.

- A *Clandestine Reader* can be used to read out information or to intercept communication (eavesdropping) without the knowledge of the legitimate RFID tag owner. How a clandestine RFID reader could be built is described in [17]. While the approach focuses on the low cost of the reader, a smaller form factor of the reader would raise costs and was not considered. However, it is well within possibilities to design small clandestine readers for illegitimate reading of tags. Nevertheless, some size constraints apply while designing a clandestine reader with regards to antenna size and the necessary power source. Unauthorized readouts of RFID tags are also called skimming. At a first glance skimming of product codes seems unproblematic. However, skimming of tags could to information about stock turnover or similar information.

A timing analysis is a sophisticated attack where the transaction times of readers are analysed. If the collision detection protocol is known, the number of products could be inferred by the read time, although this might not be feasible outside of a lab setup. Obviously, it would be easier to scan the tags directly, but the distance covered by the reader to tag communication is far longer than the tag to reader distance. Hence, an eavesdropping attack could be covertly carried out with significant distance from the original reader.

3.2 Classification of Attacks

The classification of the chosen attacks along the method proposed by [10] is shown in Table (i). Injection can occur physically by adding or replacing tags as well as on the protocol layer by injecting information at reader requests, and on the application layer where malicious code might get executed.

Layer	**Type of Attack**
Application Layer	Injection
Protocol Layer	Timing Attacks DoS Eavesdropping Injection
Physical Layer	EMP Injection

Table (i) Classification of attacks regarding the affected layer.

The layer, where an attack is carried out, is also the highest layer where a countermeasure can be implemented. One cannot defend against an EMP, which amounts to the physical destruction of the tag, on the application layer [10].

The main benefits of the introduction of RFID in a supply chain come from increased visibility and real time information [18]. This data may also be very valuable for an attacker. An attack is carried out if the cost of the attack is smaller than the value gained. The cost of the attack can be divided into the direct cost of the attack (material, infrastructure, man hours, etc.) and the cost of detection (loss of reputation, legal consequences, etc.) and the detection probability.

RFID drastically lowers the cost of attacks on the supply chain and the detection probability. Hence, some attacks which were costly and not profitable have become economically viable.

4 Results, analysis and discussions

4.1 Risk maps for RFID enabled supply chains

In order to create a risk matrix, the likelihood and consequence of an attack needs to be known. While the consequence of an attack is more easily deductible, the likelihood can only be determined indirectly from other characteristics of an attack. The cost to carry out an attack, the detection probability and benefits to the attacker are determinants of the likelihood of an attack. Table (ii) summarizes the attacks and their respective likelihood.

Attack	**Implementation Cost**	**Detection Probability**	**Benefit of attack**	**Likelihood**
EMP	Low	High	Low	Low
DoS	Low	High	Low	Low
Injection	Medium	Medium	Medium	Medium
Eavesdropping	Medium	Low	High	High

Table (ii) Attacks and their likelihood to occur.

While disruption attacks, like EMP or DoS, are cheap and easy to implement, it is important to note that they do not have a high benefit except for attackers with high intrinsic motivation (hackers, protesters, etc.). However, the threat of those attacks could be used for extortion. Such behaviour was observed before and during DoS attacks on websites [19]. Skimming or injection attacks on the other hand can be quite profitable, since information on stock turnover is very valuable.

Regarding the consequences of the attacks, a distinction between open and closed loop cases is necessary, since the attacks have a different impact depending on the RFID setup in the supply chain.

Table (iii) gives an overview of consequences of a successful attack on an open loop RFID setup in a supply chain. The risk type defined in [8] is included in order to clarify the point of impact of the attack.

Attack	Range	Risk Type	Direct Cost Consequence	Overall Impact
EMP	Shelf	Process Risk	High	Medium
DoS	Shelf to Warehouse / Store	Process Risk	Medium	Medium
Injection	Supply Chain	Process and Intelligence Risk	Medium	High
Eavesdropping	Supply Chain	Intelligence Risk	Low	High

Table (iii) Attack impact with open loop setup.

Table (iv) provides an overview of consequences of a successful attack on a closed loop RFID setup in a supply chain.

Attack	Range	Risk Type	Direct Cost Consequence	Overall Impact
EMP	Shelf to Warehouse	Process Risk	High	High
DoS	Shelf to Warehouse	Process Risk	Medium	Medium
Injection	Warehouse / store	Process and Intelligence Risk	Medium	High
Eavesdropping	Warehouse / Store	Intelligence Risk	Low	Medium

Table (iv) Attack impact with closed loop setup.

A closed loop setup is more vulnerable to an EMP attack, since the tags circulate in a relatively confined space. Obviously, an EMP would not only destroy tags but also other unshielded electronics in vicinity. However, tags are especially vulnerable, since they are not shielded and designed to capture electromagnetic waves.

Based on the overall impact and the likelihood of the attacks, it is possible to build a risk matrix. To give a level of comparability, the manual destruction of tags is included in the risk map. Manual tag destruction is comparable to a destruction of barcodes in likelihood and impact. However, the risk level shown is relative to the other attacks discussed and cannot be compared to existing SCM risk maps without detailed quantitative analysis. In the following figures, a darker shade of grey equals a higher level of risk. A risk map for an open loop RFID setup is show in figure (ii).

Likelihood	**High**			Eavesdropping
	Medium			Injection
	Low	Manual Tag destruction	EMP DoS	
		Low	**Medium**	**High**
	Impact			

Figure (ii) Risk Matrix for an open loop system.

Since a RFID system with shared tags is more complex, more possible attack vectors exist. Especially during transport, a batch is vulnerable to an injection attack, since physical security is typically lower than in warehouses. Figure (iii) illustrates the risks of RFID attacks in a closed loop setup.

Likelihood	**High**		Eavesdropping	
	Medium			
	Low	Manual Tag destruction	DoS	Injection EMP
		Low	**Medium**	**High**
	Impact			

Figure (iii) Risk Matrix for closed loop system.

The reduced impact of the espionage attack (eavesdropping) is due to the focus of the risk map for the entire supply chain. A successful espionage in a closed loop setting can be business endangering for an individual company in the supply chain. However, the impact on the entire supply chain is generally smaller than in an open loop setup.

One notices that the impact of disruption attacks is higher with a closed loop setup. This is due to the fact that it is possible that the destruction of tags or respectively the disruption of the communication may affect the entire closed loop system.

Tag injection attacks are inherently more difficult since the number of tags in the system is known and additional tags should be noticed by the backend system which is the reason for a lower likelihood compared to Table (ii). Replacement of tags and injection of data into tags might still be possible if the tags contain more than an identifier (e.g., environmental data such as temperature or pressure).

4.2 Practical implications

Prior to the implementation of RFID in a supply chain, a risk analysis of the exposed infrastructure and information should be carried out. So far very little data on attacks of RFID enabled supply chains exist. This can be explained by the following reasons. Supply chains having implemented an RFID system are still in a shakedown phase, where the main issues are ensuring the functionality. Due to the limited number of targets, there is less opportunity for a successful attack. Furthermore, potential attackers may still be learning how to best exploit real life RFID supply chains, as most published attacks so far were merely proof of concepts in a lab setup. The fact that successful attacks are often not published by the victims is widely discussed in security literature generally (e.g. [20]) and might be especially relevant in the RFID setting, since the negative publicity associated with an attack on a model implementation of RFID in a supply chain could be perceived as failure and weaken the acceptance of the technology.

The following approaches, documented in risk management literature, apply to RFID as well. Prevention, early detection and response, and risk transfer are suitable means to deal with risk in a company or supply chain. It may, of course, also be acceptable to bear a risk without an appropriate control in place, as long as it is based on an explicit decision [21].

Prevention of RFID specific attacks firstly relies on good physical security of facilities. It is important to note that in some cases factories need enhanced security measures to keep the same level of risk compared to a case without RFID, since some attacks are easier.

Another prevention option is to strengthen the security properties of RFID tags through cryptography. However, one of the main problems of most proposed cryptographic solutions is their high cost in computing time and chip memory [22]. Even though there is promising research on the reduction of logic gates needed to implement cryptographic algorithms [23], cost pressures will likely prevent their widespread adaptation. Furthermore, the computing time required for complex cryptographic operations effectively prevents real time and near real time applications of RFID. Unfortunately, this is precisely where the use of RFID would yield the highest gains in visibility and efficiency.

Added redundancy, meaning the combination of a RFID based system and another system in the automated processes makes it possible to mitigate some of the risks associated with RFID in supply chains. Special attention needs to be given at the organizational handover

points, which are more vulnerable since they are less controllable. The automation due to the use of RFID makes injection attacks easier. With an automated incoming goods process the substitution of products with tags by counterfeit or empty boxes with the same tags are possible. A continuous monitoring should be able to pick up when the same tag appears twice in the system. However, such a system of continuous monitoring is not always in place. Furthermore, an increase in automation leads to a decrease in manual checks, which are able to detect empty boxes. More than one system should be used at goods arrival, e.g. a RFID system for automatic data entry and an automated scale which cross checks the goods arrival.

The ongoing research into Attack Detection Systems or Intrusion Detection Systems (IDS) for RFID has so far mainly focused on privacy protection. A closer look at supply chain settings would be beneficial. The RFID Vindictive Sentinel proposed by Sarma [24], which allows only registered readers to communicate with the tags in the protection zone of the Sentinel, could be seen as an RFID IDS. However, by flooding the communication channel, which is the standard response to non-authorized readers, it amounts to a homemade DoS attack. While the tags are thus protected from illegitimate kill commands and data leaks, the RFID communication in the zone is disrupted, which could also be of heavy consequence in a real time scenario.

Since the attacks discussed are already covered by existing legislation, there is little need for RFID specific legislation in the SCM context. However, the forensics needed to prove an attack is difficult and has not yet been described in sufficient detail. So far, audit trails end at the back-end system, or, in the best case, at the reader, which holds a record of transactions. To enhance the chances of successful forensic analysis and in order to create an audit trail, a tamper resistant Radio Frequency (RF) recording device which is separate from the rest of the RFID infrastructure should be developed and implemented in all critical areas.

Further research is needed in proof of concept attacks, especially the feasibility of the attacks in real world supply chains settings to test the resilience of response systems and, in the case of disruption attacks, fall back mechanisms. Furthermore, a quantitative cost analysis of RFID risks and their impact on visibility and time critical applications would provide insight on the business impact of the risks discussed above.

5. Conclusions

The analysis of the potential attacks shows that their impact depends on the setup of the RFID system, with open loops more prone to eavesdropping and closed loops to disruption attacks.

Process and intelligence risks for the implementing company as well as for the supply chain result from using RFID systems. The management of those risks relies on physical security, added redundancy with non-RF systems and early detection by intrusion detection systems. Forensic proof after a successful attack on RFID systems is a widely unrecognized issue in RFID risk management.

Most RFID projects are currently in a shakedown phase, meaning the implementing organization is mainly trying to get the systems to work correctly and efficiently, with little or no consideration of security. The lack of security concern amongst RFID project sponsors and managers is akin to the lack of security concern in Internet projects in the late nineties, where viruses and attacks were mainly discussed in academic circles. As George Santayana said *"Those who cannot remember the past are condemned to repeat it."*

5 References

[1] Stockman, H., 1948, Communication by means of reflected power. *Proceedings of the IRE,* **36**(10), 1196-1204.

[2] Landt, J., and Catlin, B., 2001, Shrouds of time the history of RFID. Retrieved 2006-01-10, from http://www.aimglobal.org/technologies/RFID/resources/shrouds_of_time.pdf

[3] Michael, K., and McCathie, L., 2005, *The pros and cons of RFID in supply chain management. Proceedings of the International Conference on Mobile Business (ICMB'05),* 623- 629.

[4] Knolmayer, G., Mertens, P., and Zeier, A., 2002, *Supply chain management based on SAP systems*. Springer.

[5] Avoine, G., 2005, Cryptography in radio frequency identification and fair exchange protocols. *Faculté Informatique et Communications.* Retrieved 2007-06-07, from http://lasecwww.epfl.ch/~gavoine/download/papers/Avoine-2005-thesis.pdf

[6] Niemeyer, A., Pak, M. H., and Ramaswamy, S. E., 2003, Smart tags for your supply chain. *The McKinsey Quarterly*, **2003**(4), 6-8.

[7] Jules, A., 2005, *RFID: The problems of cloning and counterfeiting. Talk at the Workshop on RFID and Light-Weight Crypto*.

[8] Karygiannis, T., Eydt, B., Barber, G., Bunn, L., and Phillips, T. (2007). Guidelines for securing radio frequency identification (RFID) systems. Retrieved 2007-06-

15, from http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf

[9] Garfinkel, S., Juels, A., and Pappu, R., 2005, RFID privacy: An overview of problems and proposed solutions. *IEEE Security and Privacy*, **3**(3), 34-43.

[10] Avoine, G., 2005, RFID traceability: A multilayer problem. In A. Patrick and M. Yung (Eds.), *Financial cryptography – fc'05, volume 3570 of lecture notes in computer science* (pp. 125-140). Springer.

[11] Paulauskas, N., and Garsva, E., 2006, Computer system attack classification. *Electronics and Electrical Engeneering*, **66**(2), 84-87.

[12] Spiekermann, S., and Ziekow, H., 2005, *RFID: A 7-point plan to ensure privacy. Proceedings of the European Conference on Information Systems.*

[13] MiniMe, and Mahajivana., 2005, RFID-zapper. Retrieved 2006-01-21, from https://events.ccc.de/congress/2005/wiki/RFID-Zapper.

[14] Juels, A., and Brainard, J., 2004, *Flexible blocker tags on the cheap. Proceedings of the Workshop on Privacy in the Electronic Society – WPES*, 1-7.

[15] Rieback, M., Crispo, B., and Tanenbaum, A., 2005, *Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags. Proceedings of the "13th Security Protocol International Workshop".*

[16] Rieback, M., Crispo, B., and Tanenbaum, A., 2006, *Is your cat infected with a computer virus? Proceedings of the Pervasive Computing and Communications.*

[17] Kirschenbaum, I., and Wool, A., 2006, *How to build a low-cost, extended-range RFID skimmer. Proceedings of the 5th USENIX Security Symposium*, 43-57.

[18] Lee, H., and Özer, Ö., 2007, Unlocking the value of RFID. *Production and Operations Management*, **16**(1), 40-64.

[19] Gosling, P., 2004, Crooks gang up to beat banks, *infosecurity*.

[20] Hoffer, J. A., and Straub, D. W. J., 1989, The 9 to 5 underground: Are you policing computer crimes? *Sloan management review.*, **30**(4), 35-43.

[21] Müssigmann, N., 2006, Mitigating risk during strategic supply network modelling. In W. Kersten and T. Blecker (Eds.), *Managing risks in supply chains* (pp. 213-226). Erich Schmidt.

[22] Avoine, G., Dysli, E., and Oechslin, P., 2005, Reducing time complexity in RFID systems. In P. Bart and S. Tavares (Eds.), *Selected areas in cryptography – SAC 2005, lecture notes in computer science*. Springer.

[23] Feldhofer, M., Dominikus, S., and Wolkerstorfer, J., 2004, Strong authentication for RFID systems using the AES algorithm. In M. Joye and J. J. Quisquater (Eds.), *Lecture notes in computer science* (pp. 357-370). Springer.

[24] Sarma, S., 2006 *Some issues related to RFID and security. Talk at the Workshop on RFID Security 2006.*