12 Threat Modeling in EPC-Based Information Sharing Networks

Alexander Ilic, Trevor Burbridge, Andrea Soppera, Florian Michahelles, and Elgar Fleisch

CONTENTS

EPC-based information sharing networks are a global effort to standardize the supply chainwide exchange of operational trace data. Due to the complex nature of supply chains and different information sharing relationships, security is a critical issue. Prior research and end-user feedback suggest that there is currently a limited understanding of how to assess and address security threats that could affect multiple parties. In this chapter, we describe a threat model that can help to compensate this shortcoming. Our model helps to assess current as well as future risks. Our findings suggest that designers, operators, and users of EPC-based information sharing networks should focus on providing accountability as a key aspect of improving collective security.

12.1 INTRODUCTION

Today's global market places face information uncertainty. The demands in almost every industrial sector are volatile, and product and technology life-cycle times have shortened dramatically. Many companies have experienced difficulties to predict the effect of market changes and the effect of understocking or overstocking increases. In this dynamic context, we see the need for supply chains that are able to cope with high level of heterogeneity and customization. RFID technology is a cost-efficient way of gathering trace data about logistic objects. Amongst other benefits, RFID is said to optimize supply chain operations [1], reduce theft [2], and prevent counterfeiting [3]. The EPCglobal Architectural Framework [4] offers standards for gathering, filtering, and sharing trace data with other partners in a supply chain through the EPC information service (EPCIS). Sharing trace data through information sharing network beyond a single organization enables a radical new degree of supply chain visibility and traceability. Capturing and sharing supply chain information is valuable for many trading partners. This information can be used to improve and customize services and processes, to provide statistical and marketing information and could, in certain situations, be sold to third parties. On the other hand, we have to be careful that misuse and unauthorized access to this information could violate service agreements, cause fraud, and, in certain cases, disrupt critical supply chain processes. The risk is that a great deal of dependency on external processes and information could lead to a loss of control and expose a company to greater supply chain vulnerability.

Organizations perceive and address security issues in different ways, ranging from completely ignoring them and losing control of confidential information (mainly due to lack of awareness), to being so cautious as to prevent new technology being deployed because of the lack of expertise in recognizing and dealing with potential threats. The prevailing, dominant, strategy is to consider these threats as an internal risk, and to manage them locally (within the bounds of the enterprize). The wider supply chain context is only rarely considered, and there is minimal support for those needing to optimize large-scale, global-level, supply chains. This is paradoxical and most likely contrary to the real source of the greatest threat. It can be argued that the biggest risk to an enterprise may in fact be in the wider supply chain network, and the data control mechanisms applied within an organization itself is just a small part of the security it really needs. The result of this is often an exposure to higher levels of risk as a result of miscommunication and lack of tools to express authorization to electronically manage information. Consequently, EPC-based information sharing networks suffer from so-called interdependent security problems (as described by Kunreuther and Heal [5], e.g.).

It is important for senior managers to identify the most relevant and critical threats and to concentrate on sharing this information across the supply chain partners so that an appropriate supply chainwide security strategy can be put in place. Overall we seek to provide means for simplifying security management experience so that organizations can feel they are in control of their confidential data and that this data is managed in an accountable way. The goal of this chapter is to provide a tool and a method for reasoning so that the most relevant and critical threats can be identified. As the suspected interdependent nature of security problems increases the problem domain complexity, a structured approach is needed. Hence, we employ a threat modelling approach that can serve as a basis for existing enterprise risk management frameworks. The purpose of our threat model is

therefore to establish where potential weak areas lie and what impact threats for internal processes and for the wider network have. Once an organization understands its potential threats, it can then start to put in place an appropriate security strategy (counter measures), and will have a clear picture of how security breaches could compromise their own processes, as well as potentially damaging their customers or partners.

To achieve the goal of providing a structured understanding for IT security threats associated with EPC-based information sharing networks, this chapter is structured as follows. First, we start with related work and present that, to our best knowledge, no threat model for an EPCglobal-based information sharing network exists. In Section 12.3, we develop our threat model based on the information life cycle of an EPCglobal-based network. Section 12.4 then completes the threat model by providing an attacker perspective on the different life-cycle phases. We use a qualitative analysis approach, where we introduce the potential attacker types together with their motivations and capabilities. Different attacks are enumerated, described, and categorized against their threat to the classical security goals of confidentiality, integrity, and availability (CIA). Section 12.5 shows the practical relevance of our threat model for improved security risk management. We provide an application guideline that is concluded with a fictive example. In Section 12.6, we discuss our learnings and findings. Finally, Section 12.6 concludes and summarizes the key results.

12.2 RELATED WORK

The goal of this chapter is to provide a threat model to better understand the nature of security problems in the domain of EPC-based information sharing networks. In general, security is a topic that is largely discussed in the area of RFID. A recent research survey of Juels [6] shows, the academic community is currently mainly focused on securing RFID tags or the tag to reader link. A reason for this may be the current hype on privacy issues [7] due to insecure tag implementations and the amplifications of public perception in the media. Avoine and Oechslin [8] recognize that RFID technology imposes a multilayer privacy problem. Their perspective focuses on a physical, a communication, and a simplified application layer. Garfinkel et al. [9] look at the RFID privacy problems not only from a multilayer perspective but also beyond the scope of a single organization. Also, general security RFID security documents such as the National Institute of Standards and Technology (NIST) [10], boot-sector infector (BSI) [11], and BRIDGE [12] report confirm that there are security issues beyond the protection ability of a single entity. Explicitly focused on the security of the EPCglobal network specification is the work of Konidala et al. [13], which assesses the security of individual interfaces and elicits a broad range of security threats. However, although all of the previously mentioned works state one or more solutions concerning the hardware and software levels, they rarely discuss the interorganizational and network aspects of security investments. On a general perspective for interorganizational security problems, Kunreuther and Heal [5] discuss the class of so-called interdependent security problems. They use a game-theoretical approach to prove that organizations are better off if they cooperate in different scenarios. Yet, they confirm that each party may have the incentive to "cheat" and save on investment, at the same time increasing the risk of a potential loss to itself and other partners through security vulnerabilities. A threat analysis should therefore always consider the risk of contagion from other organizations that have not yet implemented the same level of security. Moreover, as Anderson [14,15] indicates, a solution to the interdependent security problems requires properly aligned incentives for each participating organization to cooperate for higher collective security. In contrast to the cited papers above, we look at the RFID security from an interorganizational and economically motivated perspective to demonstrate that EPC-based information sharing networks suffer from interdependent security problems. We use a structured threat modeling approach to identify potential threats and weak areas in EPC-based information sharing networks. The threat model is hereby a suitable representation to identify threats in a certain domain. The idea is that this domain knowledge of security threats can feed into

existing risk management processes or frameworks of organizations and therefore improve the overall security management process.

12.3 THREAT MODEL OVERVIEW

A system may be exposed to many different kinds of threats. For the remainder of this chapter, we will focus on threats that could emerge from a previously unknown vulnerability. As the probability of such an event is not predictable outside a specific context, we will focus on understanding within which areas threats can theoretically occur. Our threat model is based on a simple information life cycle for RFID read-event data, which will be introduced in the following section. The threat model comprises the following three components:

- The system model, which offers a suitable perspective on the system that should be protected
- The attack sources, which describe the characteristics of likely attacker types
- A threat list, which contains some attacks against the classical security goals of CIA

12.3.1 Information Life Cycle

Instead of focusing only on technology aspects, this chapter is concerned with the security problems associated with the exchange of item-level event information in EPC-based networks. We assume that the information of interest is generated through reads of RFID tags. As these RFID tags are attached to logistic objects, the supply chainwide sharing of these read events may be of significant business value. Generally, if data is generated at one organization and should be shared with another one, the following steps occur. First, the event data is created by an organization. Second, the organization prepares and approves the data for sharing with other selected parties. Finally, interested and authorized parties can search and retrieve the data from the offering party. The described flow resembles an information life cycle (Figure 12.1), which is a suitable baseline for analyzing information security risks [5].

The advantage is that the life-cycle model helps to structure the weak areas of a system by decomposing it into functional phases critical for the information handling. Like other academic papers (e.g., [17]), we map the life-cycle phases to specific architectural system components. Figure 12.2 shows one loop of the resulting information life-cycle model for EPCglobal-based information sharing networks. The loop consists of five distinct life-cycle phases, in which organizations can take one or more of the following roles suitable for the exchange of RFID data traces [18]: data supplier*, data consumer, or metadata operator.

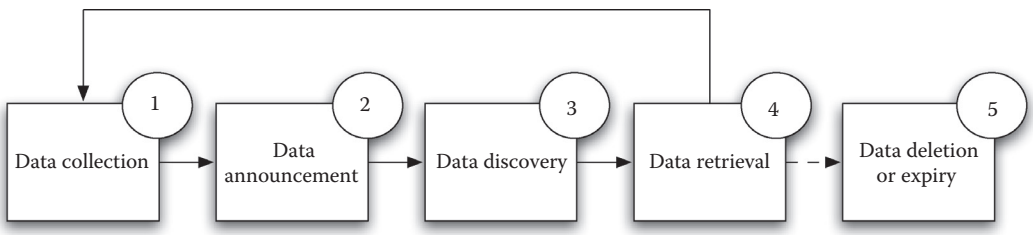

FIGURE 12.1 Generic trace data information life cycle with its five phases.

* As we focus on the information sharing aspects, we will use the term trace data supplier instead of distinguishing between trace data creator and trace data publisher.

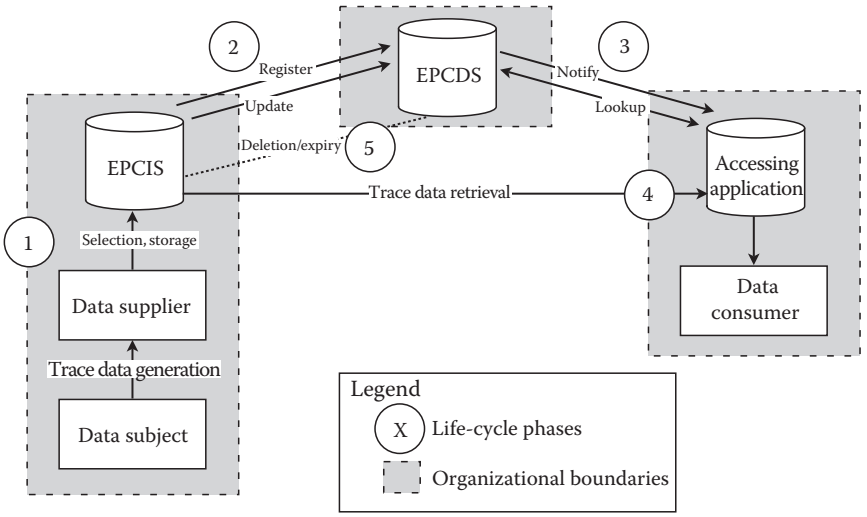

FIGURE 12.2 Information life cycle of the EPCglobal-based network.

12.3.2 System Model Based on Life-Cycle Phases

The following sections describe the functionality, components, and interactions in detail. The description is relevant, as each of the components constitutes potential entry points or vulnerable assets for the overall system.

12.3.2.1 Phase 1: Trace Data Creation and Storage

In this phase, trace data is generated and prepared for sharing throughout the network. First, a trace data supplier uses RFID readers to interrogate tags and create trace data events for specific trace data subjects. The subjects can be any type of tagged object such as container, pallets, cases, or even individual items. Moreover, the RFID tags contain unique identifiers that act as proxy for identifying trace data subjects. By means of these unique identifiers, trace data can be collated to establish trace histories of the data subjects across multiple organizations. Second, the trace data supplier selects the trace data information he or she would like to share with others and stores this information in a database, the so-called EPCIS repository. The EPCIS repository contains access policies that determine which data can be seen by whom and makes sure that an organization can control access to its data.

12.3.2.2 Phase 2: Trace Data Announcement

As information about a certain trace data subject is distributed over a supply chain (due to its logistic flow), the EPCIS discovery service (EPCDS) provides a service to determine which EPCIS repository might have information about a particular object. For this concept to work, each partner offering data traces regarding a particular EPC must announce to the EPCDS that they have related trace data by sending an update announcement to the EPCDS.

12.3.2.3 Phase 3: Trace Data Lookup and Notification

In this phase, a trace data consumer submits a query to the EPCDS to find out which EPCIS repositories have data about specific objects. The query may be a onetime call or a standing query. In the case of a standing query, the EPCDS sends notifications to a trace data consumer whenever a trace data announcement matches their expressed interests.

12.3.2.4 Phase 4: Trace Data Retrieval

After querying the EPCDS for potential information sources (phase 3), phase 4 is now concerned with the actual trace data information retrieval. Depending on the credentials of the trace data consumer and the security policy of the trace data suppliers, the trace data can be retrieved from the different EPCIS systems.

12.3.2.5 Phase 5: Trace Data Deletion

Although this issue is not discussed on a broader scope, it can be assumed that in an information life cycle all of the trace data will not be retained forever. Therefore, we foresee a phase 5, which is typical for almost every life cycle, where trace data is purged through an explicit operation or reaching an expiry time.

12.4 ATTACKER PERSPECTIVE

To complete our threat model, we will now apply an attacker-centric perspective against our life-cycle model established in the previous section to explain the extent and nature of threats. The attacker-perspective was chosen over a system-centric view, as actual implementations of EPC-based information sharing networks may differ in their security strengths and vulnerabilities [19].

12.4.1 Attacker Types and Capabilities

In the following section, we describe and characterize the most important attacker types. The three types were chosen due to their access abilities (internal/external) and their main motivation (benefits/damage).

Being aware of the attacker characteristics helps to conduct better risk assessment. The attractiveness to a certain attacker type and the characteristics of the attacker types (as summarized in Table 12.1) largely determines the probability and damage potential of attacks during the life-cycle phases.

12.4.1.1 Competitors

Malicious organizations may want to attack the trace data network to either strengthen their position, to harm their competitor, or a combination of both. Typically the goal is to steal confidential information to gain competitive advantage or to disrupt the information integrity and thereby affect business processes. Process failure can result in direct and indirect financial damage, while subversion of a

TABLE 12.1
Summary of the Characteristics of Investigated Attacker Types

	Competitor	Insider	Saboteur
Main motivation	Competitive benefit	Personal benefit	Damage
System knowledge	Limited knowledge	Full knowledge	Limited knowledge
Trust level	Untrusted	Trusted	Untrusted
Probable entry points	External interfaces	From within	External interfaces
Critical phases	Data announcement	Data creation	Data announcement
	Data retrieval	Data announcement	Data lookup
		Data retrieval	Data deletion
		Data deletion	
Attack scale	Single target	Single target	Single–multiple targets

process can result in benefits to the attacker such as the availability of private assets. One example of this subversion is the use of regular distribution channels for the sale of counterfeit goods. What makes a competitor an attractive target is that the damage and losses caused can directly translate into the other organization's benefits. The access and knowledge to the network's security weaknesses is, however, fairly limited. Competitors need to find vulnerabilities in a very cautious way. They will therefore likely target the vulnerabilities where the attack is easy to perform and hard to trace, which usually lie in system configuration and interaction [20]. Potential entry points may therefore focus on the public network interfaces of a trace data supplier (in phases 2 and 4). Moreover, the manipulation of physical items or tags in phase 1 is also possible, as is observation of network traffic during phases 2, 3, and 4.

12.4.1.2 Insiders

Insiders are employees of network participants that have malicious intentions of disrupting the network or stealing information for their personal benefit. Personal motivational reasons often include low wages and working environment, affiliation with a competitor or terrorist organization, or personal benefits, for example due to predictive stock market reactions. Insiders are particularly dangerous, as they can have the full knowledge of the internal system of an organization and the resources at their disposal to run an extensive and well-prepared attack. They have a trusted status within one organization and can exploit this to harm either the whole system (including the organization they work for) or specific targets. Unlike other attacker types, insiders do not need to rely on finding vulnerabilities. Instead, they can abuse their privileges or attack the network via hidden attacks. Attack situations may become particularly attractive if observation and therefore punishment is difficult or unlikely [21]. Entry points for attacks usually come from within an organization and can consist of both remote and local proximity attacks. Life-cycle phases 1, 2, 4, and 5 are particularly vulnerable to an attacker within the data supplier organizations.

12.4.1.3 Saboteurs

In contrast to other attacker types, the motivation of saboteurs is not primarily to get personal benefits from attacks but rather to cause as much damage as possible in as little time as possible [17]. Like competitors, they need to invest in finding vulnerabilities or to use an insider (e.g., social engineering) before being able to mount an attack. Once they find a vulnerability that is applicable to more than one particular target, they will likely aim at exploiting the vulnerability and attack multiple targets. Potential entry points include especially centralized or shared network elements such as the EPCDS, attacks on which would affect phases 2, 3, and 5. An attack affecting these phases could cause damage to all participants by disrupting the service availability or metadata integrity. If an attack is targeted more specifically at individual targets, potential entry points can be found in the EPCDS interface (phase 2) and the EPCIS interface (phase 4). Also, saboteurs are able to mount attacks on phase 1, by using either insiders or specially prepared tagged objects equipped with malicious software (e.g., RFID-virus [22]) or other hardware (e.g., blocker tags [6], radio jamming).

12.4.2 Threats

In this section, we discuss threats against components of the trace data systems. To structure the discussion, we categorize potential attacks against the information life-cycle phases and refer them to the (CIA) security goals. The following list briefly explains each of the CIA goals:

- Confidentiality: Only authorized parties should have access to the trace data at specified times and in a specified manner. This applies to data in storage (tag, EPCIS), during processing (ALE) or in transit (over a network).

- Integrity: The trace data should remain accurate and complete. In addition, system components should retain their integrity and operate as intended.
- Availability: Data, networks, and information systems must be available in a timely manner to meet the requirement of business operations.

Attacks that compromise the CIA goals can result in numerous threats to the business. Each business must analyze the severity of the business threat that can result from the attack on the trace data system. Such threats may include the stalling or subversion of a business operation. For example, a shipment may be stopped or delayed, or sent to the wrong location. Attacks on the trace data may also be used for activities such as theft or the introduction of counterfeit goods into the existing supply chain. Compromising the confidentiality of any trace data activity may also be used to infer business activity and implement competitive strategies, resulting in a loss of market or suppliers.

12.4.2.1 Attacks during Trace Data Creation and Storage

Trace data is generated by reads of RFID tags and the resultant processing. Attacks are possible on the tags themselves, along with the collection and processing networks and the trace data storage systems. The communication networks, such as the wireless tag–reader protocol and the trace data supplier's internal networks should also be considered open to attack.

- Confidentiality: Such attacks comprise of both unauthorized access to trace data and eavesdropping on legitimate communications. For example, tags may be read by unauthorized readers for competitive intelligence, identifying opportunities for theft, or the cloning of the tag or other communications. Network traffic may also be observed and unauthorized access attempts made to trace data collection components or storage systems.
- Integrity: Attacks on the integrity of the system may impact on the CIA and accountability of the trace data. Attackers may seek to compromise the integrity of the trace data by attacking the elements or networks within the trace data supplier. The attacker may also target the tag or reader devices that may be physically accessible at certain points in their lifetime. The trace data integrity may be compromised by modification or removal of the data on the tag, EPCIS, or as it passes through any network or intermediate systems. Cloning and replay of trace data should also be considered. The tag itself may be cloned for later presentation to a tag reader, for example on a counterfeit good. Communications may also be replayed to the original trace data supplier's systems, or systems within a different organization. Other injection attacks may use falsified information, delivering this into the system where sufficient checks are not performed on the data integrity or the identity of the injecting system.
- Availability: Attackers may seek to remove the availability of system components (and hence trace data) from dependent systems and processes. Access may be disrupted by attacking the system components or communications capabilities. External attackers may attack external interfaces and components. This will include physical attacks on tags and readers and disruption of the tag communication, for example through radio or protocol jamming [6]. Wireless networks used for the tag communication and wireless reader devices are particularly vulnerable.

12.4.2.2 Attacks during Trace Data Announcement

Attackers can target the systems involved in the announcement of trace data, including the originating trace data supplier, the EPCDS, or the intervening network such as the Internet.

- Confidentiality: Attackers may seek to gain access to the announcement of trace data. They can do this by eavesdropping on the network used to communicate with the EPCDS from the trace data supplier. Attackers may also impersonate an authorized recipient of the announcement, for example subscribing to trace data announcements with false credentials at either the EPCDS or the trace data supplier systems.
- Integrity: Attackers may attack the integrity of trace data announcements by modifying or removing announcements, or injecting false or replayed announcements. This may cause trace data consumers to miss the announcement of trace data, be mislead about the existence of trace data, or be diverted to incorrect trace data suppliers.
- Availability: Attackers may attack the availability of the EPCDS update interface, along with the network carrying such updates and the systems in the trace data supplier producing updates. Such availability attacks will affect the integrity of the trace data held in the EPCDS or the timely availability of the trace data for use within business processes. Because the EPCDS update interface is likely to be available to other entities over the Internet, it is particularly vulnerable to large-scale denial-of-service (DoS) attacks from external entities such as saboteurs.

12.4.2.3 Attacks during Trace Data Search

Attackers can target the search activity between the trace data consumer and the ECPDS. This can involve attacks on the communication network, the EPCDS, or the trace data consumer systems.

- Confidentiality: Attackers will attempt to compromise the confidentiality of the trace data announcements held in the EPCDS, and may also eavesdrop on the trace data searches and responses from other parties. The availability and interest of parties in EPC identifiers may constitute sensitive business information. The patterns of EPCs announced and accessed may be mined to infer business information. Such patterns may include the parties and EPCs involved along with the timing of the announcements/searches, and any other information that may be available such as geographic location. Even if such communications are securely encrypted, the network traffic may still be mined to infer business activity. For example, attacker may learn that a certain pattern of announcements and searches occurs when Company A receives a palette of a specific type of goods.
- Integrity: Attackers may mount man-in-the-middle attacks to affect the trace data consumer, along with attacking the integrity of the trace data held by the EPCDS or the operation of the EPCDS itself. This can subvert operations relying solely on the trace data announcements, cause trace data to remain unnoticed (stalling business operations), or lead trace data consumers to perform trace data retrieval on the incorrect systems.
- Availability: Attackers may launch DoS attacks to exhaust the trace data search capabilities. This will prevent trace data consumers from being able to search and retrieve trace data announcements. Processes will fail to act on new trace data in a timely manner, producing delays in business operations.

12.4.2.4 Attacks during Trace Data Retrieval

Attackers may target the trace data supplier and consumer systems or the communications network used to transfer trace data.

- Confidentiality: Attackers may seek to compromise the confidentiality of the trace data maintained in the EPCIS or eavesdrop on communications between the trace data consumer and trace data supplier. Along with the confidentiality of the trace data, the confidentiality of the trace data consumer should also be considered. The trace data requests will reveal detailed information about the trace data consumer's operations.

- Integrity: Attackers may compromise the integrity of the trace data in the EPCIS, or the integrity of the networked communications between the trace data consumer and supplier. The trace data consumer may be misled by removing trace data from the retrieval response, or by modifying or fabricating additional trace data.
- Availability: Attackers may target the trace data consumer and supplier external interfaces or communication networks to remove their ability to perform trace data retrieval. Because the EPCIS is a widely reachable service, it is vulnerable to DoS attacks. Although the EPCIS may restrict service to only trusted trace data consumers (under normal operation or during times of service overload), attacks to deny network bandwidth will remain possible. Solutions to availability threats should consider solutions that address both the network and system availability.

12.4.2.5 Attacks during Trace Data Deletion

Attacker may target the trace data and announcement storage systems or the operations to remove or renew trace data and announcements.

- Confidentiality: Attackers may seek access to the trace data deletion information. Such messages may inform the attacker that the trace data was present, along with revealing information about the lifetime and usefulness of the trace data. Depending on the system implementation, the attacker may listen to expiry and refresh messages, or explicit deletion instructions.
- Integrity: Attackers may attack the integrity of the trace data deletion communications or seek to delete trace data (announcements). Deletion of the announcement information from the EPCDS will mean that trace data is not found by trace data consumers. Removal of trace data from the trace data supplier will cause confusion as trace data consumers attempt to retrieve data that no longer exists, particularly if this breaks service level agreements (SLAs) for the retention of data and incurs financial or other penalties.
- Availability: Attackers may attack the availability of the systems and networks during the trace data deletion phase. This may result in the data being retained unintentionally, or may actually lead to the premature removal of data (e.g., if a refresh instruction is disrupted).

12.5 APPLICATION GUIDELINES

Organizations rely on risk management to select cost-effective countermeasures for mitigating potential threats. Risks are usually assessed in the dimensions of negative impact (potential damage, unfavorable adverse effects, and consequences) and probability (at which a risk is likely to occur) [23]. To evaluate risks according to these factors, a comprehensive understanding of the situation is required. In IT security, threat modeling is regarded as an enabling step for effective security risk management [24]. Organizations can use our threat model as a tool to better understand and estimate security risks associated with trace data sharing networks. A security process based on threat modeling, as described in Ref. [25], is depicted in Figure 12.3.

12.5.1 General Guidelines

To be able to actually use the proposed threat model as a basis for risk management, the following steps need to be applied to put the threat model into an organization's context (Figure 12.3). The context allows for determining the individual threat exposure depending on the roles and phases of the life-cycle model. The threat model supports the identification of the risks based on contextual factors as shown in Table 12.2. After the risk identification phase, risks can be evaluated by using our context factors together as input failure mode and effect analysis (FMEA) [26] model or to a proven

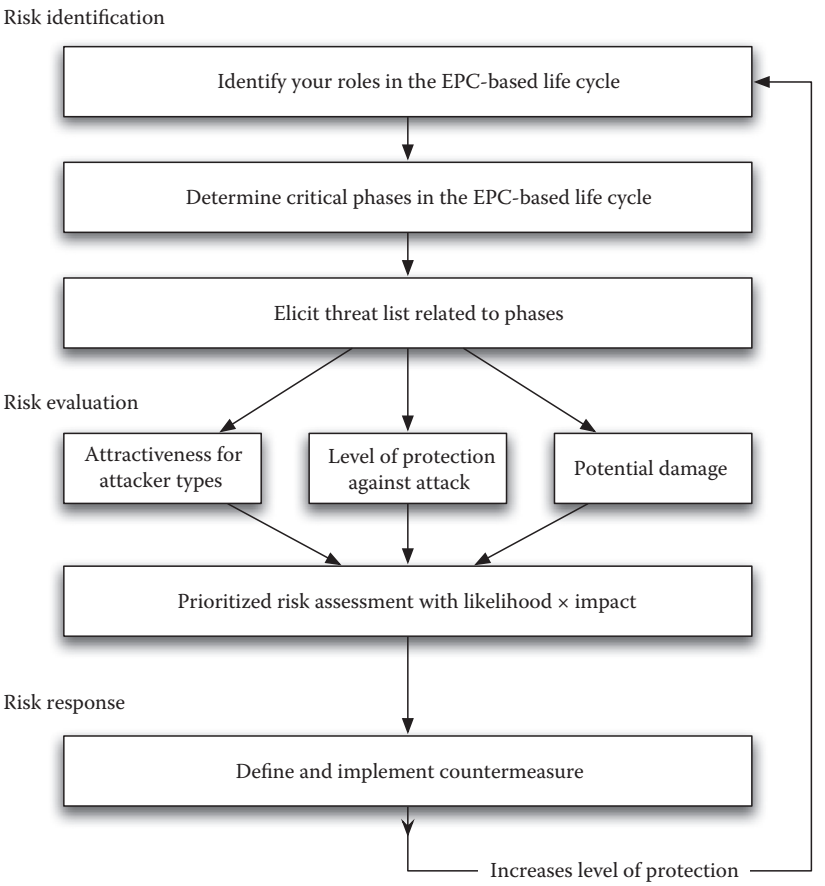

FIGURE 12.3 Threat modeling as basis for security risk management. (Adapted from Hasan, R. et al. Toward a threat model for storage systems, *Proceedings of the 2005 ACM Workshop on Storage Security and Survivability*, ACM Press, New York, 2005, pp. 94–102.)

TABLE 12.2
Summary of the Relevant Context Factors for Risk Identification and Risk Evaluation

Threat Model Elements	Subjective Context Factors	Influence on
Roles	Relevance, goals	Threat exposure, number of risks
Phases	Dependency on others	Threat exposure, number of risks
Attacker characteristics	Attractiveness for attacker	Impact, probability
Attack	Own protection strength	Impact, probability

framework as COSO risk management framework [27]. The objective is to estimate the dimensions of probability and negative impact for each identified threat. The resulting threat list can now be prioritized and visualized with a likelihood/impact diagram [27]. Depending on an organization's risk appetite [27], appropriate risk responses and countermeasures may now be specified. Finally, the implementation of these actions mitigates or prevents the assessed risks and improves the overall risk profile for a given organization.

What is an FMEA?

An FMEA is an risk assessment technique for systematically identifying potential failures in a system or a process. FMEA is normally used within the design phase with the aim to avoid future failures. The objective is to prioritize our security threats according to four criteria: how serious the consequences are, how frequently they occur, how easily the attack can be detected, and how attractive a successful attack is for the attacker. The four criteria, as discussed in Table 12.2, are impact (I), probability (P), threat exposure (T), and ability to control the attack (D).

The four criteria are then associated with a range from 1 (lowest risk) to 3 (highest risk) as discussed in the table below. The overall risk for each threat is then called risk priority number and it is obtained by multiplying the four scores together. In the table below we describe an example of a rating system, the analysis performed at points 3 and 4 will help to identify the correct value for each index.

12.5.2 Threat Analysis Step-by-Step

In the following, we describe each step of Figure 12.3 in detail and relate to the existing frameworks and proven methodologies where possible. In line with the general remarks above, we note that the application of the threat model builds the foundation for the risk identification step. The steps of risk evaluation and risk response are captured here only to provide a sound application example. Actual implementations of risk evaluation and risk response may depend on an organizations practice. The threat model's output, a customized list of threats, is, however, vital for their success. It adds the domain specific threat knowledge required for determining the right actions.

12.5.2.1 Risk Identification

To identify the risk profile of the EPC-based network system is important to analyze the critical operations together with the critical sources of risk within the specific organization's context.

- Identify key roles: The objective is to identify which role an organization takes up for a specific EPC-based information sharing application. This could be one or more of the roles stated in Section 12.3, namely, trace data consumer, trace data supplier, or metadata operator. For example, in an e-pedigree application, a manufacturer could take up only the role of a trace data supplier, whereas a retailer would take up only the role of a trace data consumer. All parties in between might take up both, the roles of a trace data supplier and a trace data consumer.
- Identify critical phases: The objective of this point is to identify which phases of our life-cycle information model if compromised or sabotaged could affect internal and external supply chain operations of the organization. It is likely that components of the EPC-based information sharing networks which are involved in the critical phases are those, where we want to focus our future security investments. A critical phase could be identified by fulfilling one of the following characteristics:
  1. An element of the system on which many others could depend, for example the "trace data announcement" phase where information contained in an EPCIS is needed to enable a timely track and trace for other trading partners.
  2. An element of the system with limited amount of alternatives, for example the phase "trace data retrieval" where the only source of information is a single EPCIS repository. If this repository is compromised, no other way of retrieving the required data is possible.

3. An element of the system that is associated with a high risk environment, for example the phase of "trace data search" where a publicly running web service (e.g., EPCDS) could expose confidential supply chain information without a secure access control mechanism.

12.5.2.2 Risk Evaluation

Rather than evaluating in depth all the possible security risks that a company might face, the threat model analysis helps to isolate the most relevant threats based on the previous steps, the attacker types, and relevant supply chain scenarios. EPC-based networks can be seen as a complex web of interconnected nodes and relationships. The nodes represent components, EPCIS, discovery service, and the links are the means by which information is exchanged—network connection. The security threats represent the risk of failure of these nodes and links and our goal is to identify which combination of these nodes and links are critical.

- Attractiveness for attacker types: How likely is for a certain element of the system to attract a certain type of attack? Where are the protection mechanisms? How much additional capacity is available if the system fall under a DoS attack that consumes system's resources? Traditionally, we could expect that if a component transports valuable information then it represents a high risk element. However, for an EPC-based network the risk of failures for most services does not depend on a single component, for example an e-pedigree service relies on the integrity of a set of supply chain record and an attacker could just decide to perform an action against the weakest link to bring the whole system offline.
- Own protection strength: What are the security mechanisms already in place? Are standard monitoring tools available to warn about security vulnerabilities? Do I have good communication with suppliers and customers to develop a greater understanding of potential vulnerabilities and attacker strategy? Ideally organization needs to be able to react quickly, and protection mechanisms should be reviewed regularly as part of the risk assessment process.
- Internal and external potential damage: Threats identified in step 2 could lead to various damages to internal supply chain processes and logistic operations (roles). The challenge is to isolate the impact of these threats for a specific scenario.
- Risk assessment with likelihood per impact: The purpose of this step is to define where the greatest threats lie. Generally accepted risk management frameworks such as COSO [27] or FMEA [26] can help to quantify the dimensions of individual risks by evaluating the combination of probability and impact. Note that the previously gathered threat domain knowledge with the list of several potential risks is used as an input to them. The output is a prioritized list that reflects the risk estimation of a particular context. A brief description of FMEA is provided in Table 3. A curious reader may refer to Ref. [27] for more details.

12.5.2.3 Risk Response

Once the major threats of the system have been identified and prioritized, we can develop specific countermeasures to mitigate the potential damage of an attack or to prevent an attack nearly completely. At this stage we could also consider to redesign some processes if the probability of occurrence and severity of the attacks are too high. Again it is essential that security issues receive attention on an ongoing basis, the risk identification, and the evaluation task needs to be performed on a regular basis to ensure an appropriate mitigation strategy. Standardization could also play

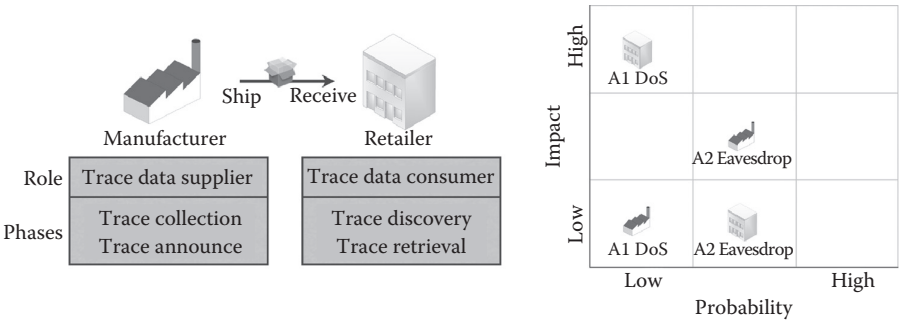

FIGURE 12.4 Example of a fictive two-tier supply chain with the associated threat model roles, phases, and the probability/impact matrix for the selected attacks.

a fundamental role. The EPC global standard will drive for standardization of platforms and components that should reduce the complexity to manage this process across multiple organizations and increase the visibility of potential threats across the chain. However, we should not forget to diversify our technology suppliers, if all components come from the same suppliers it is likely that a single vulnerability could have major effect on our internal system. Access to threat analysis and attack reports from other organization is also another major component that should be considered to mitigate the risk and increase the resilience of our systems. Within a supply chain we should create a collaborative working environment that enables to share relevant information about upstream and downstream threats and that motivate commitment to mitigate and address these security vulnerabilities. The EPCglobal network is already built on these principle and a proposal could then be to provide an extended management of these risks. We will detail this discussion in Section 12.6.

12.5.3 Example of an Interdependent Security Problem

Consider a two-tier supply chain with a manufacturer and a retailer who implement an e-Pedigree application to ensure food traceability. Figure 12.4 shows the scenario put into the threat model context with the corresponding roles and phases. The traceability scenario requires the retailer to verify the pedigree of all incoming objects. Therefore, the retailer is dependent on the availability of the manufacturer's EPCIS database. In contrast, the manufacturer requires confidentiality of the trace data, as the data might be misused by a competitor to reveal shipment quantities between manufacturer and retailer. Figure 12.4 shows the perceived risks for two selected attacks against the life-cycle phase trace retrieval. The attack A1 represents a DoS attack against the EPCIS of the manufacturer and the attack A2 denotes an eavesdropping attack on the data exchanged during trace data retrieval. Although both parties might perceive the probability of the attack realization equally, the impact of the damage can be considerably different (as depicted on the matrix in Figure 12.4). For example, the manufacturer might perceive the potential damage of A1 as low while the retailer would suffer from a high damage potential. The manufacturer is not strongly dependent on the EPCIS availability and therefore such an attack might just consume more bandwidth and traffic costs, but not threaten the business at all. In contrast, the retailer faces process holdups or delays that could cause high costs. The interdependent security problems become apparent when looking at the ability of each party to reduce the imposed risks. For example, the manufacturer can employ encryption and access control to prevent eavesdropping attack A2. However, if the retailer treats security for this aspect loosely and leaks the encryption key to a malicious party, the whole security of the encrypted data traffic is compromised. In conclusion, the security of one party is strongly dependent on the other parties interacting in a certain life-cycle phase.

12.6 DISCUSSION

As illustrated in Section 12.5.3, EPC-based information sharing networks suffer from interdependent security problems. Taking into account that supply networks are rarely as simple as two symmetric partners, this section discusses how to improve the overall collective security of the multipartner supply chain community. Even though the threat model does not claim completeness, it provides a structured and practical way of assessing risk exposure for individual parties, along with an assessment of risk that they place on other parties and the recompense that they can expect for removing those threats. Different risk perceptions are the source for unbalanced motivations for investing in security. If, for example, the costs of security are higher than the risks against that partner in isolation then clearly no partner will ever invest in security, regardless of the behavior of its partners. However, if the costs of security are less than the internal risks combined with the external benefit to other partners, then there exists another equilibrium where all partners can benefit from the combined investment in security. The problem is therefore to convince all parties in the system to move to this beneficial collaborative equilibrium. There are several options to achieve this goal. In the following, we discuss cooperative, noncooperative, and externally motivated solutions. In a cooperative approach, organizations would share their views on threat probabilities and especially threat impacts. The threat model would be used for a joint risk assessment with a bilateral understanding of the risks and attractiveness for certain attacker types. The result could be a joint action plan for protecting identified critical points. In a noncooperative approach, organizations would assess and implement security measures based on their own risk perceptions. Each party would be held accountable for the losses of other parties resulting in the failure of its security measures against previously set critical points. These points and penalties are usually coordinated through contracts such as SLAs. Simpler market mechanisms may include the choice of whether to do business with a trading partner, knowing that our organization will be exposed to uncontrolled risks. A business may chose only to do business with partners who can show compliance to a security accreditation, technical standards, and business practices. With supply chain, wide contracts, the benefits of proper security investments to external parties can be internalized, making a decision to implement security straightforward for every party. Therefore, we reason that a secure EPC-based information sharing system must include clear accountability. Such accountability can include records of who submitted trace data, along with who accessed data, and for what purpose. Data may be signed as proof-of-origin, and systems provided to ensure nonrepudiation of trace data, only when implementing proper accountability, incentives, or penalties can be applied effectively. In externally motivated solutions, coordinating bodies, such as an industry consortium or government agency, can be used to encourage the implementation of security across all partners. This can be achieved through different means such as subsidies for implementing security, fines for failure to adopt industry standards, and even regulation. In such circumstances, regulation can be in the interests of all the parties because it forces a multilateral move toward security. Again, accountability is a key property of the technical solution to allow for implementing this approach. Based on the threat model, we reason that the shared motivation to implement secure trace data systems is not sufficient without the tools to implement security, and the ability to gain assurance that supply chain partners have also done so. Security does not stop at the product selection and integration, but continues with the business practice. Regular audits from external trusted agencies can ensure that trace data partners continue to operate their business to manage the risks that can be introduced to their partners' supply chain processes. Technology can assist with the accountability of trace data operations, preventing many attacks and ensuring that others can be traced and corrective action taken to reduce future threats. The above discussion has largely been around the motivations of the trace data supplier and trace data consumer relationships to implement security; however, there are other parties within a trace data network that must also be considered. Parties such as the trace data operator (implementing the EPCDS) must consider both the trace data suppliers and trace data consumers that it works with. In this case, however, it is expected

that security failures will result in internalized losses through the breach of SLAs, and the loss of business to other trace data operators.

12.7 CONCLUSION

The objective of this chapter has been to provide a tool to identify and prioritize potential risks associated with EPC-based information sharing networks. We developed a general trace data information life-cycle model that allows further tailoring to specific organizations. We introduced threat modeling as a basis for individual risk management and outlined factors that should be considered within each life-cycle stage to analyze the threat. These factors include the role performed during the life-cycle phase, attractiveness for certain attacker types and the protection strength of the implemented system against specific attacks. We then discussed some guidelines to be able to actually use the proposed threat model as a basis for risk management on a specific context. The context allows for determining the individual threat exposure depending on the roles and phases of the life-cycle model. We focused on the fact that when tailoring the threat model to a specific context, the interdependent nature of the security risks become apparent. For the fictive example of a retailer and manufacturer, we show the magnitude of one's risks is strongly dependent on the actions of the other party. With increasing complexity of supply chains, the interdependent security risks become pervasive and require a supply chainwide solution. Therefore, we discussed the potential to mitigate the interdependent security problems by cooperative risk assessment, market mechanisms such as contractual incentive design, and external enforcement.

Our findings suggest that designers, operators, and users of EPC-based information sharing networks should focus on providing accountability as a key to improve collective security. Technical accountability mechanisms within standardized security frameworks are essential to the enforcement of service contacts or regulatory practices and are also essential to identify the root of any attack and remove future threats. In addition, because security incidents are not completely preventable, the issue of recovery has major practical relevance. For example, how long does it take until a network can recover from a compromised digital signature key? As EPCglobal-based information sharing networks support business processes, they not only need to focus on how to manage the security risks, but also how quickly they can recover and restore operations.

We highlight that future research is needed to investigate the role of security frameworks and contractual design for making interdependent security problems explicit and their resolution more efficient.

REFERENCES

[1] H. L. Lee and O. Ozer, Unlocking the value of RFID, Graduate School of Business, Stanford University, Working paper, 2005.

[2] A. D. Smith, Exploring the inherent benefits of RFID and automated self-serve checkouts in a B2C environment, *International Journal of Business Information Systems*, 1, 2005, 149–181.

[3] T. Staake, F. Thiesse, and E. Fleisch, *Extending the EPC Network: The Potential of RFID in Anti-Counterfeiting*, ACM Press, New York, 2005, pp. 1607–1612.

[4] K. Traub et al., The EPCglobal architecture framework, EPCglobal Final Version, 2005.

[5] H. Kunreuther and G. Heal, Interdependent security, *Journal of Risk and Uncertainty*, 26, 2003, 231–249.

[6] A. Juels, RFID security and privacy: A research survey, *IEEE Journal on Selected Areas in Communications*, 24, 2006, 381–394.

[7] F. Thiesse, RFID, privacy and the perception of risk: A strategic framework, *Journal of Strategic Information Systems*, 2007.

[8] G. Avoine and P. Oechslin, RFID traceability: A multilayer problem, *Financial Cryptography and Data Security*, 2005, 125–140.

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

[10] T. Karygiannis et al., *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, Special publication, National Institute of Standards and Technology, 2007, pp. 800–898.
[11] Security Aspects and Prospective Applications of RFID Systems, Federal Office for Information Security, Bonn, Germany, 2004.
[12] M. Aigner et al., D-4.1.1: Security analysis, A. Ilic, Ed., *Building Radio Frequency IDentification for the Global Environment (BRIDGE)*, 2007.
[13] D. M. Konidala, W.-S. Kim, and K. Kim, Security assessment of EPCglobal architecture framework, Auto-ID Labs White Paper Series, WP-SWNET-017, 2006, Auto-ID Labs, Available from http://www.autoidlabs.org.
[14] R. Anderson, Why information security is hard—An economic perspective, *Computer Security Applications Conference*, *Proceedings of the 17th ACSAC*, 2001, pp. 358–365.
[15] R. Anderson and T. Moore, The economics of information security, *Science*, 314, 2006, 610–613.
[16] R. Bernard, Information lifecycle security risk assessment: A tool for closing security gaps, *Computers & Security*, 26, 2007, 26–30.
[17] R. Hasan et al., Toward a threat model for storage systems, *Proceedings of the 2005 ACM Workshop on Storage Security and Survivability*, ACM Press, New York, 2005 pp. 94–102.
[18] M. Bauer et al., Emerging markets for RFID traces, Arxiv preprint cs.CY/0606018, 2006.
[19] D. M. Nicol, Modeling and simulation in security evaluation, *IEEE Security and Privacy*, 3, 2005, 71–74.
[20] S. E. Schechter and M. D. Smith, How much security is enough to stop a thief. *Proceedings of the Financial Cryptography Conference*, Guadeloupe, Springer, January, 2003.
[21] T. Moore, Countering hidden-action attacks on networked systems, *Proceedings of the Fourth Workshop on the Economics of Information Security*, 2005.
[22] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, Is your cat infected with a computer virus? *IEEE Computer Society*, 2006, 169–179.
[23] Y. Y. Haimes, *Risk Modeling, Assessment, and Management*, John Wiley & Sons, 2004.
[24] S. Evans et al., Risk-based systems security engineering: Stopping attacks with intention, *IEEE Security & Privacy Magazine*, 2, 2004, 59–62.
[25] S. Myagmar, A. J. Lee, and W. Yurcik, Threat modeling as a basis for security requirements, *Symposium on Requirements Engineering for Information Security (SREIS)*, 2005.
[26] D. Bell, L. Cox, S. Jackson, and P. Schaefer, Using causal reasoning for automated failure modes & effects analysis (FMEA). *IEEE Annual Reliability and Maintainability Symposium*, 1992, pp. 343–353.
[27] Enterprise risk management—Integrated framework, American Institute of Certified Public Accountants, 2004.