International Journal of
Engineering in Computer Science

E-ISSN: 2663-3590
P-ISSN: 2663-3582
IJECS 2023; 5(1): 15-18
Received: 15-10-2022
Accepted: 30-11-2022

Seyfali Mahini
Islamic Azad University, Khoy Branch, Khoy, Iran

Correspondence
Seyfali Mahini
Islamic Azad University, Khoy Branch, Khoy, Iran

Early model-based risk analysis for mobile, distributed applications

Seyfali Mahini

DOI: https://doi.org/10.33545/26633582.2023.v5.i1a.83

Abstract
Applications that include mobile components are exposed to particular risks. For example, communication in mobile, distributed applications poses a challenge in terms of data security and security against eavesdropping. A separate protection requirement analysis is therefore required in the context of these applications. Using the example of an information system with mobile connected clients, this article shows how a consistent security and risk analysis can be integrated into the model-based development process of such a system. Possible weaknesses in the system can thus be identified and eliminated in the early development phases.

Keywords: Early model, mobile, components

Introduction

Until a few years ago, it was unthinkable that mobile phones, for example, could be used for anything other than making calls. Smartphones, tablet PCs and other mobile end devices are increasingly being integrated into complex IT systems and business processes. Of course, with these new opportunities come new risks. While a locally limited system can be adequately and reliably protected against attacks and failures, mobile, distributed systems face new challenges, for example when sensitive data leaves the secure company network [Eck06] [2]. The transmission of data from/to a field worker can, for example, be protected by suitable encryption. However, the fact that if the device is lost/stolen it can fall into the wrong hands or that the stolen device itself represents a point of attack for the company's IT, is often not taken into account. The above risks and security gaps can already be counteracted in the planning phase of an IT system. A risk in the sense of this work is a security-relevant vulnerability of a computer system or the insufficiently secured communication between them. The security of software systems should already be taken into account in the planning phase, since it is very difficult or impossible to enforce security guidelines afterwards. Especially with model-driven development methods, the existing software models offer a good basis for the first well-founded risk and safety analyses. Based on the existing work on model-based safety and risk analysis (Section 2), we propose a new methodology in the following, with which corresponding analyzes are already possible in particularly early planning phases, i.e. long before the detailed software design, where compliance requirements are also taken into account. The core of our methodology (Section 3) is the integration of business processes, e.g. available as BPMN models [FR10] [3], and the planned distribution to various system components, e.g. with UML deployments [OMG05] [9]. Fundamental risks can already be localized on the basis of these simple models, as we will show using the example of an IT system for direct sales. Finally, we discuss the proposed methodology and open research questions (Section 4).

Existing approaches

Various approaches to model-based safety analysis already exist. Two well-known examples for specifying security requirements in software models are UML sec [Jur04] [6] and Secure UML [LBD02] [8]. While Secure UML is an extension of UML for access management and control (RBAC), UML sec also enables the specification numerous other security properties in UML models. Existing tools allow an automated check of these properties, e.g. through consistency checks. An application of UML sec for the analysis of mobile devices has already been shown in [Bar06] [1].

The first tools also exist for general IT risk analysis. An example is the Risk Finder, which examines UML models for safety-relevant vocabulary and highlights possible sources of danger or risks [PHJB11] [10]. Schneider propose in [SKH+11] [11] a heuristic search that performs security analyzes based on Bayesian filters. HeRA provides a feedback-based approach to security testing during requirements analysis [KLM09] [7]. Although the approach provides powerful rules that also work on the vocabulary used, these always refer to single words and do not include text databases.

There is also an approach in [Wol08] [13] to represent security requirements in BPMN models. However, these relate to the presentation of security measures in a closed system. The approach presented in this work also takes into account the later distribution of the software components.

Early model-based safety and risk analysis

Process modeling languages, such as BPMN, are used to visualize business processes or workflows. For example, documents or information that are exchanged during a process can be modeled. Various actors involved in a process can be represented by so-called swimlanes. Business process models are usually already available before an IT system is created, especially if the system is to be implemented to support these processes.

UML deployment diagrams can be used to plan which program components are distributed to which parts of the system (particularly hardware). However, the focus here is not on the fine-grained distribution of individual artifacts, but on the basic structure (rough draft) of a system. For example, it is identified that there will be tablet PCs for field workers. We can therefore assume that BPMN models and UML deployment diagrams are already given in very early development phases.

Example: Figure 1 shows an example based on the ordering process of the fictitious direct sales company Eisfrost. An order can either be carried out immediately if the desired goods are in the vehicle, or reserved for the next tour by the sales driver. The associated deployment diagram shows the system structure. This is only a possible draft of the system and does not yet represent the final architecture. The sales driver uses a tablet PC for the customer's order on site to select the customer data and take the order. The tablet PC communicates with the Central Car Unit (CCU) in the vehicle via Bluetooth. The CCU handles communication with the Enterprise Resource Planning (ERP) system at the company headquarters, to retrieve the customer data and to check the customer's creditworthiness before the execution of the order. The result of the check is then sent to the sales driver's tablet PC, which, based on the data, decides whether to carry out the ordering process or cancel it.

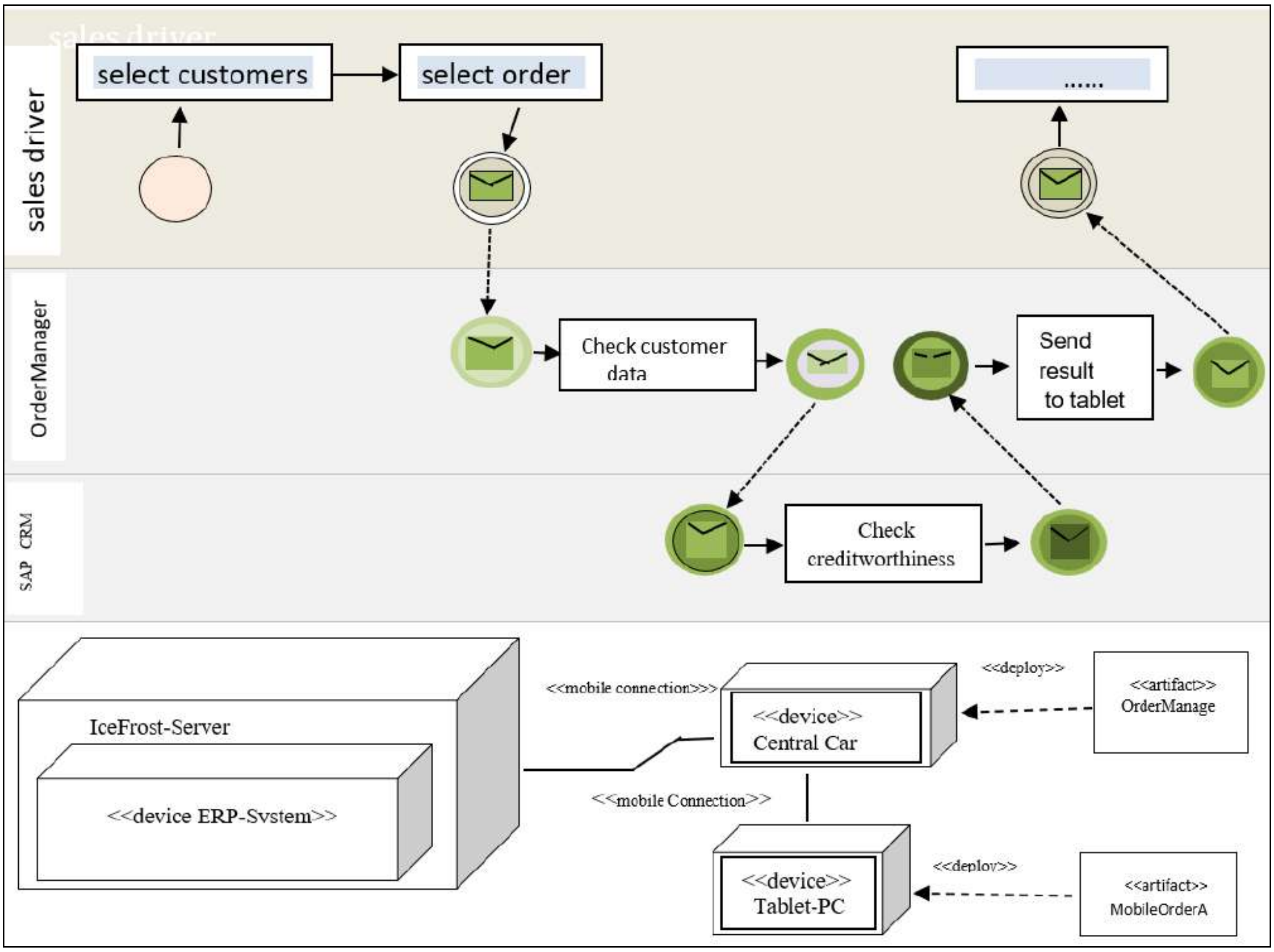

Fig 1: Example of customer data retrieval by a mobile system from the central server

Method: The example shown above contains some risks and security issues that can be uncovered with a systematic analysis. The procedure proposed here for examining the models essentially consists of three steps:

1. Examination of the (physical) distribution
2. Study of communication
3. Analysis of (functional and non-functional) risks

The individual steps will be considered in more detail below.

Investigation of the distribution: The distribution of the components involved in physical systems is of central importance for the security of a system. Mobile components in particular are subject to hazards that do not apply to stationary systems. For example, mobile systems can be lost or stolen. Eavesdropping on or manipulating the communication of the mobile components also represents a significant risk. The distribution of the system can be identified using deployment diagrams.

As soon as the classification has been determined, the components of the deployment diagram can be assigned to the actors of the BPMN diagram. For the components and actors that require increased attention with regard to their danger, it is advisable to visualize them accordingly in order to direct the focus to them.

The assignment of actors from the BPMN model to the components of the deployment diagram can be done in the form of a simple table. An example of the scenario shown in Figure 1 can be seen in Table 1. With the help of this assignment it is possible to generate a combined view of business process and distribution diagram and to carry out the security analysis on it.

Table 1: Allocation of the actors in the business process to the components of the distribution diagram

Business process	Distribution diagram
SAP CRM	Eisfrost-Server/ERP-system
Order Manager	Order Manager
Sales driver	Mobile Order App

Study of communication: The different types of communication are also important features, since they can be exposed to different risks. These can also be extracted from the deployment diagram. A possible example is the division of communication links into radio, local network and Internet. This means that it is also clear which communication medium is used for message exchange. The communication channels that are particularly worthy of protection can then also be visualized.

The <<Secure Links>> stereotype exists in UML sec for this purpose. With this, security requirements for data transmission are demanded. Each connection between two nodes can then be annotated with the respective line type, e.g. <<Internet>> or <<encrypted>>. The transmitted data can, for example, be marked as secret (<<secrecy>>), so that an automatic check can be made as to whether a connection is suitable for the corresponding data [Jur04] [6].

The example shows that there is wireless communication between the tablet PC and the CCU and thus also with the ERP system. In order to manifest this need for protection in the model, we propose an extension for BPMN that is defined analogously to UML sec. However, it is not primarily about the specific type of communication, but rather about the type of data that is to be transmitted. For example, in the case of personal data, this should be annotated accordingly in the BPMN model, in that the message flow can be provided with a special type of text annotation, the semantics of which can be analogous to a UML sec stereotype. With this extension, protection requirement analyzes can then also be carried out directly on the business process model.

Analysis of the risks: In the previous two steps, threats resulting from the distribution of the system and its communication were considered. However, there are other risks due to the activities themselves, which we want to make possible to identify as follows.

Based on established IT security standards, e.g. the catalogs and standards of the Federal Office for Information Security (BSI) and the ISO standards of the 27000 series [ISO05] [5], security-related activities can be identified by analyze the vocabulary of each activity. The Risk Finder can be used for this [PHJB11] [10]. However, we propose an abstraction from concrete notations. A process to be examined consists only of a set of (independent) activities, each of which is assigned a set of texts. In the usual notations, these are the titles of activities and any additional comments. This is particularly suitable for the investigation of business processes, where a large number of formal and semi-formal notations are used [Fra11] [4]. If a risk can be assigned to an activity, it can be marked accordingly.

In addition, critical structures in the process resulting from the lack of activities can also be uncovered. In the example presented, no separate authentication is required when the customer's data is transmitted. It must therefore be assumed that the login is implicit and that the access data required for this is stored in the device. If the tablet PC or the CCU is lost, e.g. through theft, it is therefore possible to access company data without logging in accordingly.

Furthermore, the risk analysis can support the previously considered investigation of communication. For example, messages triggered by activities that process sensitive data can themselves be marked as critical.

Discussion and open research questions Risk and security

Analysis is an essential step in the development of information systems. New risks arise particularly with mobile, distributed applications. In this paper, we have proposed a new method for model-based analysis of such systems, which can already be applied to early-stage documents such as process models and rough UML deployment diagrams.

As a rule, the business process models should already exist and distribution diagrams can also be designed without a great deal of detailed knowledge. However, our proposal is not limited to BPMN models. For the pure risk analysis, the identifiers of the process steps/activities alone are sufficient. The current version of the RiskFinder is currently being revised so that other data sources are also possible. In addition, we integrate text databases for the evaluation, e.g. of synonymous and co-occurring terms, so that the hit rate is made even more precise.

An advantage of our approach compared to the existing ones is that the security patterns are applied systematically to the activities found, thus enabling a comprehensive security analysis.

Another necessary extension of the Risk Finder is to detect the non-existence of certain properties (see the missing login information in the example). This is not a trivial problem since a negated search for keywords is not sufficient. Rather, the context of the non-existence must be considered in order not to generate too many false reports.

The investigation of communication has already been realized for UML design models [Jur04] [6]. As shown above, the concept can be easily transferred to business processes. Here it is still necessary to evaluate more precisely how the information on the protection requirements of messages can be meaningfully integrated into the models. There are no extension mechanisms analogous to UML stereotypes in BPMN, the annotation elements could possibly be an option for this. In addition, a suitable heuristic has to be designed with which the Risk Finder proposes the need for protection for data transfers. In particular, transitivity properties still need to be discussed, since it is not always clear which information from a process step is used in later steps. Finally, a corresponding tool support for the consistency check between the protection requirements of the messages and the communication channel used is to be implemented.

Overall, the tool support should be improved so that an integrated tool is available. We are thinking of an integration into the CARiSMA analysis tool in order to offer the user a holistic view. There is still a need for a suitable graphical user interface.

It would also be interesting to discuss how the approach scales into existing scenarios where business process models are used for orchestration. A related approach to this topic has already been mentioned in [Men09] [12].

References

1. [Bar06] Barman P. Model-based security analysis of mobile devices. Dissertation, Technical University of Munich; c2021
2. [Eck06] Eckert C. IT security. Oldenburg; c2022.
3. [FR10] Freud J, Rucker B. Practice Manuel BPMN 2.0, Jgg. 2. Carl Hanser Publisher; c2021.
4. [Fra11] Fraunhofer IAO. Business Process Management Tools 2021. Fraunhofer-IRB-Publisher; c2021.
5. [ISO05] ISO. ISO27001: Information Security Management System (ISMS) standard; c2020.
6. [Jur04] Jurjens J. Secure Systems Development with UML. Springer, 1. Edition, 11; c2020.
7. [KLM09] Knauss E, Lubke D, Meyer S. Feedback-driven requirements engineering: The Heuristic Requirements Assistant. ICSE' 09.
8. [LBD02] Lodderstedt T, Basin DA, Doser J. SecureUML: A UML-Based Modeling Language for Model-Driven Security. UML 2021. Springer-Publisher.
9. [OMG05] Object Management Group. Unified Modeling Language Specification v2.0; c2022.
10. [PHJB11] Peschke M, Hirsch M, Jurjens J, Braun S. Tool-based identification of IT security risks; c2021
11. [SKH+11] Schneider K, Knauss E, Houmb S, Islam S, Jurjens J. Enhancing security requirements engineering by organizational learning. Requirements Engineering; c2022.
12. [Men09] Michael Menzel, Ivonne Thomas, Christoph Meinel. Security Requirements Specification in Service-Oriented Business Process Management. ARES; c2021.
13. [Wol08] Christian Wolter, Michael Menzel, Christoph Meinel. Modelling Security Goals in Business Processes. Modelling; c2020.