

Security related BPMN-extensions for RPA

Anastasiya Kurylets*, Nikolaj Goranin
Vilnius Gediminas Technical University, Lithuania
anastasiya.kurylets@vilniustech.lt

Abstract: Direct Robotic process automation (RPA) has received a lot of attention because of the increasing demand for solutions to improve the efficiency of business processes in an organization. With RPA, organizations can develop robots that automate a large number of processes. However, despite its relevance, RPA is a relatively young field and many of its concepts remain open to discussion. One of the primary tasks in creating a robot is the identification of threats at the design stage, which reduces the number of possible attacks, identifying vulnerabilities, thereby increasing the security of the robot itself. The increasing use of RPA-based solutions in mission-critical systems has created a need and interest in assessing their threats. The foundation for successful creation, launch and use of a secure RPA-based solution would be application of classical design techniques and evaluating the risks on all SDLC cycle stages. But in order to perform this appropriate tools taking into consideration the specific nuances of the domain area are needed. BPMN notation, used for describing business processes can be seen as a good candidate for designing RPA solutions. However, BPMN is not able to cover the description of all aspects in the robot process, namely, issues related to the specifics of RPA security remain unaccounted for. This study analyses business process notation (BPMN) as a modelling tool for the design of automated processes in RPA, proposes an approach for defining security-related extensions of BPMN using its own extension mechanism, that can be used for risk analysis on different SDLC stages.

Keywords: RPA, BPMN-EXTENSIONS FOR RPA, SECURITY RPA, THREATS OF RPA.

1. Introduction and problem discussion

Robotic process automation (RPA) is the use of scripts and software algorithms to efficiently and safely automate repetitive and routine tasks that are typically performed by company employees.

Before integrating software, it is important to have a good understanding of robotic process automation. In small companies, the process of robotization is usually quite simple: an analyst describes the process, and then RPA is implemented. In large companies, things are much more complicated. Using BPM, it is necessary to identify processes suitable for robotization, evaluate the effectiveness and potential of robotization, develop an algorithm and launch the robot.

Therefore, a structured modeling language is essential for mapping concepts related to the implementation of a robot.

A common solution for process modeling, including robotization steps, is to apply traditional business process modeling methodologies. There are several standard business process modeling languages.

Business Process Model and Notation (BPMN) is considered to be one of the major standards among others. BPMN was developed by the Business Process Modeling Initiative (BPMI) and is now adopted by the Object Management Group (OMG), which provides a business standard for representing business processes or procedures using graphical notation. It covers business functions of an organization by modeling the interaction between different departments and processes. However, it does not provide any mechanisms to show the security requirements of these processes, which is the main concern of today's IS. There are goal-based and threat-based approaches to analyze the security requirements. The goal-based approach is an abstract approach that highlights the goals that can be achieved and includes all threats underlying the goal. While the threat-based approach is more detailed and analyses-specific threats define security requirements [1]

Traditionally, security requirements are considered only after defining the business process. However, this will inevitably increase the vulnerability of the system due to the functional behavior of the system and security is usually are not independent of each other. It calls for security experts cannot get enough feedback on the system safety requirements. Therefore, security must be not only considered at a technical level, but also at an abstraction the level at which the business process was first defined.

This study analyzes business process notation (BPMN) as a modeling tool for the design of automated processes in RPA, proposes an approach for defining security-related extensions of BPMN using its own extension mechanism, that can be used for risk analysis on different SDLC stages.

2. Objective and research methodologies

An analysis of the modeling of conduct cases on the use of RPA made it possible to determine that the most common type of attack is spoofing, due to the presence of a large amount of data exchange. Data leakage and theft are the two main threats. Critical data, such as passwords of RPA bots or consumer data processed by RPA, can be accessed by attackers if the appropriate security measures are not taken[2].

Also, conducted threat analysis using RPA shows that the cybersecurity risks associated with implementing RPA are not much different from the traditional cybersecurity risks that are commonly encountered when working with other systems (fig.1).

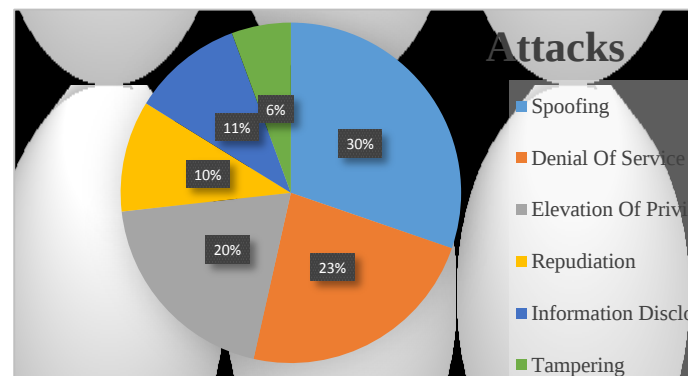


Fig.1 Type of attack in cases using RPA.

However, you should pay attention to the presence of specific threats that are unique to RPA systems. To visually display up-to-date information, a security ontology for RPA was created [3].

To create the security related BPMN-extension, deliberate non-physical threats to the RPA were used from the ontology(fig.2).

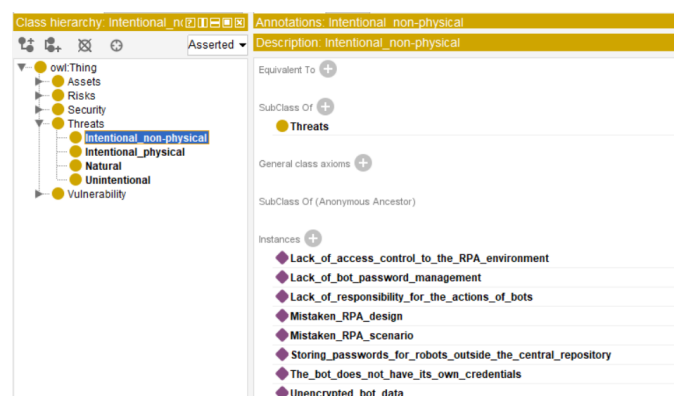


Fig.2 Non-physical threats to the RPA.

The next step was the development of the BPMN diagram, for this was used Bizagi Modeler 3.8.

Was create the case «Contract management process». The "gear" icon marked blocks that can be robotized(fig.3).

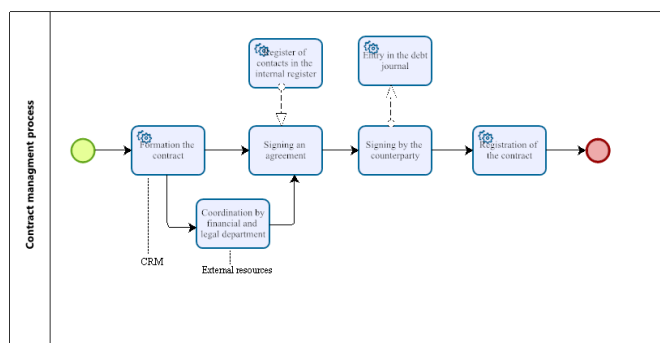


Fig.3 Case «Contract management process».

Table 1 lists the design of the new extended notations.

Table 1. Extended elements for security requirements

Element	Design
Retracing data in unsafe location	
Data leakage (credentials)	
Unencrypted bot data (own credential)	
Data change	
Third party access	
Generates consistent logs	
Lack of access control to the RPA environment	
Changing data in a robot report	
Mistaken RPA script	
Lack of bot password management	

Further, it was necessary to add the developed set of extensions to the Bizagi Modeler tool for its further use. Extensions were added as new custom artifacts (fig. 4).

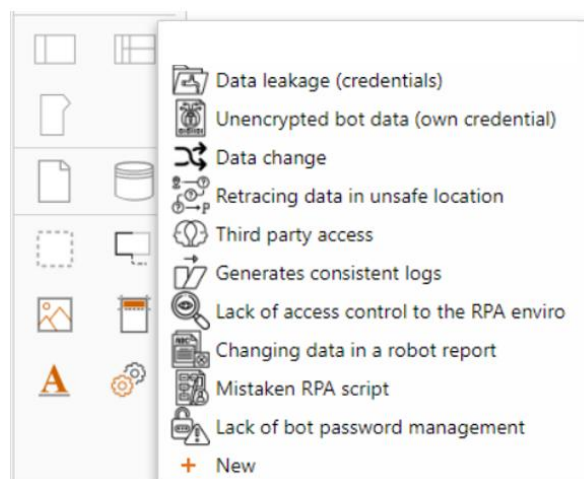


Fig.4 Custom artifacts.

In Figure 5 we demonstrate an extended version of the BPMN diagram with the help of our newly designed security elements for representing the security requirements within BPMN. There are several security requirements that are demonstrated here.

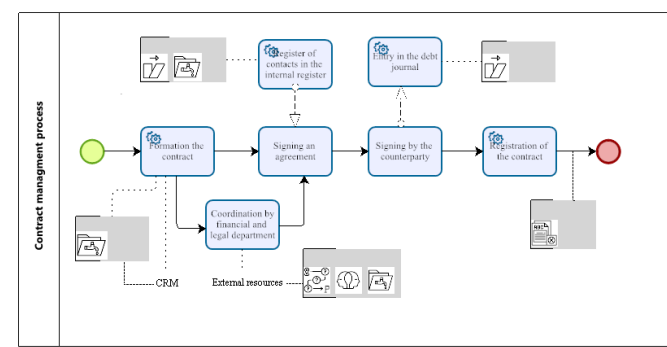


Fig.5 Case «Contract management process».

The issue of safety in the application of RPA technology is becoming increasingly relevant. This is critical for reflecting safety requirements in the conceptual business process flow, which is a preliminary step in the development of a robot.

In this article, we extend the BPMN standard to accommodate Security Requirements in the first place. It provides an opportunity to improve and increase security awareness in RPA. A set of security extensions is implemented in Bizagi Modeler as a custom artifact. The usage of the security extensions are illustrated with a simple an example of the contract management process.

3. References

1. Y. Cherdantseva, Ph.D. Thesis, Cardiff University, Wales, UK, Secure* BPMN—a Graphical Extension for BPMN 2.0 Based on a Reference Model of Information Assurance & Security, (2014)
2. Kurylets A., Goranin N., Threat modeling in RPA-Based systems., DOI, 10.15388/DAMSS.13.2022. ISBN, 9786090707944, (2022)
3. Kurylets, A., Goranin, N., Security Ontology OntoSecRPA for Robotic Process Automation Domain, Appl. Sci. 2023, 13, 5568, (2023)