Threat Modeling in RPA-Based Systems

Anastasiya Kurylets, Nikolaj Goranin
Department of Information Systems, Faculty of Fundamental Sciences, Vilnius Tech

Introduction

Robotic process automation (RPA) is the use of scripts and specialized software to efficiently automate repetitive and routine tasks that are usually performed by company employees. As any new technology, RPA has a number of potential cybersecurity weaknesses, caused ether by fundamental logical mistakes in the approach, or by cyber-human mistakes made during the implementation, configuration and operation phases. It is important to have an extensive understanding of the related risks before RPA integration into enterprise IT infrastructure.

The main asset operated by RPA **is confidential enterprise data.** Data leakage and theft are **the two main threats**. **The main risks** associated with the integration of robotic process automation can be divided into two groups: **Compliance risks** and **Operational risks**.

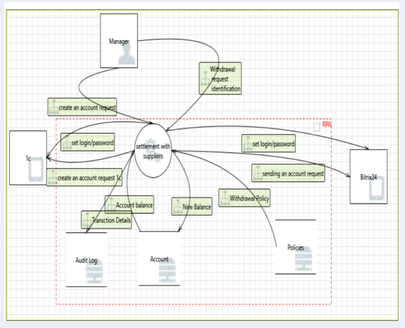
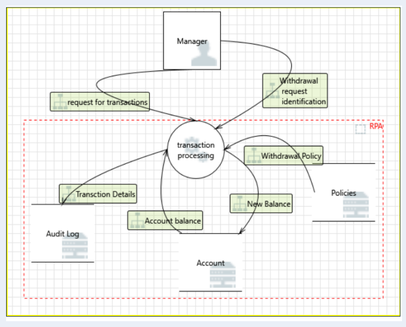
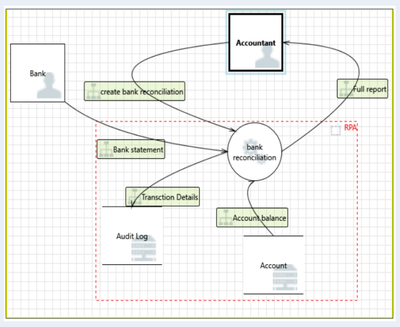
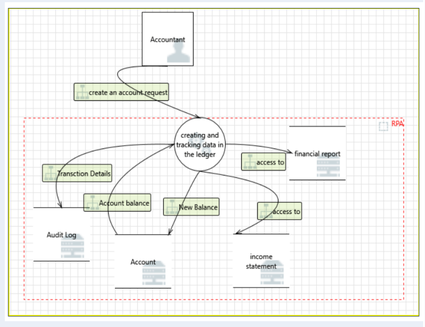
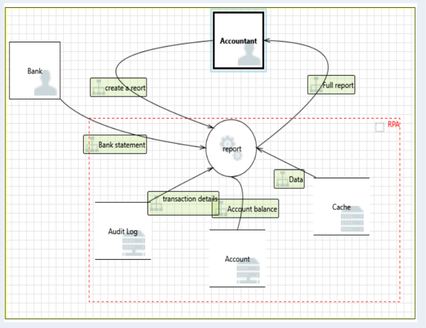
Root causes for RPA security risks:

- *Confidential data*, such as consumer data processed by RPA, can be accessed by attackers if appropriate security measures are not taken.
- *Credentials* for automating robotic processes are usually remain unchanged and unprotected. A cyber attacker can hijack them, use them to elevate privileges and quickly gain access to systems and data.
- *RPA passwords* are often exchanged in a plaintext. A cybercriminal can intercept these accounts and passwords, use them to elevate privileges and transfer data in other directions to gain access to confidential networks, software and data.
- Passwords can be extracted by malicious insiders or system administrators.

Classical risk management approach suggests that before *finding the countermeasures* it is necessary to *identify the existing threats and risks*. One of the methods for doing so is a **threat modeling**. The information security threat model is a description of existing threats, their categories, and the possibility of increasing or decreasing the threat priority. The threat modeling tool is a key element of the development lifecycle of secure applications. It allows developers to identify and fix potential security issues at an early stage. Still, despite the RPA security topic importance and notoriety of threat modeling approach in cybersecurity not too much research is being done.

In this research we present threat modeling for RPA case scenarios in the financial sector. Microsoft Threat Modeling Tool was used as a threat modeling tool. The construction of case models made it possible to identify risks, the categories to which they belong, their description with the possibility of raising or lowering the priority of the threat, analyze trust boundaries for software robots on real samples.

Threat Modelling in RPA Based Systems

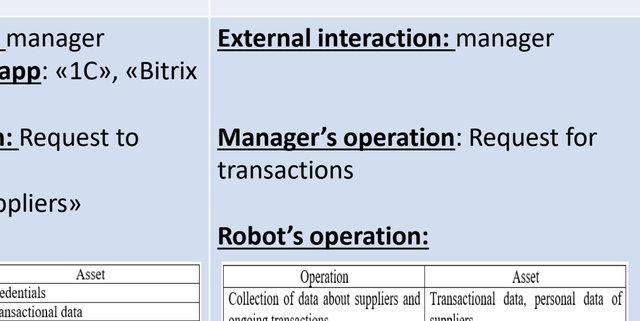
Case name	Settlement with suppliers	Carrying out a transaction	Bank reconciliation	Creating and tracking data in a ledger	Providing reports
Description	To pay with suppliers, you must create a request in «1C» "Payments with suppliers". Authentication in «1C» is carried out using the data of the robot. This is followed by work related to the use of the robot, it is necessary to verify the supplier's transactional data, check the balance of expenses, obtain permission from the expense manager - withdraw funds. Opportunity check in the Bitrix24 system.	To conduct a transaction, the manager needs to create a request for this operation. From the side of the robot, the following set of actions takes place: it is necessary to verify the details for payment in the existing data warehouse, access the bank account for subsequent payment, adhering to the withdrawal policy, and obtain permission to pay.	To perform bank reconciliation on the part of the robot, you must perform the following tasks: send a request to the bank to receive a bank statement. In the log of records, track ongoing transactions by comparing them with a bank statement. After generating the report, submit it to the accountant.	The scope of the robot's responsibility includes access to ongoing transactions, the ability to work with a bank account, income and expenditure transactions, which leads to entering and changing data in the ledger, as well as generating a report based on the above operations.	Providing reports in the prescribed form involves interaction with several external sources, handling confidential data. In this case, the operations assigned to the robot are as follows: extracting information from a bank statement, managing transaction data, bank account information and other internal company data of a commercial nature.
Diagram					
Definition	**External interaction:** manager **External interaction app**: «1C», «Bitrix 24» **Manager's operation:** Request to create in«1C» «Settlement with suppliers» **Robot's operations:** Operation / Asset Authentication in «1C» / Credentials Vendor invoice reconciliation / Transactional data Bank account balance reconciliation / Account access, data Payment / Cash Authentication in «Bitrix24» / Credentials Saving a payment receipt / Data	**External interaction:** manager **Manager's operation**: Request for transactions **Robot's operation:** Operation / Asset Collection of data about suppliers and ongoing transactions / Transactional data, personal data of suppliers Bank account access / Account, data Payment / Cash	**External interaction**: bank, accountant **Accountant's operations:** Transaction Request **Robot's operations:** Operation / Asset Access and analysis of ongoing transactions / Transactional data, personal data of suppliers Bank account balance reconciliation / Account access, data, bank statement Payment / Cash	**External interaction:** accountant **Accountant's operations:** Transaction Request **Robot's operations:** Operation / Asset Collection of data about suppliers and ongoing transactions / Transactional data, personal data of suppliers Bank account balance reconciliation / Account access, data Payment / Cash	**External interaction:** bank, accountant **Accountant's operations:** report request **Robot's operations:** Operation / Asset Receipt of internal data / Company personal data Bank account access / Account data, cash Extracting data from a bank statement / Data Collection of data on ongoing transactions / Transactional data
Attack Analysis Using the Microsoft Threat Modeling Tool	12 - Spoofing 10- Denial Of Service 6 - Elevation Of Privilege 6- Repudiation 4 - Information Disclosure 2- Tampering	9 - Spoofing 6- Denial Of Service 7 - Elevation Of Privilege 2- Repudiation 4 - Information Disclosure 2- Tampering	7 - Spoofing. 6- Denial Of Service 6 - Elevation Of Privilege 3- Repudiation 3 - Information Disclosure 2- Tampering	7- Spoofing. 6- Denial Of Service 3 - Elevation Of Privilege 1- Repudiation 2 - Information Disclosure 1- Tampering	8 -Spoofing 5- Denial Of Service 6 - Elevation Of Privilege 3- Repudiation 5 - Information Disclosure 2- Tampering

Problem Relevance

To protect systems based on the use of RPA technology, it is necessary to carry out a **risk assessment**. To do this, it is proposed to create a threat model that will clearly demonstrate the possible risks of using this system: threats with their detailed description, the possibility of raising or lowering the risk priority. For example, change from high to low if we estimate that the damage caused is insignificant for the company.

However, defining countermeasures for RPA-based systems is not an automatic feature in existing modeling tools. It is necessary to analyze the types of threats in the proposed cases, comparing them with standard sets of information security threats. Determine the specifics of using RPA in systems, what types of threats it entails. Develop a list of countermeasures when applying RPA.

Results and Discussion

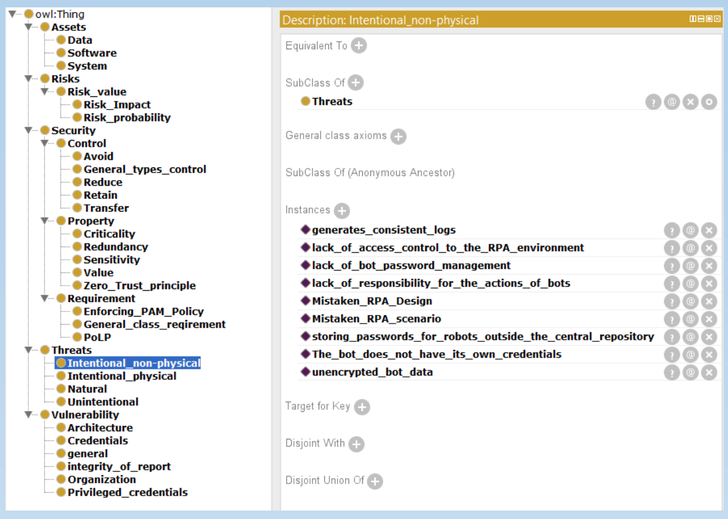


An analysis of the modeling of conducted cases on the use of RPA in the financial sector made it possible to determine that the most common type of attack is spoofing, due to the presence of a large amount of data exchange.

The above samples and scenarios show 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.

However, it is worth paying attention to the presence of specific threats that are characteristic exclusively for RPA systems. The analysis of these threats will make it possible to form a list of countermeasures aimed at reducing the priority of their danger or completely eliminating them. For a visual display of relevant information, it is planned to create a security ontology for RPA.

Based on threat modeling for RPA systems, it was determined which deliberate non-physical threats can be added to the ontology RPASec ontology.



References

1. Nesterak, Janusz & Gąsiorek, Paulina. (2020). Advantages and obstacles to implementing Robotic Process Automation in the enterprises.
2. Focke, F.; Maug, E.; Niessen-Ruenzi, A. The impact of firm prestige on executive compensation. *Journal of financial economics* 2017, 123.2, 313-336.
3. Agrawal, V.A. Comparative Study on Information Security Risk Analysis Methods. *JCP* 2017, 12.1, pp. 57-67.
4. Lošonczi, P.; Nečas, P.; Naď, N. Risk management in information security. *Journal of Management* 2016, 1, 28.
5. Asatiani, A., Penttinen, E.: Turning robotic process automation into commercial success – case. OpusCapita. J. Inf. Technol. Teach. Cases. 6, 67–74 (2016)
6. Gotthardt, M., Koivulaakso, D., Paksoy, O., Saramo, C., Martikainen, M., & Lehner, O. (2020). Current state and challenges in the implementation of smart robotic process automation in accounting and auditing. *ACRN Journal of Finance and Risk Perspectives.*
7. Chandler S., Power C., Fulton M., van Nueten N., Who minds the bots? Why organisations need to consider risks related to Robotic Process Automation. *PricewaterhouseCoopers*, London 2017

DAMSS DATA ANALYSIS METHODS FOR SOFTWARE SYSTEMS
13th Conference
Druskininkai, Lithuania, Hotel „Europa Royale"
December 1 – 3, 2022
http://www.mii.vu.lt/DAMSS
VILNIUS TECH
Fundamentinių mokslų fakultetas