Towards Secure Robot Process Automation Environments

Petri Jurmu
Connectivity Research Area
Technical Research Centre of Finland VTT
Oulu, Finland
email: Petri.Jurmu@vtt.fi

Abstract— **Information security is a part of the cyber security, but the information security will increasingly play a key role in securing and implementing cyber security operations in the future. A big challenge in deployment of robot process automation RPA is that organisations have to give an access to information for software robots like for authorised personnel. People have to take into account the information security and data protection as a basis for a risk assessment, when planning the processing of personal data. This report considers threats and vulnerabilities related to the RPA and examines the opportunities to improve security level in environments of the robot process automation. Observations of security risks are investigated in the case study part, where RPA is deployed in a public service system. Future work of a security assurance in RPA deployment is also described in this paper.**

Keywords-robot process automation; RPA; cyber security; mobiilimittari.

I. INTRODUCTION

Cyber security thinking combines the perspective of information security, continuity management and crisis management in today's society. Cyber security guarantees a rolling of wheels in our society and securing of critical functions in all circumstances. Information security is a part of the cyber security, but the information security will increasingly play a key role in securing and implementing cyber security operations in the future. People have to take the information security and data protection into account as a basis for a risk assessment, when planning a processing of personal data.

Robot process automation RPA develop an action list by repeating a user's performance for a workflow in an application's graphical user interface GUI. RPA is built with a trust on cornerstones of the information security, confidentiality, integrity and availability [1]. Undisputed and traceability of events are important aspects of protecting personal data. In the implementation of the RPA, routine tasks, that do not require a special discretion, are naturally fruitful from a viewpoint of an automation [2].

From an angle of cyber security, a big challenge of RPA deployment is that organisations have to give an access to information to software robots like to authorised personnel. Similarly, organisations have to give an access to a processing service to certain persons or software robots. It is important and in an interest of various parties to find ways to separate parts of the information or activities, which are necessary to be automated.

This paper gives practical information for a deployment of the RPA. We investigated which kind of new surface an adversarial actor can get, if we utilise RPA in maintenance operations of Mobiilimittari service [3]. Mobiilimittari service offers iOS and Android applications for end-users to test their mobile connection quality and speed. With this kind of survey, we can get additional information about safety of our Mobiilimittari service system and make certain actions for the production environment, if needed. This paper presents briefly a case study of Mobiilimittari service, where we started to deploy RPA and made observations. Some useful ideas of the security assurance were proposed as well.

The structure of this paper is as follows. Section 2 presents related work. Section 3 includes description of threats and vulnerabilities related to the RPA. Section 4 presents the overview of security assurance in the robot process automation. Section 5 describes our case study environment and security specific observations in the case study. Section 6 presents lessons learned and Section 7 concludes the paper and gives briefly ideas about the future work.

II. RELATED WORK

To be an RPA pioneer, you will need to take some risks [4]. Authors in [4] proved in a trial the effectiveness of RPA, which produced alarms in the company's IT Security system. It was stated in [4] that IT team had a mature Business Process Management System (BPMS) in-house and questioned why additional automation software was needed. Of course, a risk means more work for IT team.

Security requirements for a global RPA platform are considered in Deckard's article [5], which gives technical security guidelines for deployment of RPA. Much of the responsibility for this security lies with RPA vendors, who incorporate certain security measures into their software products. The vendor takes care of RPA tool, not whole target environment. Therefore, not all of security concerns could be pushed to vendor side.

Authors in [6] propose a new method that analyses business processes and identifies the most suitable for RPA.

 ISBN: 978-1-61208-743-6

That method has measurable parameters for the evaluation of processes. Security aspect is not especially considered in the method, however.

RPA can improve quality and efficiency of manual operations and decrease a mistake probability that would cause problems in production [7]. RPA can reduce costs of production, but handling of data is constituent operation in image recognition systems and security requirements has to be taken tightly into account in the environment as well.

In [8] RPA is mentioned to be next generation testing. From that perspective, it is an excellent way to improve security level of the software and systems.

In our earlier research, we have examined the applying of RPA and artificial intelligence AI in the public sector [1]. In addition to that, we investigated how information security and data protection should be taken into account in the application of RPA and AI in the public sector.

Our approach in this paper is to apply results of earlier research to real service environment, which has been used already several years. In addition, it has been investigated, if there is any sense to start wider deployment of RPA. From that viewpoint security level of existing service and opportunities to improve it are considered.

III. THREATS AGAINST ROBOT PROCESS AUTOMATION

A security threat poses a threat to some of security's components, such as confidentiality, integrity, or availability. Threats against processing and using of the information are a phenomenon of recent years and it will continue to strengthen [9]. It is a consequence of a growth of microservices and an increase of the number of interfaces visible to a network [9]. The development of the prevalence of security threats is from malware to code hijacking and data phishing. The most common threats are still injections, such as SQL injection, which is a database intrusion technology. Threats to an identification and a session management have been intense at the beginning of this millennium.

Privacy is always a challenge in systems that work with machines [10]. A misuse of confidential information is the most important security threat in development and application of the robot process automation [1]. An external hostile actor can hijack codes and control a computer or software. Figure 1 describes a adversarial actor in the RPA environment exploiting observed vulnerabilities in software and systems and causes various disturbing features such as Denial of Service (DoS) to paralyse an ability of system to work or Man-In-the-Middle MItM to listen or disturb a communication path between two messengers by modifying or deleting messages and hacking encryption keys or other information. Additionally, the hostile actor can use Structured Query Language SQL injection to penetrate into a database-based applications and systems. Viruses, worms, Trojan horses and other programs are used to sniff or otherwise fill objectives of the hostile actor. Network security assurance software might also be used for hostile purposes.

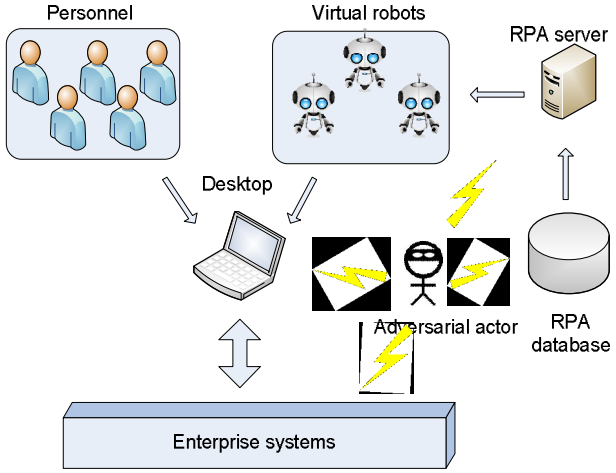

Figure 1. An adversarial actor in the RPA environment.

Robot techniques themselves are generally safer than human-oriented processes from the security point of view [10]. Robots work strictly within regulations and safety parameters of people they replace. Robots follow an accurately programmed and automated event sequence. For example robots do not respond to new arriving emails or leave a screen containing sensitive information unlocked.

One of the threats to deployment of the robot process automation and AI systems is an obsolescence of back-end systems. In a fast-paced business, organisation does not remember to modernise underlying systems, because processes are handled by robotics. In this case, a next security update may possibly break the system. A hacker can find this vulnerability and access data in corporate databases, web servers or employee computers by violating system features and functionality.

RPA and AI are conceptually separated, but it seems that in practical solutions they will be integrated [1]. Today an application of AI is mainly implemented by machine learning ML, which algorithms are tools to help AI to show smarter behavior. Algorithms need information to work correctly and accurately. More information used for learning means more accurate algorithms. The primary threat to the machine learning is through data processing [1]. Classification-based ML algorithms work by finding patterns in a data source. Identifying a source or training method for an algorithm is a valuable tool for hackers. Suitably formatted and injected malicious or incorrect inputs into a system may cause the system to produce erroneous results. Deliberate manipulation of a data source used in a teaching phase can cause bias in decisions of the AI system and even produce inaccurate results. A malicious actor may also attempt to steal algorithms or teaching resources for AI models to produce copies of models for illegal use.

 ISBN: 978-1-61208-743-6

IV. ENSURING SECURITY OF ROBOT PROCESS AUTOMATION

Modernisation of information and communication technologies by the RPA and deployment of new tools and methods always require a management and consideration of new type of risks. The risk-based approach to protect personal data is highlighted, among others, in the new EU Data Protection Regulation [11]. Changes give people better control of their personal data and make it easier for them to access their personal information. It also guarantees protection of the information in all situations, where data is transmitted, processed or stored.

Different security standards define tasks of security risk assessment. For example, the International Organization for Standardization (ISO) has defined the ISO/IEC 27001 standard, which defines the general requirements for creation, implementation and use of a system of information security management. The most important security aspect of RPA is how the robots are managed, how processes are automated and how they are maintained and developed. Security and availability must be a goal in every level of software and systems. Physical level sets own requirements to the information security as well as a level of networking, application and human interaction.

In environments of the robot process automation, it is important to take the access and data security seriously into consideration. Responsibilities and obligations have to be defined accurately for a controller of register and who is dealing with data. Role-based access management has to be a built-in authentication system, in which an access to RPA can be restricted to authorised users and tasks to be automated can be separated [5]. Using of encryption mechanisms, anonymisation or pseudonymisation of personal data have an essential role to protect sensitive data. These mechanisms wholly or partially hide an original content of the information. To achieve a stable state in every phase of automation, it is wise to automate a piece at a time. RPA tools based on TLS (Transport Layer Security) best protect the privacy of data transmitted over a network [5]. Storing logs and operations of robots and users gives traceability in problem situations.

If learning algorithms are supporting RPA functionality, a quality assurance of a system must focus more on a testing of borders and balance [12]. For example in deployment phase a corresponding output of a chatbot feed is known, but after learning, an output has become something different. In a test system, a test case corresponding to this feed is not working similarly as before. When you use the chatbot, you must also test the entire package during use. Testing during operations defines tests to check if the system is working as expected or the system has learned right things. It is also particularly useful to monitor the functionality of the system during operation. Based on the monitoring data effects of the changes can be analysed and noticed if the system has remained within specified limits and tolerances.

Traditional testing methods of software-based systems are still in strong role in a quality assurance of the RPA systems. Source code analyser of software finds the most obvious errors in a program code and errors can be removed before executing the program. Vulnerability scanning searches for commonly known security issues in the target system. Fuzz testing is a form of random testing, where random inputs are generated to a program and program outputs are monitored. Penetration testing evaluates a level of system or network security by attacking a software or system. At the same time, potential vulnerabilities in the system are monitored and analysed.

Ensuring security of a learning system requires, in addition to traditional methods, a special effort in testing design. It is important to strive to ensure strict security already in development phase of software and systems. The learning system does not necessarily have a predetermined activity that can be tested with certain inputs. Testing is done for a specific configuration and predefined functionality, but through the learning, the operation of the software or system changes. That is why a comprehensive set of historical information is needed to test the design to ensure that the right things in the system are learned and that the system does not learn harmful things.

V. CASE STUDY

A. *Overview of Mobiilimittari service*

Mobiilimittari service developed in Technical Research Centre of Finland VTT offers iOS and Android applications made publicly available for end-users in Finland to test their mobile connection quality and speed as presented in Figure 2. It measures downlink/uplink speed, delay and forms an overall connection quality metric (0-10). In addition, it has own tabs for measurement, representing results on a map (own/all), settings and detailed information about the latest measurement.

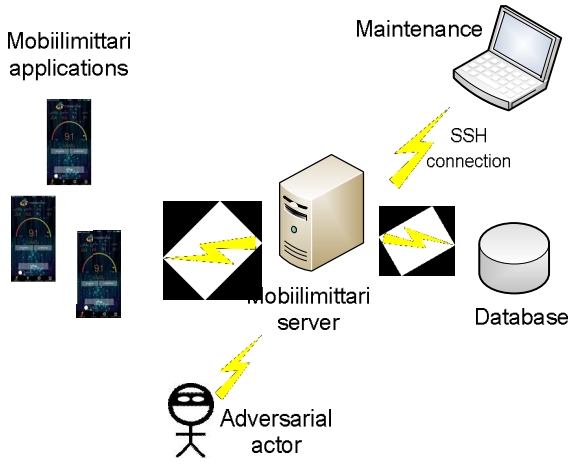

Figure 2 . A fictional adversarial actor in Mobiilimittari service.

This service has been created during the year 2015 without any support of a robot process automation. Security requirements are properly fulfilled and things are in sufficient level from that viewpoint. Security protocols are used behind port configurations, accesses for user applications are delivered via special security mechanisms. Secured connections are used for remote connections and for a handling of SQL database. In this study our aim was to investigate, how certain routines like weekly reporting to maintenance team could be performed with the RPA and which kind of security requirements this kind of deployment sets. In the maintenance team, we make a secure remote connection to move measurement results or get periodical reports about the state of the service. All of these actions have been built and is performed under tight security control.

We use Uipath free trial licence for our case study [13]. UiPath is a RPA vendor providing a complete software platform to help organisation to automate business processes. A software robot aims to manipulate the presentation layer of application software in the same manner a human does. UiPath platform includes the security and audit capabilities related to the target system as well.

In this study, we reflect findings from our earlier research to our real service environment. We used RPA in development environment with a test data, not in production environment with real personal data. In this study, we made observations of a practical RPA deployment from security perspective for example how some kind adversarial actor could have possibility to try something unexpected.

B. Observations

Earlier automated routines in Mobiilimittari service are more like solutions of Business Process Management BPM, which have built deeper to the server code. If there is need for an updating, larger coding and compiling operation is required. Robot process automation gives possibility to build certain routine without any coding skills, but you have to know details about underlying service system or other back-end systems, when building robot process automation however.

A lot of access rights have to be created and given to robots for opening remote connections and logging to databases. Remarkable amount of sensitive data could be in robot hands, which means that it has to be encrypted. In SSH connection user names and passwords may be open for the misuse if the work station is not locked during the break or some one is behind you. Robots don't leave work station unlocked and they are not doing other things same time.

It was observed, that quite a lot of malicious traffic is knocking towards server interface, which is wasting processor capacity of the server. If the RPA is used, robot does not recognize the traffic as human can see from a real time traces on the screen in other words robot's eyes are limited. It means that we have to build separate functionality for a monitoring this kind of traffic.

The utilization of RPA in a wider scale needs quite a lot of modifications to the existing service system. It could be easier to start RPA development in parallel with a product development to get best results. If we need heavy and deep analysis for example of the measurement results, learning algorithms are worth thinking to support the RPA functionality.

VI. LESSONS LEARNED

With this way, we can get additional information about safety of our service system and make certain actions for the production environment. We can watch carefully our server system and keep eye on things, what adversarial actor can do. Robot techniques themselves are generally safer than human-oriented processes, but a challenge of the RPA deployment are accesses to use services and accesses to information.

The tool used in the case study seemed to be suitable to support our requirements, but this may not be the case with all tools on the market. Special attention should be paid on selection of the robot process automation tools, how it fulfills special requirements of certain organisation and user.

Although the first look to the case study seems quite promising, it should be noted that the case study was not executed with real RPA tools yet. Full service development with early phase support of the RPA would be needed to gather metrics and information about the real benefits of the RPA from the security point of view.

VII. CONCLUSIONS AND FUTURE WORK

In this paper, we described observations, how routines like weekly report delivering to maintenance team could be performed with the RPA and which kind of security requirements this kind of service development sets. Robot process automation was applied to VTT's Mobiilimittari service, which has been made publicly available for end-users in Finland to test their mobile connection quality and speed. We observed that there is a lot of new surface for adversial actors, which requires taking tightly care of accesses to be created and given to robots. It was noted that robots should move a remarkable amount of sensitive data between separate servers.

Our case study continues with a real integration of RPA and possibly AI features to the maintenance processes of Mobiilimittari. In addition, we will investigate how we can test the system from the angle of cyber security by applying the RPA. AI comes to performing of security testing as well. AI can determine which test cases or values of parameters are best to use to detect errors. Test tools are able to do certain things in a certain phase. Based on the test results, smart test tools can further modify the tests and try new things to find bugs and bottlenecks of the target system.

In future RPA solutions will increasingly integrate with artificial intelligence solutions. This means increasing of security challenges in the RPA environments as well. Another noteworthy issue is the explosive growth of the application of RPA, which means the level of security has also to be kept up.

 ISBN: 978-1-61208-743-6

ACKNOWLEDGMENT

This research is a part of the research project cluster of Technical Research Centre of Finland VTT in the field of robot process automation. The author wish to thank project members and project partners involved in the projects.

REFERENCES

[1] J. Kääriäinen et al., "Robotic process automation and artificial intelligence – application roadmap". Publications of Government's analysis, assessment and research activities 65/2018.

[2] Quora, "What are the Feasibility parameters in robotic process automation?" https://www.quora.com/What-are-the-Feasibility-parameters-in-robotic-process-automation 2019.08.06.

[3] Mobiilimittari https:/www.mobiilimittari.fi 2019.08.06.

[4] L. Willcocks, M. Lacity, and A. Craig, "Robotic Process Automation at Telefónica O2 (Paper 15/02)," The Outsourcing Unit Working Reasearch Paper Series, 2015.

[5] M. Deckard, https://www.uipath.com/blog/the-security-requirements-for-a-global-rpa-platform 2019.08.06.

[6] A. Bourgouin, A. Leshob, and L. Renard, "Towards a Process Analysis Approach to Adopt Robotic Process Automation", 2018 IEEE 15th International Conference on e-Business Engineering (ICEBE), page 46-53.

[7] S. C. Lin, L. H. Shih, D. Yang, J. Lin, J. F. Kung, "Apply RPA (Robotic Process Automation) in Semiconductor Smart Manufacturing", e-Manufacturing & Design Collaboration Symposium 2018.

[8] S. Bhukan, "Robot Process Automation and the Testing future", https://www.testingbits.com/robotic-process-automation-and-the-testing-future/ 2019.08.06.

[9] OWASP Foundation, The Open Web Application Security Project, https://owasp.org 2019.08.06.

[10] The Shared Services and Outsourcing Network SSON, "How to Manage Risk and Ensure Control – What to Look Out for in Robotic Process Implementation", https://www.ssonetwork.com/robotic-process-automation/articles/how-to-manage-risk-and-ensure-control-what-to 2019.08.06.

[11] EU 2016/679, Regulation of the European Parliament and the Council, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=FI 2019.08.06.

[12] H. Shaukat, T. Gansel, R. Marselis, "Testing of Artificial Intelligence, AI Quality Engineering Skills - An Introduction", https://www.sogeti.com/globalassets/global/downloads/reports/testing-of-artificial-intelligence_sogeti-report_11_12_2017-.pdf 2019.08.06.

[13] Uipath Platform, Robot Process Automation RPA tool, https://www.uipath.com/product/platform 2019.08.06.