TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Darya Harachka 184053IVSB

Securing a Semi-Attended Self-Service Kiosk based on the Example of the Services offered by Apollo Digital

Bachelor's thesis

Supervisor: Priidu Paomets

Master of Science

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Darya Harachka 184053IVSB

Iseteeninduskioski lahenduse turvalisuse analüüs Apollo Digitali näitel

Bakalaureusetöö

Juhendaja: Priidu Paomets

Tehnikateaduste magister

Tallinn 2021

Summary

The spread of self-service kiosks caused the necessity for developing new security features for existing services. As the setups in question are developed to function in unattended or semi-attended environments, service providers need to ensure that end clients can use services provided only in an intended way. It also raised the question of providing physical security and security of the underlying operating system for all the elements of self-service kiosks, as opposed to using services through attended service points or online from users' personal devices. Therefore, it became necessary to enhance the existing approach to securing services provided to accommodate for the specifics of the semi-attended self-service setup.

This thesis paper aims to identify the risks arising from the operation of semi-attended self-service kiosks developed by the Apollo Digital and used in many companies, both inside of the Apollo Group, and outside, assess the probability of them occurring and the severity of the effect they may cause, and propose potential mitigation mechanisms to address the risks that are unacceptable for the organization. The scope of the paper covers the self-service machine itself with its physical and software components, excluding the external services the setup uses and the security of the connection to those services.

The relevance of the topic in question is defined by the fact that introduction of the semi-attended self-service kiosks is an ongoing project for an organization, and there is a need to study the potential threats to the setup and ways to mitigate them. Apollo Digital provides self-service kiosk setups that are used for various businesses in a set of countries for providing retail, entertainment and food industry related services. The countries currently using the self-service kiosk solution designed by the organization include Estonia, Latvia, Lithuania, and Finland. The kiosks are usually placed on the premises belonging to the businesses owning them to provide an additional service point for the end customers. The operations that can be performed by clients using the setup include registration with the user account for the businesses supporting this functionality, selection of items to be purchased from the kiosk menu or using pre-order proof, and payment for the items or services selected.

The physical setup of the self-service kiosk installations in question is comprised from the custom hardware case designed to protect and enclose the main hardware elements of the system such as a touchscreen computer, cash recycling system, barcode scanner, receipt printer, unattended payment terminal system, and a set of cables interconnecting these devices. For the setups used in Latvia and Lithuania there is additionally a fiscal module device included with the setup, that is used for recording the transactions going through the kiosk system in accordance with the governmental requirements.

The current software setup is based on the Windows OS (Operating System), and includes the UWP (Universal Windows Platform) self-service application facing the end customers, hardware services application containing plugins for hardware interfaces, print server application responsible for issuing system print commands, TeamViewer remote access application for remote management of the system, and Miradore system monitoring software. However, there is currently a new generation of software design being developed within the organization, which would still operate based on the Windows OS, but will replace the UWP self-service application, hardware services, and print server set with a combination of a UI (User Interface) application powered by Electron JS, and a local API (Application Programming Interface), with an attached SQLite database used for storing the system state and a set of initial credentials required to start the system and connect to the external API.

The kiosk installation is designed to be used by three groups of users: end customers of the business using the kiosk, employees of the venue the kiosk is located at, and technical and IT maintenance specialists responsible for monitoring and maintenance of the kiosk system software.

The fact that the scope of the security analysis for this paper is limited to the kiosk machine itself allows to conduct an asset-based risk assessment for the setup. The risk assessment process can be conventionally divided into four separate stages:

- Identification of the list of assets
- Identification of potential threats and vulnerabilities to the assets
- Risk probability and impact assessment
- Risk calculation

Based on the description of the kiosk components a list of assets related to the setup was identified, along with associated threats and vulnerabilities. This list was used to calculate the total risk levels using qualitative risk assessment, with the assets being assessed on the scale from 0 to 4, and threats and vulnerabilities on the scale from 0 to 2 each. Resulting values were added to each other for every asset-threat-vulnerability combination in order to calculate the total risk on the scale from 0 to 8.

The risks of the levels 7 and 8 were agreed to be considered unacceptable and therefore requiring prioritized treatment. Most of these risks are caused by existing vulnerabilities related to allocation of operating system and application privileges, as well as to some inherent vulnerabilities of the Electron JS framework to be used in the new software design for the kiosk application.

The set of controls proposed to address the risks identified covers the following:

- Development of the TOTP-based QR code authenticator application that would allow to enhance the security of the method for accessing the management and maintenance kiosk system capabilities
- Splitting the users of the self-service kiosk setup into different privilege groups with the limitations set according to the needs of each group
- Replacing textual user input capability for the kiosk application by the usage of QR codes
- Security configurations for development of the new generation web-based UI application utilizing the Electron JS framework

Most of the solutions proposed do not require additional investments, and none of them require hardware adjustments to be introduced to the kiosk setup. Implementation of these solutions would allow the organization to enhance the security of the currently used self-service kiosk system, as well as to address the vulnerabilities of the new design of kiosk setup.