ERPScan

GET TO THE MONEY: HACKING POS AND POP SYSTEMS

Dmitry Chastuhin
Vladimir Egorov

Disclaimer

The given white paper is a shortened version of the research report conducted by ERPScan security analysts. Unfortunately, ERPScan is not entitled to reveal information about the most critical vulnerabilities of the devices and systems analyzed in the scope of the research.
The full version will be presented and published after the vulnerabilities are fixed by the developer.

Contents

1. Introduction to POS

In 1879, James Jacob Ritty opened his first saloon. Some of Ritty's employees took and pocketed customers' money, instead of using the cash to purchase wares. That is why later Ritty invented a mechanism that could record the cash transactions made at his saloon. The main idea was that when a customer made a purchase, the cashier should push a special button and time at the "clock" increased. This way, at the end of the workday, Ritty could check the cash. The system was not an ideal one, and sometimes cashiers did not push the button and got the money. Nonetheless, we can call this cash register "the forefather" of all Point of Sale systems.

However, if nobody thinks about security during the development of these systems, it will be rather hard to make it secure in future. The POS systems are no exception in any way. These days, a Point of Sale system is a combination of software and hardware that enables merchants to take transactions and simplify day-to-day key business operations. The most familiar example of a POS system is the check-out counter at a retail or grocery store. However, there are even more forms of POS systems used by businesses. If we google "Hack POS," it will return us plenty of information about hacking a POS terminal as a hardware device. We decided to research it.

It should be noted that some of studies have been made even earlier, in 2012-2016.

One of the studies was conducted by Lucas Zaichkowsky, who presented his research at BlackHat USA 2014.[LZ] He analyzed small and large incidents and demonstrated some security issues the POS devices have. For example, magstripe cards contain unencrypted sensitive data, that can be cloned, and EMV chip contains magstripe "equivalent" data unencrypted and can be dumped from RAM.

Another research was authored by Ross Anderson.[RA] He talks about the relay attack of 2007 and No-PIN attack. In other an attacker can manage a terminal and trick a card, and the terminal will perform a transaction.

Peter Fillmore in his research wrote about clone cards, clone transaction and the payment transaction flow.[PF] As a result, it is not possible to clone cards economically, while transactions can be cloned.

Stawomir Jasel and his "Hacking challenge: steal a car!" research. [SJ] Stawomir Jasel wrote and presented an interesting tool, GATTacking tool for MITM BLE (v4.0) connections. One of the possibilities the tool granted was to make an MITM to Mobile POS devices and sniff sensitive information that he showed at BlackHat USA 2016.

Last but not least, Nils and Jon Butler, described the way they could execute malicious code on a terminal using EMV card and play "Chippy Pin" game.

2. The architecture of the payment-processing

The first thing that triggers research interest in the POS software is is the architecture of the payment-processing (see Fig.1).

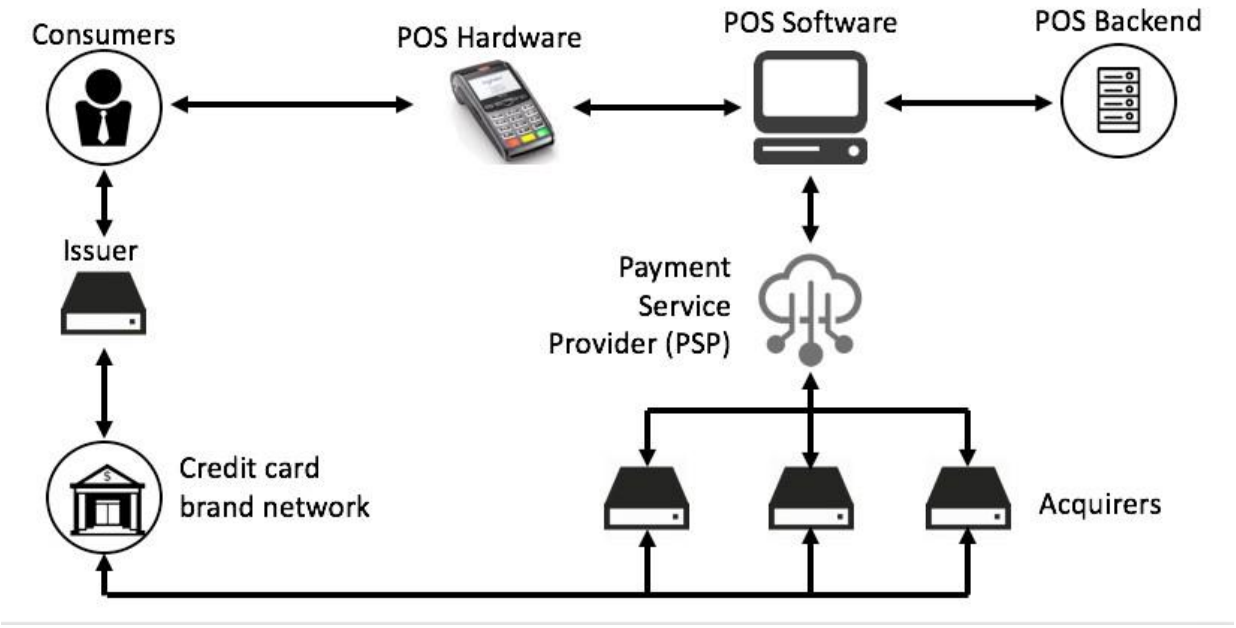


Fig.1. Architecture of the payment processing

First, consumers swipe their cards on a merchant's PoS devices to purchase goods and services. This PoS device sends the credit card data to a merchant's PoS system.

Secondly, the PoS system contacts the PSP (Payment Service Provider), who then contacts the designated acquirers to authorize the transaction, depending on a card of what brand or type was used.

Then, the acquirers use card brands' networks to contact the issuers of the credit card. The issuers return an authorization status to the acquirers via card brands' networks.

Finally, the acquirers pass on the authorization to the PSP, that forwards it to the PoS systems and devices, which complete the transaction. The communication process is swift and takes a only a couple of seconds.

Client - hardware and hardware–POS software communication types are yet to be researched. So, what will it be if cyber criminal tries to attack the backend of the store system terminal rather than a consumer or terminal? What will happen, if an attacker can manipulate prices or the other settings, make payment information go not just through the terminal and POS hardware, but the POS software as well?

3. Business day

POS business day is a key to understanding POS processes. To begin the day a manager opens a store. This action can be done just by an employee with the manager privileges. After that, the same person opens terminals, and cashiers log in the system. The terminals get updates from the server and synchronize business date and time. After that, the business day is officially started. Every minute, the terminals pass an enormous amount of information about transactions, price look-up codes and item descriptions, inventory information, promotions, cash, logs. At the end of the day, all happens in the reverse order. The cashiers log out, manager closes the terminals. All terminals send log information to the server

After that, the Manager closes the store. Therefore, no transaction can be performed until the store is closed.

All right, with a base knowledge about POS, it is high time to choose one and delve deeper into it.

Based on the 2016 RIS Software LeaderBoard published by Edgel Communications the following companies are the best software providers that specialize in retail technology: Cegid Group, MI9 Retail (Raymark), ECRS, Manthan Systems, Celerant Technology, SAP, Aptos, Oracle, PCMS Datafit, MicroStrategy. [RIS]

This top 10 contains Large Vendors and Mid-Size Vendors. In the scope of our research we analyzed Large vendors. The comparison of the vendors is presented below (see Table 1):

RANK	COMPANY	CUST. SAT.	RET. CON.	REV.FAC.	TOTAL
1	SAP	35.9	47	5	87.9
2	Aptos	38.4	43	4	85.4
3	Oracle	33.7	45	5	83.7
4	MicroStrategy	34.8	40	5	79.8

Table 1. Large vendors

In this table there are six columns:

- Rank
- Company name
- Customer Satisfaction
- Retail Concentration
- Revenue Factor
- Total Points.

The Rank, Company Name columns and Total columns are quite self-explanatory. The Customer Satisfaction, Retail Concentration and Revenue Factor columns are the three most important data points in the LeaderBoard. For full definitions of these data points see the “Methodology” section of the RIS Software LeaderBoard.

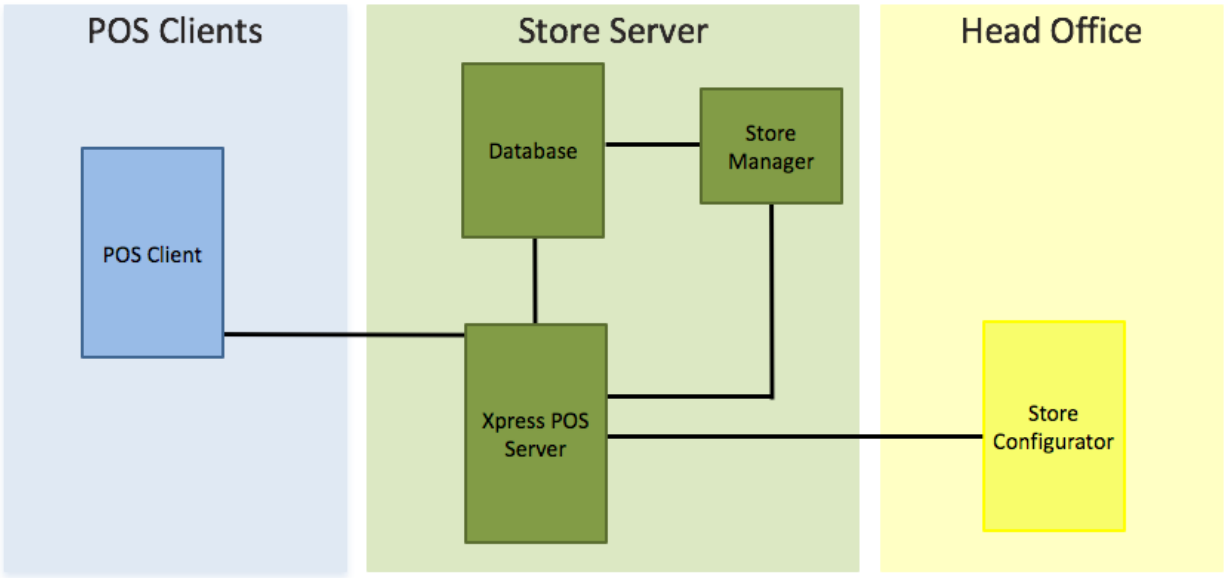
SAP was chosen as the primary subject of the research.

4. SAP Point of Sale system

SAP is the world leader in enterprise applications in terms of software and software- related service revenue. Based on market capitalization, it [SAP] is the world's third largest independent software manufacturer.

As for SAP POS, the description from the official site says, that this is client/server point-of-sale (POS) solution. Known as Triversity Transactionware GM prior to its acquisition by SAP in 2005, SAP POS meets the needs of a wide variety of retailers, with the benefit of over 15 years of refinement, development, and customization. Retail Customers include department, c-store, liquor, gas, specialty, apparel, big box, and a number of other retail verticals. Additionally, the solution is offered with powerful back-office applications, for in-depth, store-level management and reporting. It works on Windows 32-bit and 64-bit platforms, was written on C++ (see Fig. 2).

The architecture of SAP POS is rather typical for point of sale solutions (see Fig. 2). It consists of Store Client applications running on the store POS systems to process POS transactions, Store Server applications running in the store's back office to serve connective, operative and administrative needs and applications running in the head office to enable central



configuration

.

Fig. 2. SAP POS architecture.

As a part of this research the real store, with cashiers' work places, store server, and the head office server was emulated. One by one, ERPScan experts checked communications, standard behavior, and system functions.

4.1. Store Configurator and Xpress Server

Store configurator is software with GUI used to configure everything in the POS system: users, terminal appearance, PLUs, security settings, etc. Using a “pretty nice” interface, a system administrator changes all he/she wants. After that, the Configurator converts the settings into a special file, saves them in the ”PARM” directory, creates the ”newparm.trg” new file. The administrator needs to copy these files to the Xpress Server.

This file acts as a trigger. The Xpress Server application search this file every 30 seconds. If it finds the trigger file, all parameter files will be checked for updates and applied. After that, the server deletes the “newparm” file.

The “PARM” directory stores configuration files. For example, the “cnummask.cmk” file is responsible for masking card in the receipt, cashier.clg contains information about cashiers and managers of the POS System, LAYOUT.UI0 describes the appearance of the POS terminal.

4.2. Xpress Server and Store Manager

Store manager is software with GUI used to configure store`s settings. We can divide all possible functions into two parts by using ports:

- The first one is a database port. This way, the Store manager resembles the Store Configurator, but it works directly with Database and writes all changes into it.
- The second part is port 2202. After it was detected the standard user interface was checked, and available ports were scanned.

This port did not validate internal connections, so, anybody could communicate with it. When communicated with, it returns a welcome message with the POS build. Help command displays possible operations. There are more than 17 public functions. Some of them are critical as they let anybody look for any cashier`s action, open and close procedures without any authentication and simply shut down the server. Having reversed the “xps.exe” binary responsible for the 2202 port, ERPScan researchers found 17 functions along with 57 private functions. Below you can find information about some of them.

There is method APM-VALIDATE-PASSWD:

APM-VALIDATE-PASSWD [store_number] [thread] [region_number] [login];[password]

As soon as this command is sent, the server returnes the result. It is quite peculiar that there are different responses from the server and there is no try limit. There is nothing that can prevent an attacker from brute-forcing logins the first: max size is 15 numbers, if an attacker

ERPScan

gets 10 code - there is no user with this login; and password after: “1” code for wrong password and “0” for the right one.

The reset command workes in the same way, but there is a trick there. This command will not work, a password is changed to a similar one.

Another interesting part of methods is file operations. It was possible to read files on the server by using these functions without any validation.

The “File-open” method is used to open the file on the server. FILE-OPEN [file-path] [mode]

The default value of [mode] is “r”, acceptable ones are “r”, “w”, “a”, “r+”, “w+”, “a+”, like in C++. The wrong [mode] crashes Xpress Server application, cause there is no validation of [mode] parameter, it translate in fopen() function. If it all goes right, the system will return file id to call this file.

The next step is to call FILE-READ method, and we can get the file content.

4.3. Security patch

To prevent vulnerability exploitation, install SAP Note 2520064.

5. Conlusion

Not only is SAP POS system vulnerable to an attacker, but also Oracle company multinational computer technology corporation, primarily specialized in developing and marketing database software and technology, cloud engineered systems and enterprise software products has the same problems.

We hope the Retailers and Software vendors will think about security of their clients and customers and we will help them in this difficult case.

6. Future research

There are a lot of POS systems and our research shows that they are not ideal. SAP POS is just an example, we do not think, that there are no vulnerabilities in other systems. That is why, our further research may be conducted using other systems as its subjects, like Oracle`s Micros, Aptos.

References

[LZ] “Point of Sale System Architecture and Security” - https:/www.blackhat.com/docs/us-14/materials/us-14-Zaichkowsky-Point-Of-Sale%20System-Architecture-And-Security.pdf

[RA] “How Smartcard Payment Systems Fail” - https:/www.blackhat.com/docs/us-14/materials/us-14-Anderson-How_Smartcard-Payment-Systems-Fail.pdf

[PF] “Crash and Pay: Owning and Cloning Payment Devices” – https:/www.blackhat.com/docs/us-15/materials/us-15-Fillmore-Crash-Pay-How-To-Own-And-Clone-Contactless-Payment-Devices.pdf

[SJ] “Hacking challenge: steal a car!” - https:/www.blackhat.com/docs/us-16/materials/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool.pdf

[RIS] “RIS Software LeaderBoard 2016” - http:/go.cegid.com/rs/818-MJH-876/images/RIS%20News%202016%20LeaderBoard%20Results.pdf

[SAP] “SAP Poing of Sale” – https:/wiki.scn.sap.com/wiki/display/Retail/SAP+Point+of+Sale

Contacts

US Office

Mail to: 228 Hamilton Avenue, Fl. 3, Palo Alto, CA. 94301

Phone: 650.798.5255

Twitter: https:/twitter.com/erpscan/

Facebook: https:/www.facebook.com/ERPScan/

LinkedIn: https:/www.linkedin.com/company/2217474/