ERPScan

GET TO THE MONEY: HACKING POS AND POP SYSTEMS

DMITRY CHASTUHIN
VLADIMIR EGOROV

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).

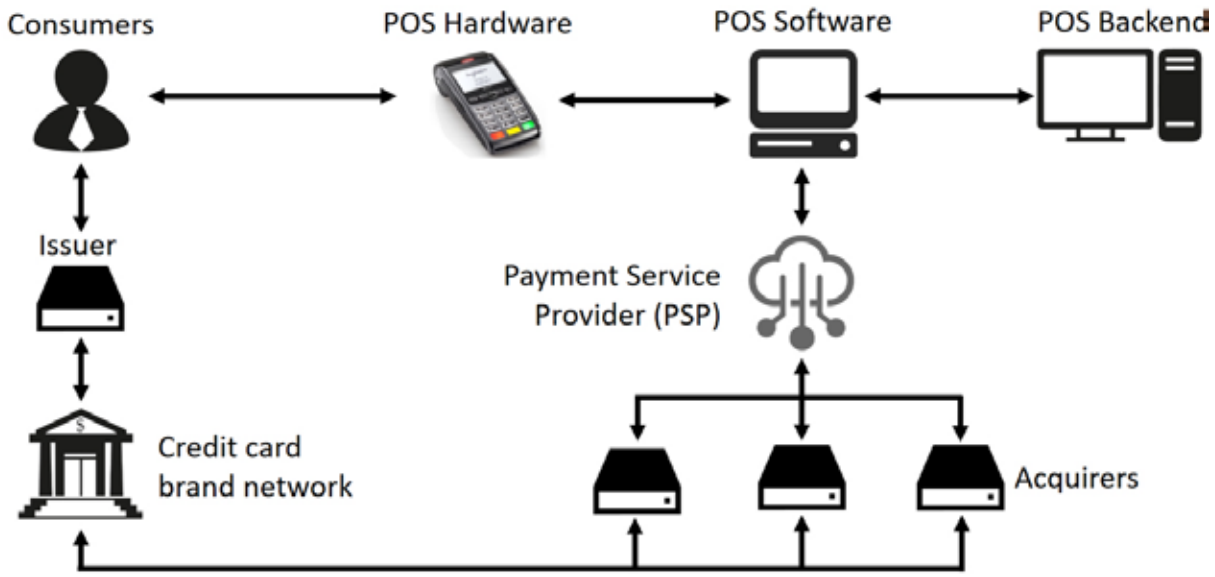


Fig.1. Architecture of the payment processing

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	39.9	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

Internal entities (HCM infotypes):

- 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.

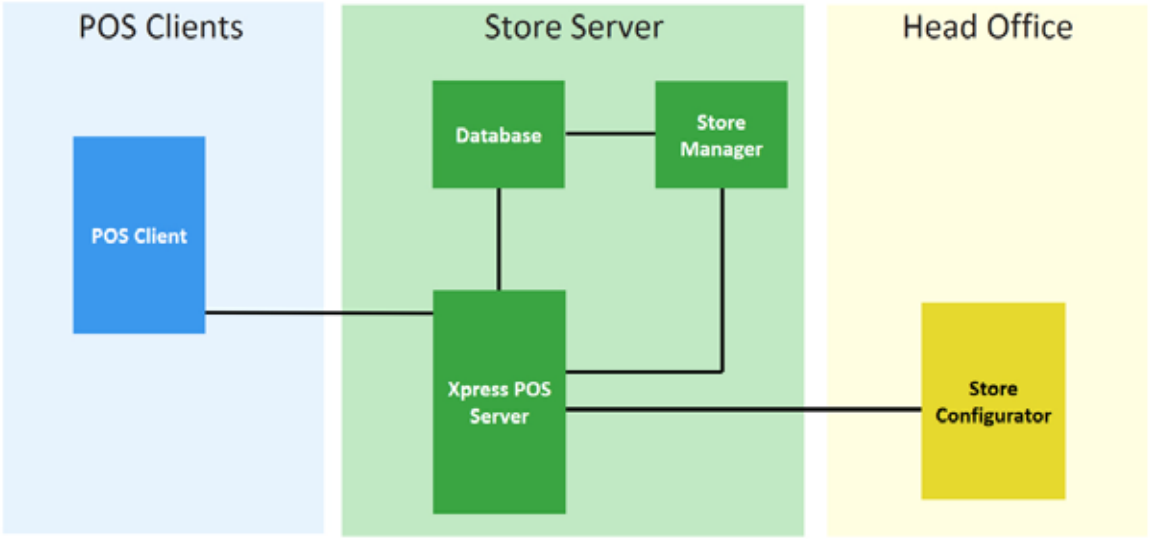


Fig. 2. SAP POS architecture.

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 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. POS CLIENT AND XPRESS SERVER

POS client connects to the store server and communicates with it using port 2200. All information like transaction, configuration and maintenance data is transferred through this port. At the beginning of the day, when a store manager opens a terminal, it sends a request, like ‘Hey, Server, I woke up, send me new parameters, pleeease.’ At the end of the day, when the manager closes the terminal and the store, it sends log files to the server.

ERPScan experts managed to capture the traffic between the client and the server, and found out that when the POS terminal sends a special packet to the Xpress Server, the response is a content of the file in the packet.

If another machine is used to perform this operation, the same result will be returned. A bit of practice and an attacker will get a working POC on reading every file on the server`s file-system!

In the scope of the research the following packet was sent (see Fig. 3)

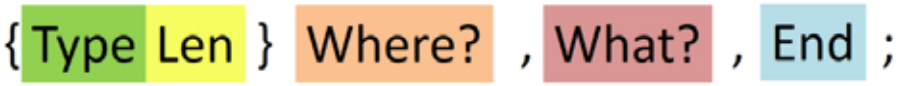


Fig. 3. Sent packet

it has 5 elements in it:

1. The first symbol determines the message type,
2. The yellow field is a message length.
3. Local file – is a path, where the Terminal writes the data. We send the message non from terminal, so, we can put here anything we want.
4. The next one data is a target file path.
5. The last one is always 0,0 and changes only in the response message.

Reverse engineered protocol shows that an attacker has even more possibilities, than just reading files.

Conversation standard sends the following messages:

- Bad file
- End of file
- Datagram
- File request error
- File Data
- Good
- Request Diretory
- Request for file sending
- Send file
- Cancel sending
- Response Directory
- Receive cancel.

To write any file on the server, it is required to send three packets on port 2200.

The first one is of the “Send file” type and contains the packet length; file path on Xpress server, where an attacker writes the data; the local path to the file (not necessary); size of the sending data and static null value.

The second one is the “File data” type packet. It contains the content length, and the data that must be written.

The last one is the “End of file” message. After that, Xpress Server application responses with “Good” message and a new file appears on the server. If a wrong size of file is sent, the Xpress application will delete the target file. All these manipulations could be done without any validation. In addition, there is also anonymous file reading, writing and deleting.

4.4. ATTACK VECTOR

So, what are possible attack vectors? All an attacker needs is an access to the local store network. There are some POS clients in every store. There are also various peripheral devices, e.g. barcode readers, scales, card readers and other devices connected to POS clients. Some gadgets are placed right at the store hall. What is more important, they are not always protected. That is why an attacker can replace one device with “Raspberry Pi” with a running script.

During the research, ERPScan experts considered 4 facts about SAP POS:

1. Store configurator creates configuration files and the Xpress Server will apply them, if it finds the ”newparm” file in the special directory.

2. Any data can be written in any file on the Xpress Server using port 2200.

3. POS Clients (Terminals) update their parameters after opening.

4. POS Terminals can be closed and opened by using telnet and port 2202.

The combination of these steps leads us to the next:

1. An attacker writes Configuration files on the Xpress server by using port 2200 in the “PARM” directory. Configuration files may be different. An attacker can change card mask number and it will be printed on the receipts; after that it is possible to change price of an item, create a new promotion or switch off encryption of sensitive data in database.

2. An attacker writes the “newparm.trg” file on the Xpress server by using the same port 2200.

3. The Xpress Server application finds the trigger file and applies new attacker`s settings.

4. It writes some of them in the Database (like promo information).

5. An attacker sends the ”Close term” message on the Xpress Server telnet port 2202.

6. The Xpress server sends a request to the POS Terminal to close it.

7. An attacker sends the “Open term” message to the Xpress Server telnet port

8. The Xpress Server application opens the POS Terminal.

9. The POS Terminal sends a request to the Xpress server, downloads attacker`s settings, and applies them.

It is not necessary to close and open terminals. As said before, there is “End of Day” process in POS business day. It means that at the end of the day the store and every terminal will be closed and opened next day.

There also several additional features here. When the Xpress Server application is starting or updates parameters, it searches for the “XPSPARM.bat” and “StopTN.bat” files in the home directory. If the process is successful, the file will be executed. Nothing can stop an attacker from uploading the special script in “XPSPARM.bat” and getting full control of the Xpress Server machine.

4.5. ENCRYPTION

SAP POS uses TWSecurity tool for the encryption. It creates a special security container with a password. This container cannot be exported, imported or read without password validation. The container should be similar for SAP POS elements: clients, the Xpress Server, the Store manager and Configurator. The sensitive data is encrypted at every process level. According to the documentation, the following tables and columns are affected by the encryption implementation (see Table 2).

TABLES	COLUMNS
TXN_PROFILE_PROMPT_RESPONSE	profileresponse1, profileresponse2, profileresponse3, profileresponse4
PTD_PROFILE_PROMPT_RESPONSE	profileresponse1, profileresponse2, profileresponse3, profileresponse4
TXN_NON_MERCH_SALE	refnum
PTD_NON_MERCH_SALE	refnum
TXN_METHOD_OF_PAYMENT	refnum
PTD_METHOD_OF_PAYMENT	refnum
Employee	password
PA_CUSTOMER	address1, address2
TXN_AUTHORIZATION	cardnum, authnum, creditresponse, captresp, cardholdername
PTD_AUTHORIZATION	cardnum, authnum, creditresponse, captresp, cardholdername

Table 2. Affected tables and columns

In the table “CryptoRegister” there is a list of columns and stored procedures, which are affected by the encryption too with an encryption level. For example, employee`s passwords are stored as a hash value, and reference number of the card as 3DES cipher text. However, is it as secure, as it sounds?

Encryption token and encryption as the function are set by the administrator in the Store Configurator. Encryption token is converted in ASCII file and sent to the Xpress Server. An attacker can change it to the null, and this way it will be possible to switch-off encryption mechanism in future transactions and processes.

What is about stored and encrypted information in the database? Let`s have a closer look at TWSecurity tool. In fact, the security container is nothing but some rows in the system registry. TWSecurity tool helps to create new keys for the encryption and re-encrypt sensitive data with a new key. It means, that this tool connects to the database, gets cipher-text, decrypted it using the old key and encrypt one more time with an another key, after that it updates database rows.

An attacker can use this tool and just steal clear text data from the memory. In the scope of the research Frida, a python library was tested. The given method proved to be efficient.

4.6. SECURITY PATCH

The patch “Missing Authentication checks in SAP Point of Sale (POS) Retail Xpress Server” was released on 11 July, 2017 as a part of SAP Security Note 2476601. The patch is an archive with 14 files in it, which will replace some original ones. The main executable files xps.exe, xpsctrl.exe are among them. The main idea of this fix is that if an attacker could send something on the port 2202 and control terminals, it would be necessary to restrict access to this port. The description says that a new parameter appears after the patch that determines an IP address, which accepts connections by the Xpress Server. The default value is the localhost. However, there is one thing this patch misses: the problem is not only with the 2202 port, but also with port 2200. The latter provides too many opportunities to an attacker. By using them an attacker can bypass the defense mechanism. There are two cases to discuss depending on the Store manager’s location: it could be either remote or local.

4.6.1. LOCAL STORE MANAGER

When the Store manager application connects to the Xpress server, it checks if the incoming IP address is localhost and rejects it if it is not. So, presumably, only local applications and users could communicate with this port. As it was described before, an attacker, by using port 2200 could send the command to the Xpress server to connect to itself on port 2202 and bypass validation.

4.6.2. REMOTE STORE MANAGER

The second way to install Store Manager is to use another machine. When the Store manager connects to the 2202 port, the Xpress application opens configuration file “local.ini,” gets the «BACKOFFICEIPADDRESS» parameter, compares it with the incoming connection IP. To bypass this validation, an attacker could just read current settings in the “local.ini” file, replace the correct IP with the evil one and rewrite the file. This way, the Xpress server application will consider an attacker’s IP as a legal one.

5. Conlusion

On the whole, if there is no bug on the 2200 port, the security patch will protect the system from an external attacker. However, there is one, and it is the problem.

This bypass was reported to SAP. The defense team made an additional security patch in no time.

Nonetheless, 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”

[RA] “How Smartcard Payment Systems Fail”

[PF] “Crash and Pay: Owning and Cloning Payment Devices”

[SJ] “Hacking challenge: steal a car!”

[RIS] “RIS Software LeaderBoard 2016”

[SAP] “SAP Poing of Sale”

Contacts

ERPScan is the most respected and credible Business Application Cybersecurity provider. Founded in 2010, the company operates globally and enables global Fortune 2000 to secure their mission-critical processes. ERPScan's primary mission is to provide Smart solutions to assess and protect ERP systems and business-critical applications from both cyber attacks and internal fraud.

ERPSCAN & GARTNER

GARTNER HYPE CYCLE FOR APPLICATION SECURITY

GARTNER MQ FOR APPLICATION SECURITY

GARTNER MS FOR SOD TOOLS

OUR ACHIEVEMENTS

3X CUSTOMER BASE GROWTH

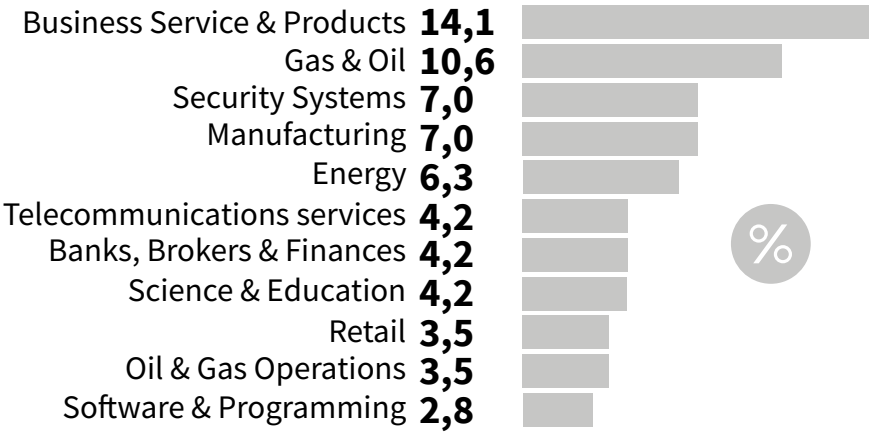
2015 **5X** 2016
REVENUE GROWTH

CLIENTS IN COUNTRIES **44**

500 VULNERABILITIES REPORTED

200 DEPLOYMENTS WORLDWIDE

INDUSTRIES 40+



US OFFICE

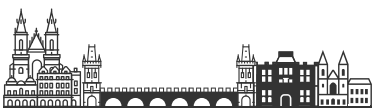
PALO ALTO

EMEA OFFICE

AMSTERDAM

R&D OFFICE

PRAGUE



BLOG WEBINARS NEWSLETTERS

ERPSCAN CONTACTS:
inbox@erpscan.com
erpscan.com