onapsis

Securing Business Essentials

Attacks to SAP® Web Applications

Your crown jewels online

Mariano Nuñez Di Croce

mnunez@onapsis.com

March 30th, 2011

Troopers, Germany

Disclaimer

This publication is copyright 2011 Onapsis SRL – All rights reserved.

This publication contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.

Who is Onapsis?

- Company focused in the **Security of ERP systems and Business-critical Applications** (**SAP®,** Siebel®, Oracle® E-Business Suite™, PeopleSoft®, JD Edwards® …).
- Working with Fortune-100 and large governmental organizations.
- Core business areas:
  - Development of security software (Onapsis X1, Onapsis Bizploit).
  - Security consultancy services.
  - Trainings on business-critical systems security.

Who am I?

- **Director of Research and Development at Onapsis.**
- Discovered **vulnerabilities** in Microsoft, Oracle, SAP, IBM, …
- Developer of the first **opensource SAP/ERP Penetration Testing frameworks**.
- Lead author of the “SAP Security In-Depth” publication.
- **Speaker/Trainer** at Black Hat, HITB, Sec-T, Hack.lu, DeepSec, Ekoparty..

Agenda

- Introduction to the SAP world
- The evolution of threats to SAP systems
- The different SAP Web Application Servers
- Exploitation of SAP WebApps: the cyber-attacker’s dream
- The anatomy of the attacks and how to protect yourself
- Conclusions

Introduction

What is SAP?

- **Largest** provider of **business management solutions** in the world.
  - More than 140.000 implementations around the globe.
  - More than 90.000 customers in 120 countries.

- Used by **Fortune-500 world-wide companies**, **governmental organizations** and **defense facilities** to **run their every-day business processes.**
  - Such as Revenue / Production / Expenditure business cycles.

FINANCIAL PLANNING TREASURY PAYROLL

INVOICING **LOGISTICS**

SALES BILLING

PRODUCTION PROCUREMENT

What this talk is about

- Security aspects of *standard* SAP Web applications.
- Common mis-configurations and weaknesses that could allow remote attackers to compromise SAP servers from the Internet (and Intranets).
- Live demonstrations with real-world business impacts.
- How to protect yourself from these threats, increasing the security of your business-critical ERP systems.

What this talk is not about

- Security aspects of *custom* SAP Web applications.
- Exploiting and protecting against SQL Injections, XSS, XSRF and Path traversals in *custom* applications.
- This is to be covered in a future talk.

The evolution of threats to SAP systems

What “SAP Security” used to be

- Traditionally, **“SAP security” has been a synonym of “Segregation of Duties” controls.**
  - **Goal:** “Make sure that if Tim can create a new vendor, he can not create purchase orders”.
  - This is mapped to a SoD matrix with SAP transactions/authorization objects.

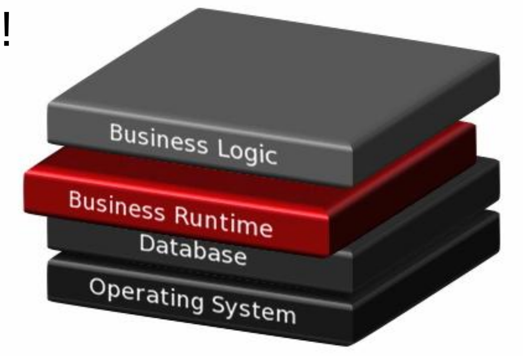
- Large organizations that have “SAP Security” in place:
  - **Spend hundreds of thousands dollars yearly** by having dedicated human resources and software licenses for their “SAP Security” Team.
    - If someone’s job title starts with the word “SAP”, his salary is twice ours.
    - Common software in this area costs **between $500K and $2M**.

The worst of all this: Many organizations have a false sense of security!

What "SAP Security" is now

- SoD controls are necessary, but **they are not enough**!
- They only address one of the layers where security must be enforced.
- **The forgotten layer: The Business Runtime (NetWeaver/Basis).**
  - Base framework in charge of **critical tasks** such as authentication, authorization, encryption, interfaces, audit, logging, etc.
  - Can be susceptible of security vulnerabilities that, if exploited, can lead to **espionage, sabotage and fraud attacks** to the business information.

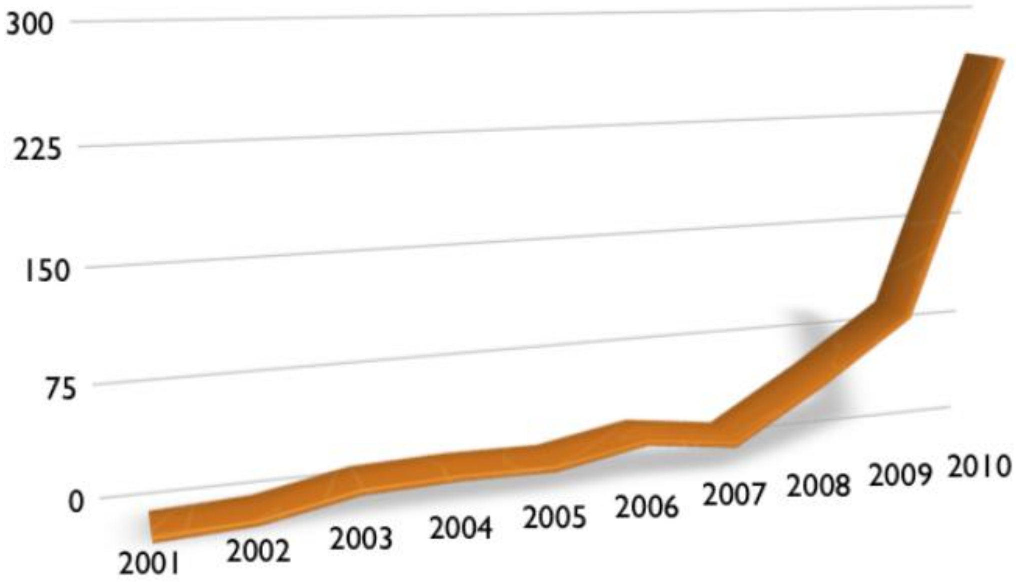
- **Involves much higher risks than SoD violations** -> In many cases, the attacker does not even need a user account in the system!
  - Quick example: By default, a remote attacker can take complete control of SAP Application Servers *anonymously* by exploiting RFC vulnerabilities.



A Rising Threat

- **The number of SAP Security Notes** has increased drastically over the last years.
- Security Notes usually address one or more vulnerabilities.
- Most of these issues affect the *Business Runtime.*

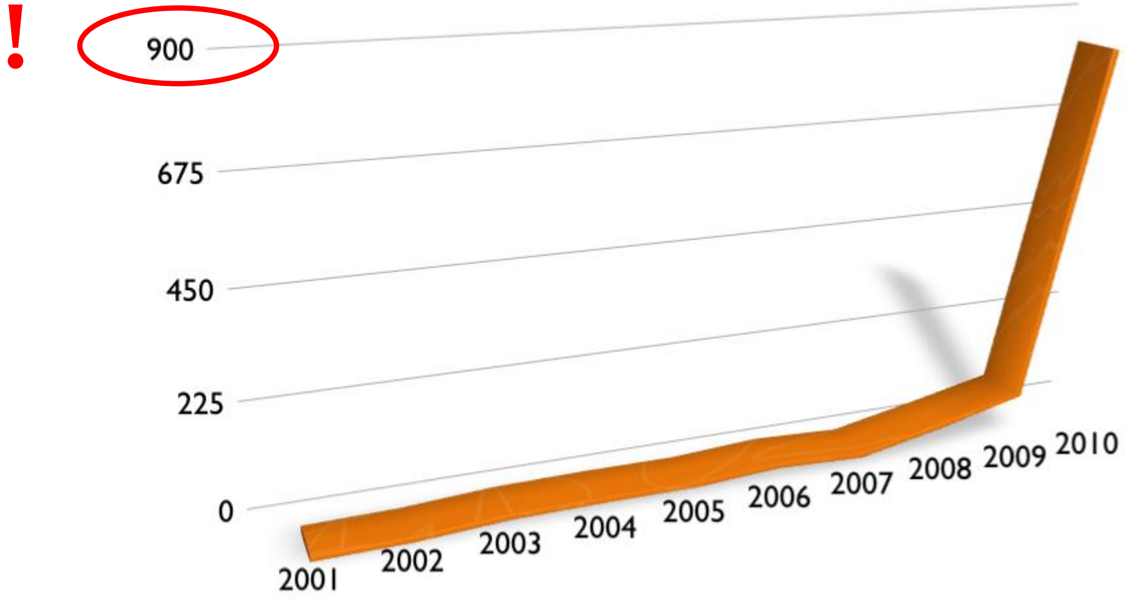
Number of SAP Security Notes per Year (estimated in mid-2010)



A Rising Threat

- **The number of SAP Security Notes** has increased drastically over the last years.
- Security Notes usually address one or more vulnerabilities.
- Most of these issues affect the *Business Runtime.*

Number of SAP Security Notes per Year (final results 2010)



What is SAP doing about this?

- **SAP is moving quickly** to adapt to this new reality.
- On September 2010, the "Security Patch Day" was launched.

- The same month, SAP released a new whitepaper that provides **"a set of security measures for ABAP systems against unauthorized access within the corporate network."**
  - This will become a **de-facto standard** in the near future.
  - By using **Onapsis X1**, it's possible to check compliance automatically ;-)

- On December 2010, a new whitepaper "Protecting SAP Applications Against Common Attacks".

- **SAP security is getting definitely better with each release**.

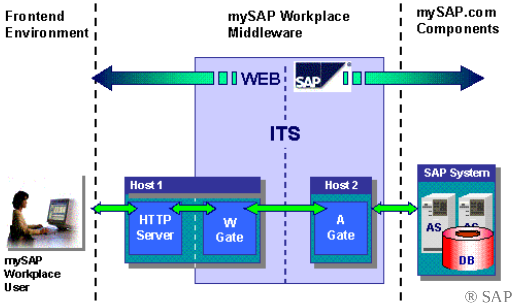
The different SAP Web Application Servers

The SAP Internet Transaction Server (ITS)

- The ITS was released in 1996, being **SAP's first approach to enable Internet access to SAP systems.**
- This component acts as a **middleware** which works mainly by translating SAP Dynpros (dynamic programs) into HTML pages.
- It's built upon two components: the **Wgate** and **Agate**.
- Functionality is provided through Agate services.
- URLs have the following syntax:

```
http://<server>:<port>/<path_to_wgate>/<service_name>/!?<optional_params>
```

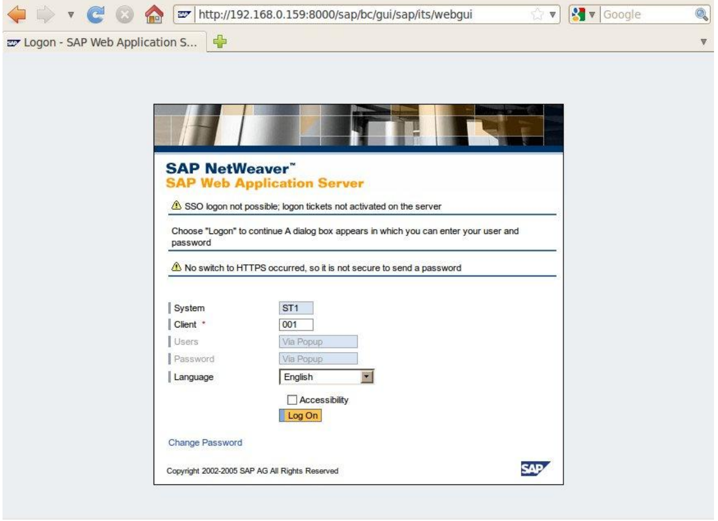
- path_to_wgate usually is */scripts/wgate*
- The ITS was integrated into the WAS 6.40.



® SAP

The SAP Internet Communication Manager (ICM)

- **The evolution of the ITS component.**
- The SAP kernel was enhanced to support HTTP(S) and SMTP protocols.
- No need to implement middleware components.
- **Warning: No middleware == direct access from the Internet?**
  - A **reverse proxy** should be placed in the public DMZ! (SAP Web Dispatcher)
- The ICM web requests are handled by the ICF, which provides *services.*
- Since Release 6.20, ICF services are inactive by default.



http://192.168.0.159:8000/sap/bc/gui/sap/its/webgui

Logon - SAP Web Application S...

SAP NetWeaver™
SAP Web Application Server

⚠ SSO logon not possible; logon tickets not activated on the server

Choose "Logon" to continue A dialog box appears in which you can enter your user and password

⚠ No switch to HTTPS occurred, so it is not secure to send a password

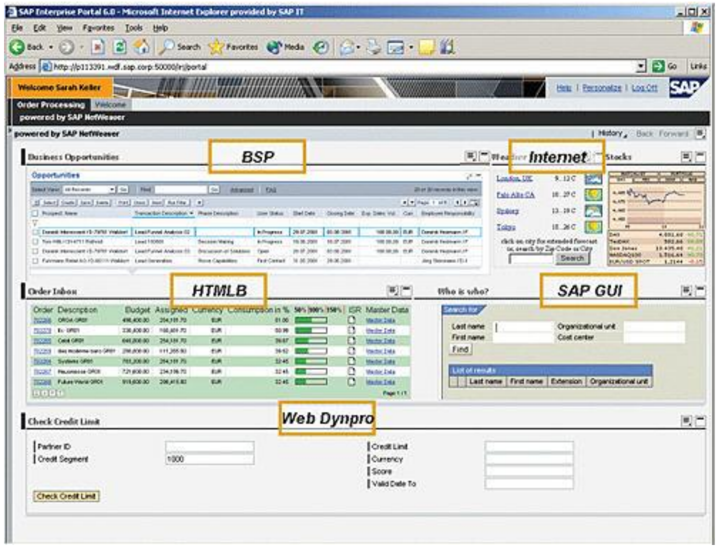
System	ST1
Client *	001
Users	Via Popup
Password	Via Popup
Language	English

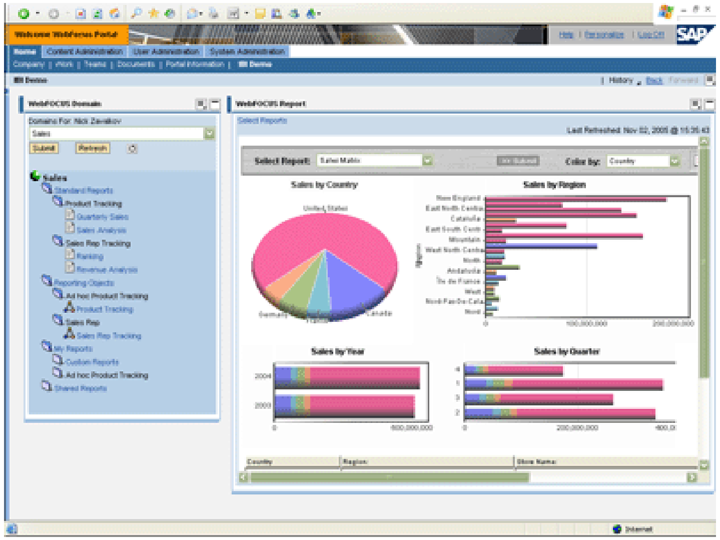
□ Accessibility

Copyright 2002-2005 SAP AG All Rights Reserved

The SAP Enterprise Portal (EP)

- Latest Web technology from SAP.
- **Goal: Provide an unique access point to the organization's SAP (and non-SAP) systems through the Web.**
- It “provides employees, partners, customers, and other workers with immediate, secure, and role-based access to key information and applications”.
- Technically, it’s a complex Java application running in the SAP J2EE Engine.



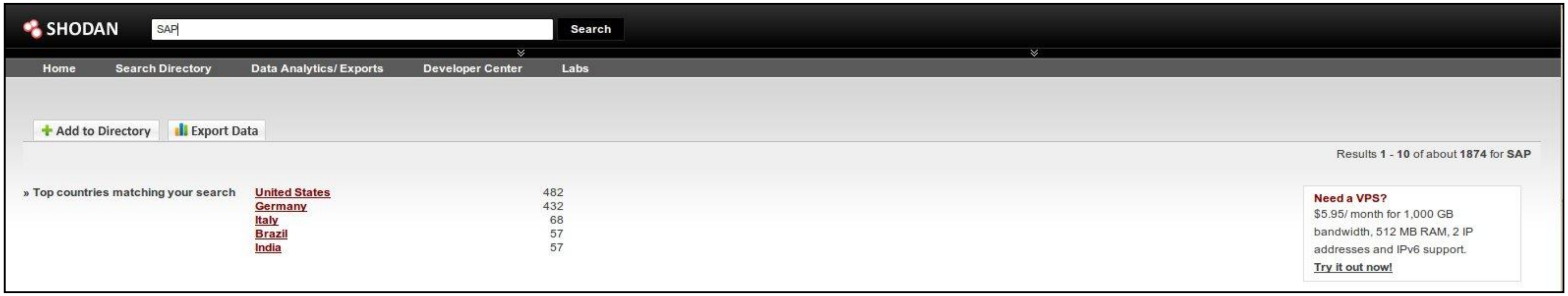


Exploitation of SAP WebApps

The cyber-attacker's dream

“My SAP system is only used internally”

- While that was true more than a decade ago, now it’s common for **SAP systems to be connected to the Internet.**
- **Attackers know how to find them** using regular search engines.

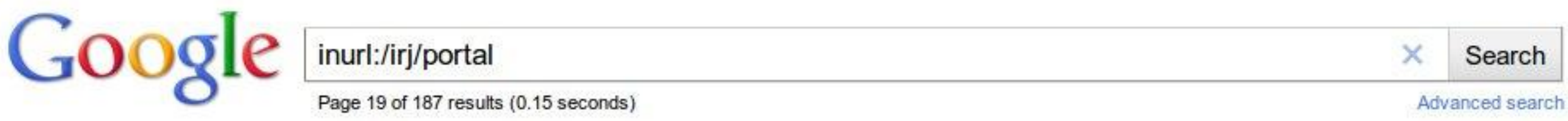


Results **1** - **10** of about **1874** for **SAP**

» Top countries matching your search

United States	482
Germany	432
Italy	68
Brazil	57
India	57

Need a VPS?
$5.95/ month for 1,000 GB bandwidth, 512 MB RAM, 2 IP addresses and IPv6 support.
Try it out now!



Page 19 of 187 results (0.15 seconds)

If your SAP is not supposed to be public, make sure it’s not there!!

The Attacker's Dream

- Typically, **it won't be easy for an external attacker to reach internal SAP systems.**
  - However, he enjoys the privilege of being **harder to catch**.

- **Internal attackers have much more power**.
  - However, they are **more prone to detection**.

- The new paradigm: **If SAP Webapps are not securely implemented, the attacker is having the best of both worlds.**

- Some **illustrations** of what this can really mean next…

The anatomy of the attacks and how to protect yourself

Identification through Server Banners

- Just as any regular web server, SAP web servers return a “Server” header in HTTP responses.
- This information can be used by attackers to identify the components and versions in use.

Component	Some Examples
SAP ITS	N/A
SAP ICM	server: SAP Web Application Server (1.0;640) server: SAP NetWeaver Application Server (1.0;700) server: SAP NetWeaver Application Server / ABAP 701 server: SAP NetWeaver Application Server 7.10 / ICM 7.10
SAP J2EE Engine (EP)	Server: SAP J2EE Engine/700 Server: SAP NetWeaver Application Server 7.10 / AS Java 7.10

Identification through Server Banners

- Just as any regular web server, SAP web servers return a “Server” header in HTTP responses.
- This information can be used by attackers to identify the components and versions in us

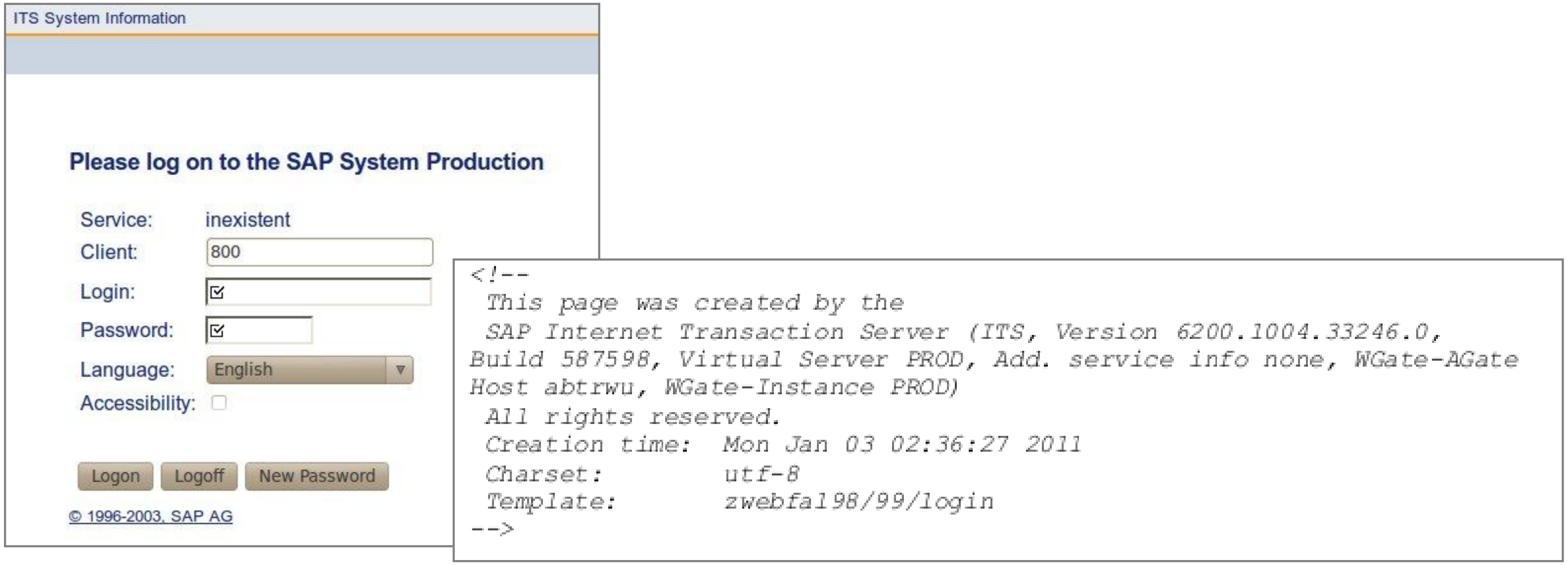
Protection / Countermeasure

- Disable or configure a customized HTTP Server header for the ICM server. Check SAP Note 1329326.
- Disable the Server header in SAP J2EE Engine. Check [1].

Compone	
SAP ITS	
SAP ICM	server: SAP Web Application Server (1.0;640) server: SAP NetWeaver Application Server (1.0;700) server: SAP NetWeaver Application Server / ABAP 701 server: SAP NetWeaver Application Server 7.10 / ICM 7.10
SAP J2EE Engine (EP)	Server: SAP J2EE Engine/700 Server: SAP NetWeaver Application Server 7.10 / AS Java 7.10

Exploration through Error Messages

- By triggering special requests it's also possible to fingerprint the SAP components in use and obtain configuration information about them.
- **SAP ITS:**
  - Triggering of a non existent service (*/scripts/wgate/inexistent/!*) shows an error message or logon screen.
  - Analyzing the source code, it's also possible to obtain the exact ITS version.



ITS System Information

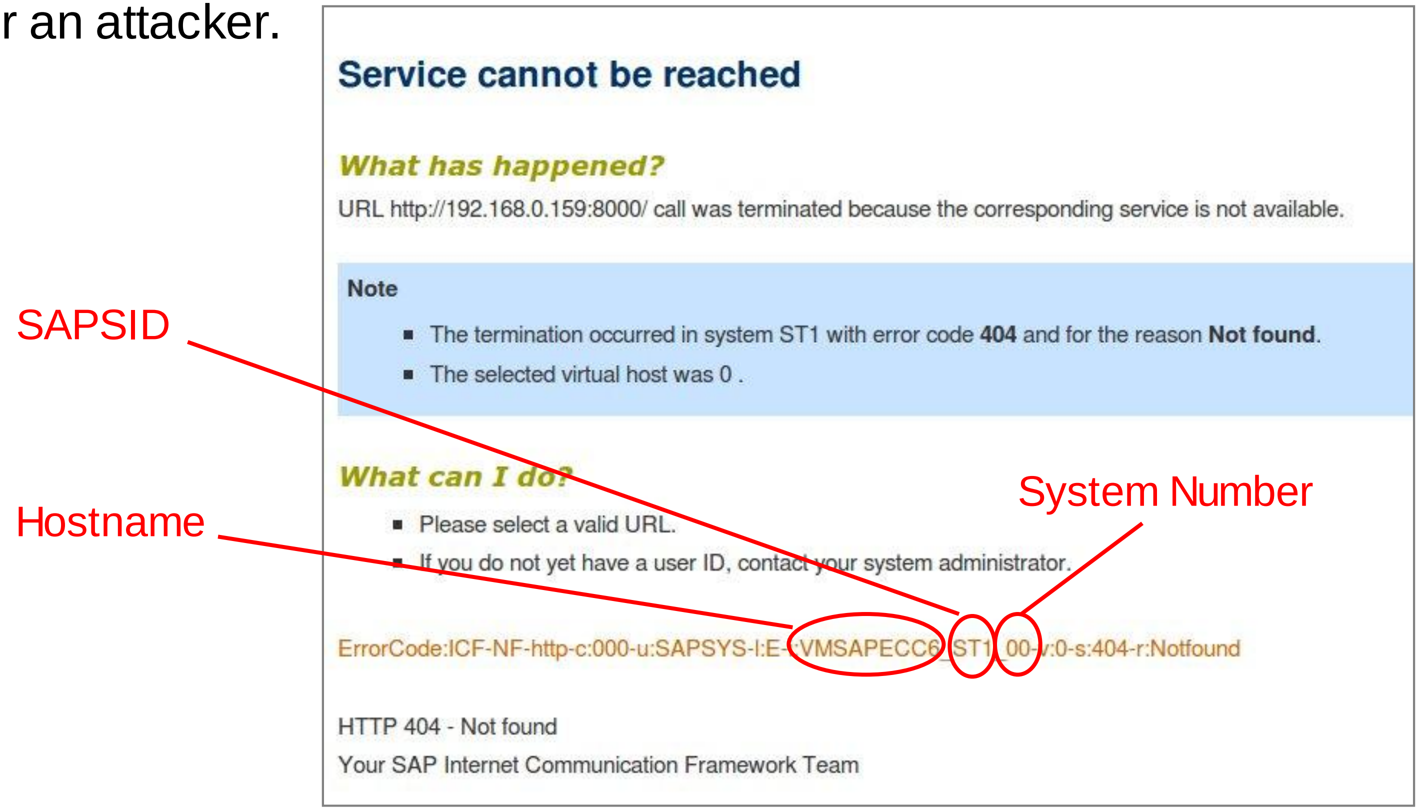
Please log on to the SAP System Production

Service:	inexistent
Client:	800
Login:	☑
Password:	☑
Language:	English
Accessibility:	□

```
<!--
 This page was created by the
 SAP Internet Transaction Server (ITS, Version 6200.1004.33246.0,
Build 587598, Virtual Server PROD, Add. service info none, WGate-AGate
Host abtrwu, WGate-Instance PROD)
 All rights reserved.
 Creation time:  Mon Jan 03 02:36:27 2011
 Charset:        utf-8
 Template:       zwebfal98/99/login
-->
```

Exploration through Error Messages

- **SAP ICM:**
  - By default, HTTP 404 and 403 messages disclose information that can be useful for an attacker.



Service cannot be reached

What has happened?

URL http://192.168.0.159:8000/ call was terminated because the corresponding service is not available.

Note

- The termination occurred in system ST1 with error code **404** and for the reason **Not found**.
- The selected virtual host was 0 .

What can I do?

- Please select a valid URL.
- If you do not yet have a user ID, contact your system administrator.

ErrorCode:ICF-NF-http-c:000-u:SAPSYS-l:E-t:VMSAPECC6_ST1_00-v:0-s:404-r:Notfound

HTTP 404 - Not found
Your SAP Internet Communication Framework Team

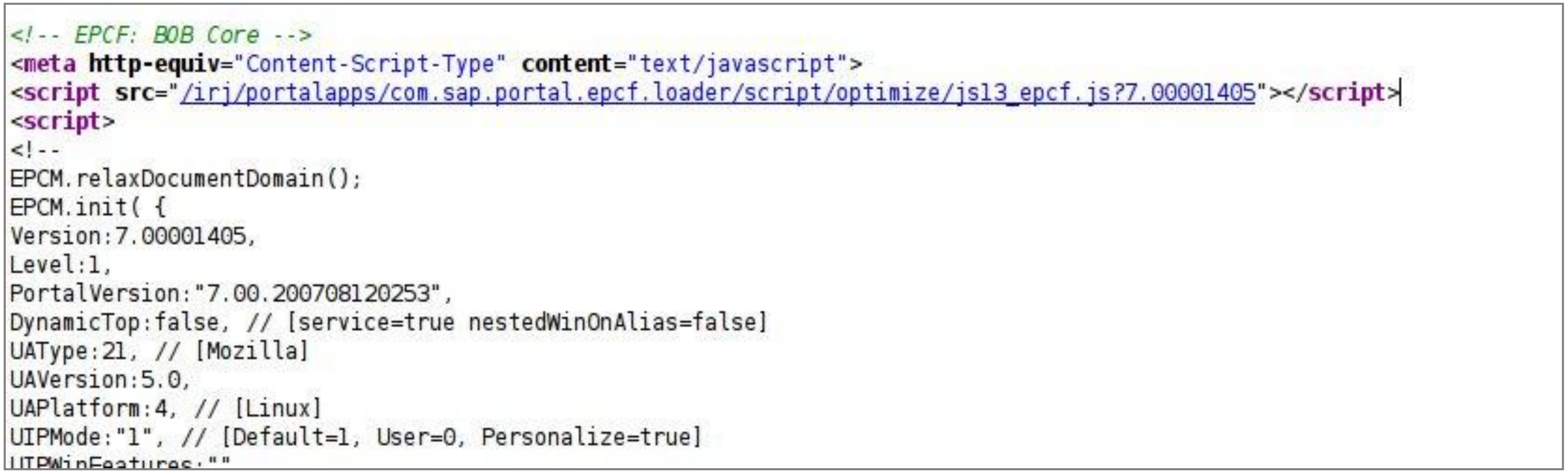
SAPSID

Hostname

System Number

Exploration through Error Messages

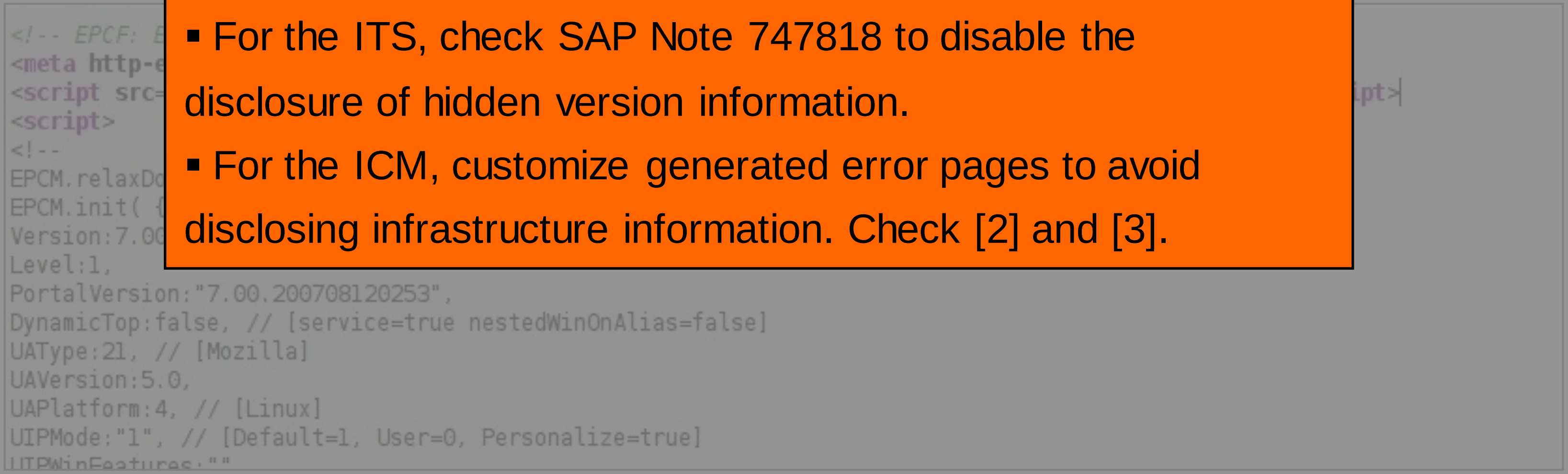
- **SAP Enterprise Portal:**
  - By default, an attacker can obtain Enterprise Portal’s version by checking the source code of generated HTML pages.



```
<!-- EPCF: BOB Core -->
<meta http-equiv="Content-Script-Type" content="text/javascript">
<script src="/irj/portalapps/com.sap.portal.epcf.loader/script/optimize/js13_epcf.js?7.00001405"></script>
<script>
<!--
EPCM.relaxDocumentDomain();
EPCM.init( {
Version:7.00001405,
Level:1,
PortalVersion:"7.00.200708120253",
DynamicTop:false, // [service=true nestedWinOnAlias=false]
UAType:21, // [Mozilla]
UAVersion:5.0,
UAPlatform:4, // [Linux]
UIPMode:"1", // [Default=1, User=0, Personalize=true]
UIPWinFeatures:""
```

Exploration through Error Messages

- **SAP Enterprise Portal:**
  - By default, an attacker can obtain Enterprise Portal’s version by checking the source code of generated HTML pages



```
<!-- EPCF: E
<meta http-e
<script src=                                                                                   ipt>
<script>
<!--
EPCM.relaxDo
EPCM.init( {
Version:7.00
Level:1,
PortalVersion:"7.00.200708120253",
DynamicTop:false, // [service=true nestedWinOnAlias=false]
UAType:21, // [Mozilla]
UAVersion:5.0,
UAPlatform:4, // [Linux]
UIPMode:"1", // [Default=1, User=0, Personalize=true]
UIPWinFeatures:""
```

Protection / Countermeasure

- For the ITS, check SAP Note 747818 to disable the disclosure of hidden version information.
- For the ICM, customize generated error pages to avoid disclosing infrastructure information. Check [2] and [3].

Attacks to the ICM: Dangerous ICF services

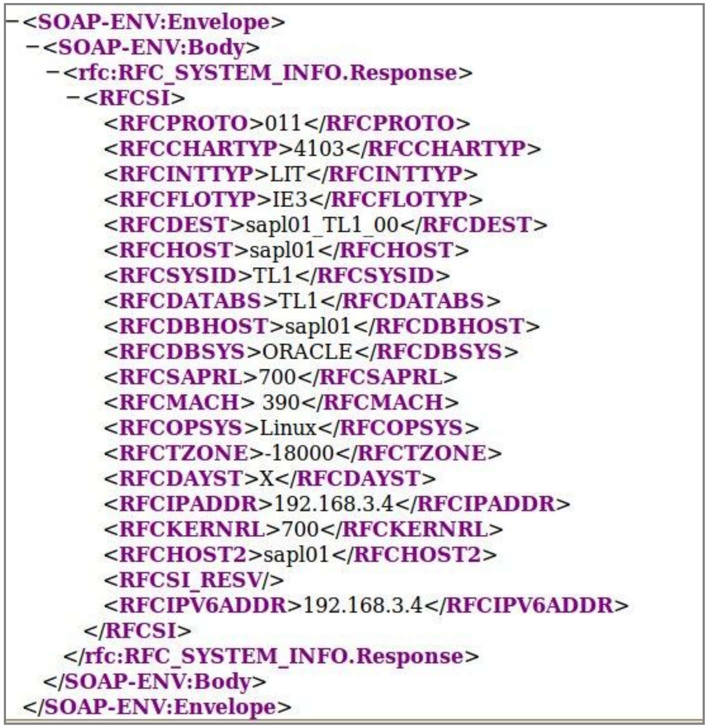
- There are **over 1500 standard ICF services** in a typical SAP ECC installation.
- They would be the equivalent to *.asp* or *.php* pages.
- **Each of these services is an access point into the system**, receiving parameters and performing actions based on them.

- When a request for a service is received, the following procedure takes place:
  - The framework checks if the service is *private* or *public.*
    1. If public, the service is executed directly.
    2. If not, the service is checked for stored Logon Data or Client Certificate.
    3. If none is configured, the defined authentication mechanisms take place.
    4. After authentication, the ICF authorization check is performed.
    5. The service code is executed.

- Most services require authentication.

Attacks to the ICM: The Info Service

- A quick example of a dangerous public ICF service.
- Accessible at */sap/public/info*
- Returns sensitive information about the SAP platform (anonymously!).



```
-<SOAP-ENV:Envelope>
  -<SOAP-ENV:Body>
    -<rfc:RFC_SYSTEM_INFO.Response>
      -<RFCSI>
          <RFCPROTO>011</RFCPROTO>
          <RFCCHARTYP>4103</RFCCHARTYP>
          <RFCINTTYP>LIT</RFCINTTYP>
          <RFCFLOTYP>IE3</RFCFLOTYP>
          <RFCDEST>sapl01_TL1_00</RFCDEST>
          <RFCHOST>sapl01</RFCHOST>
          <RFCSYSID>TL1</RFCSYSID>
          <RFCDATABS>TL1</RFCDATABS>
          <RFCDBHOST>sapl01</RFCDBHOST>
          <RFCDBSYS>ORACLE</RFCDBSYS>
          <RFCSAPRL>700</RFCSAPRL>
          <RFCMACH> 390</RFCMACH>
          <RFCOPSYS>Linux</RFCOPSYS>
          <RFCTZONE>-18000</RFCTZONE>
          <RFCDAYST>X</RFCDAYST>
          <RFCIPADDR>192.168.3.4</RFCIPADDR>
          <RFCKERNRL>700</RFCKERNRL>
          <RFCHOST2>sapl01</RFCHOST2>
          <RFCSI_RESV/>
          <RFCIPV6ADDR>192.168.3.4</RFCIPV6ADDR>
        </RFCSI>
      </rfc:RFC_SYSTEM_INFO.Response>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
```

Attacks to the ICM: An Explosive Combination

- Most of the services require authentication.
- Once the user is authenticated, the system checks if he has the authorization object S_ICF configured to the Authorization value of the requested service.

- **Problem #1: By default, ICF services are not assigned an Authorization value** -> The authorization check does not apply!
- This means that *the attacker only needs a user account in the system, and he will be able to execute many functionalities* (only subject to code-level authorizations).

- **Problem #2: Standard users with default passwords**. Many SAP systems are shipped with users with default passwords, such as SAP*, DDIC, EARLYWATCH, SAPCPIC and TMSADM.

- **Problem #3: The attacker is able to control which client to connect to!**

The attacker has fair chances of accessing sensitive business functionality through the ICM server.

Attacks to the ICM: The SOAP RFC Service

- The RFC protocol is used to call ABAP Function Modules in remote SAP servers.

- We have researched on threats to this interface since 2007 (BlackHat Europe).

- This protocol is (usually) not accessible from the Internet.

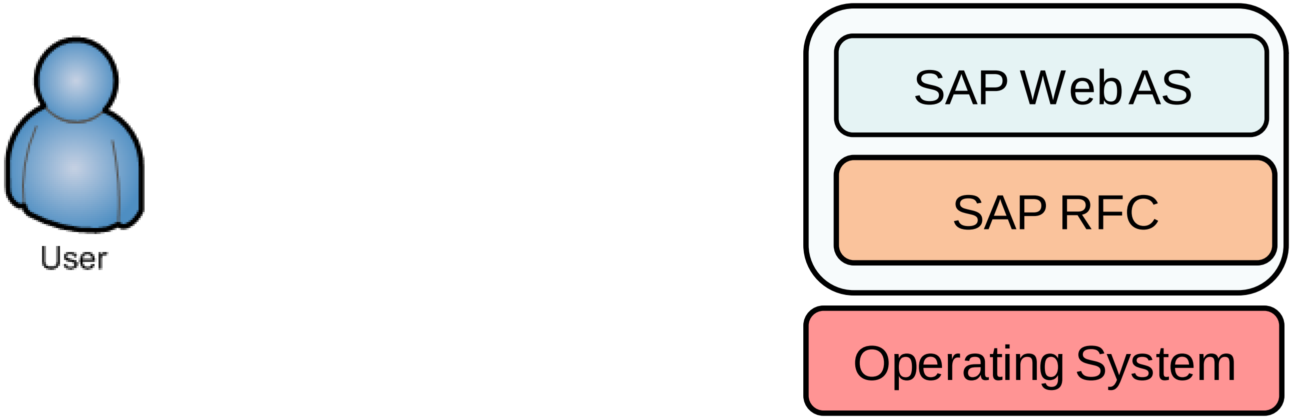
- But …**there is an ICF Service that can be used to perform RFC calls**.

- **If this service is enabled, an attacker can perform RFC calls to the SAP Web Application Server, just as he was sitting in the local network!**

Attacks to the ICM: The SOAP RFC Service

User
SAP Web
Application Server

Attacks to the ICM: The SOAP RFC Service



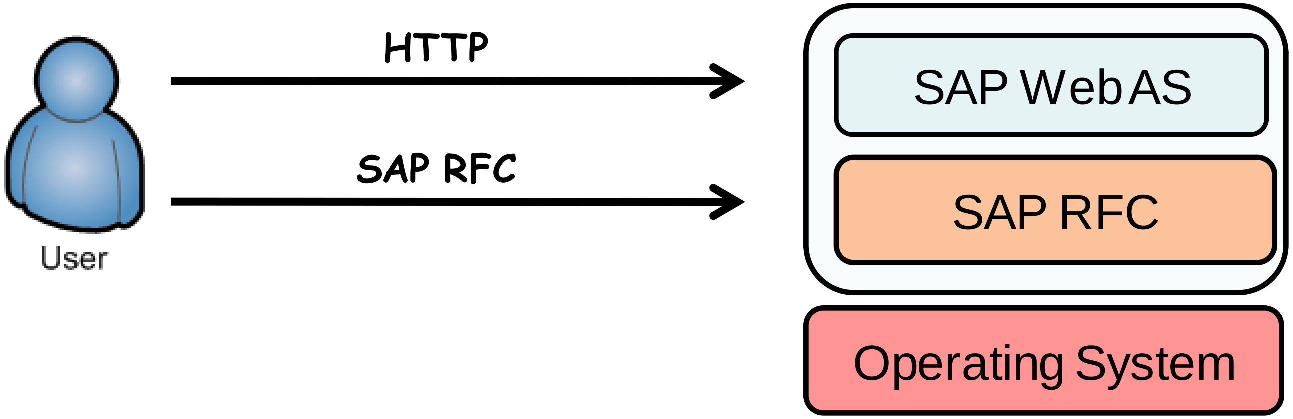
User

SAP Web AS

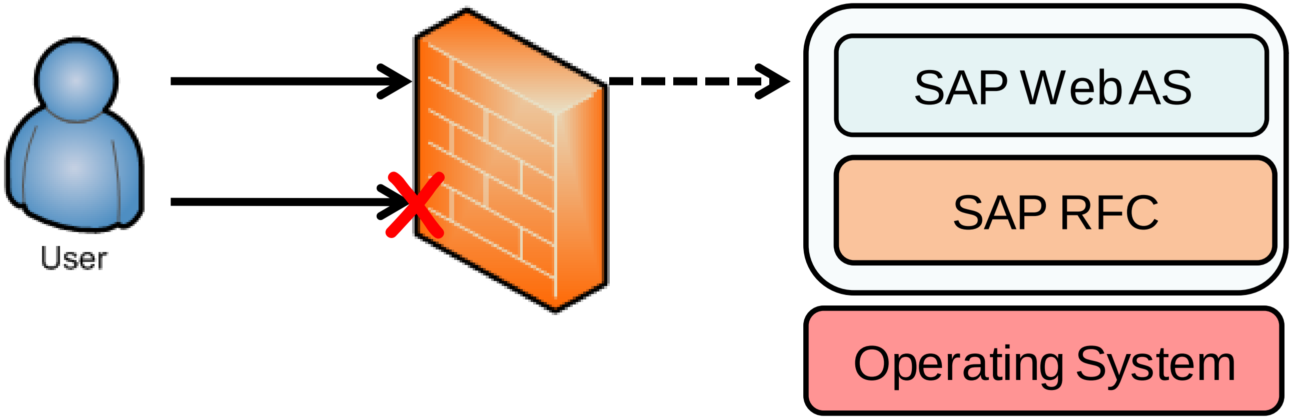
SAP RFC

Operating System

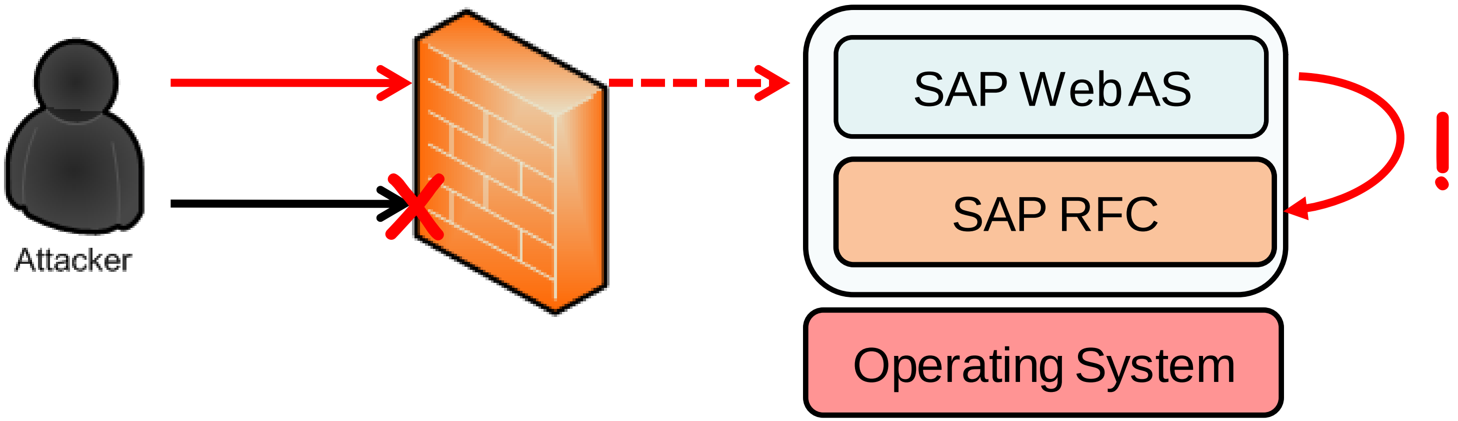
Attacks to the ICM: The SOAP RFC Service



Attacks to the ICM: The SOAP RFC Service



Attacks to the ICM: The SOAP RFC Service



Live demo #1

Attacks through the SOAP RFC Service

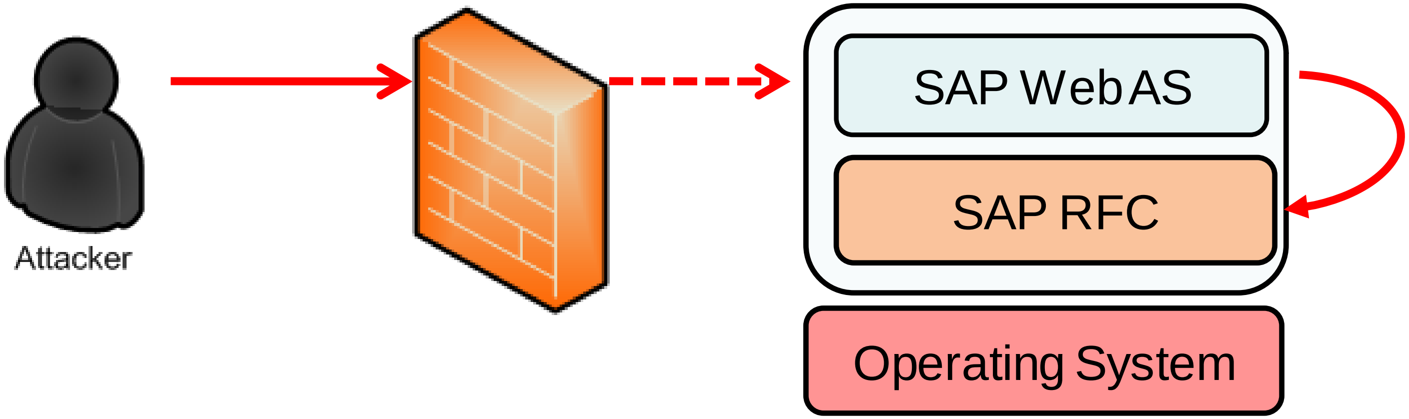
The finger –l @SAP for the Web

Live demo #2

Attacks through the SOAP RFC Service

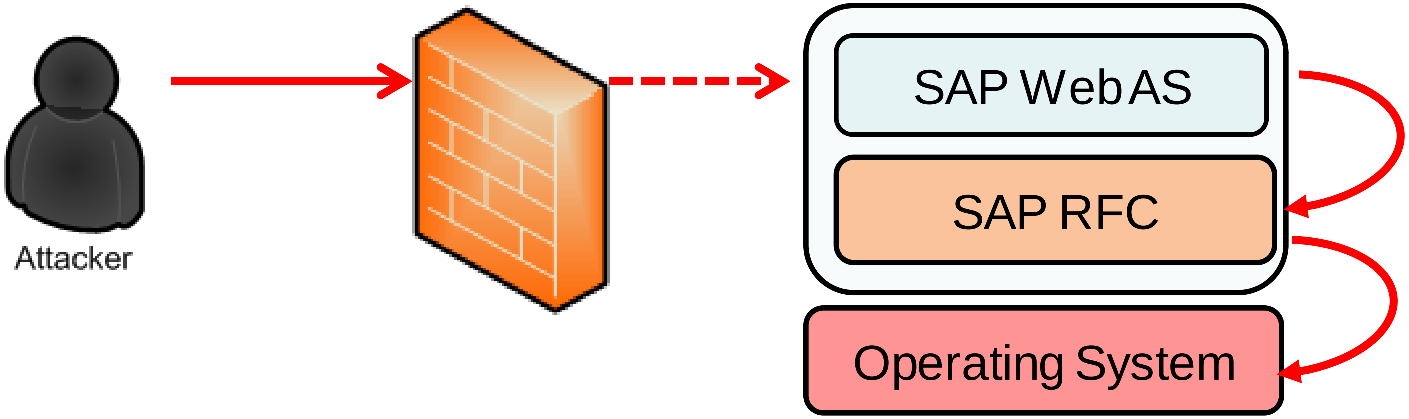
From the Web to the Shell

Wait a minute…What has just happened?



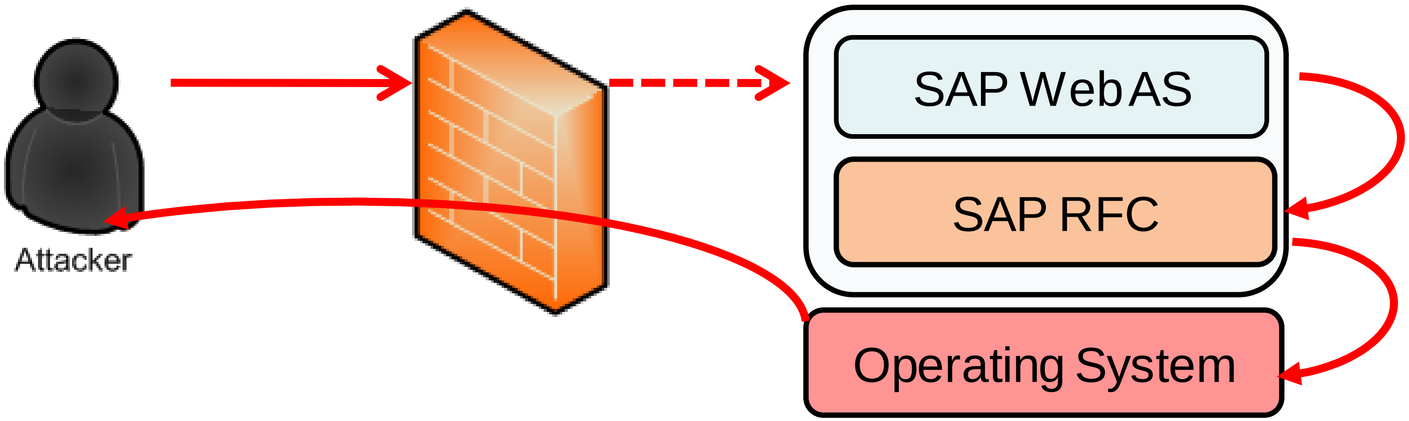
- The attacker sends a SOAP request to run the TH_GREP function module.
- This function module is used to search for strings in files.
- It can be executed by the EARLYWATCH user (!)
- Joris van de Vis discovered a command injection vulnerability in this module.

Wait a minute…What has just happened?



- The attacker can then execute arbitrary commands in the SAP operating system.

Wait a minute…What has just happened?



- He exports the DISPLAY and executes an *xterm* (yes, *so old-school*!)
- **The attacker does not require outbound connectivity**:
  - The attacker is running commands as the SAP administrator (<sid>adm).
  - He can connect to the database as DBA.
  - He is GOD.

Live demo #3

Attacks through the SOAP RFC Service

Espionage Attacks to the Business

Live demo #4

Attacks through the SOAP RFC Service

Espionage Attacks to the Business

Protection / Countermeasure

- Make sure that standard users don’t have default passwords. You can use report RSUSR003.
- Disable any ICF service that is not enabled due to business requirements. Check SAP Note 1498575 and [4].
- Protect against TH_GREP vulnerability applying SAP Note 1433101.
- Maintain ICF Authorization Data as described in [5] and [6].

Attacks to “Secured” Enterprise Portals

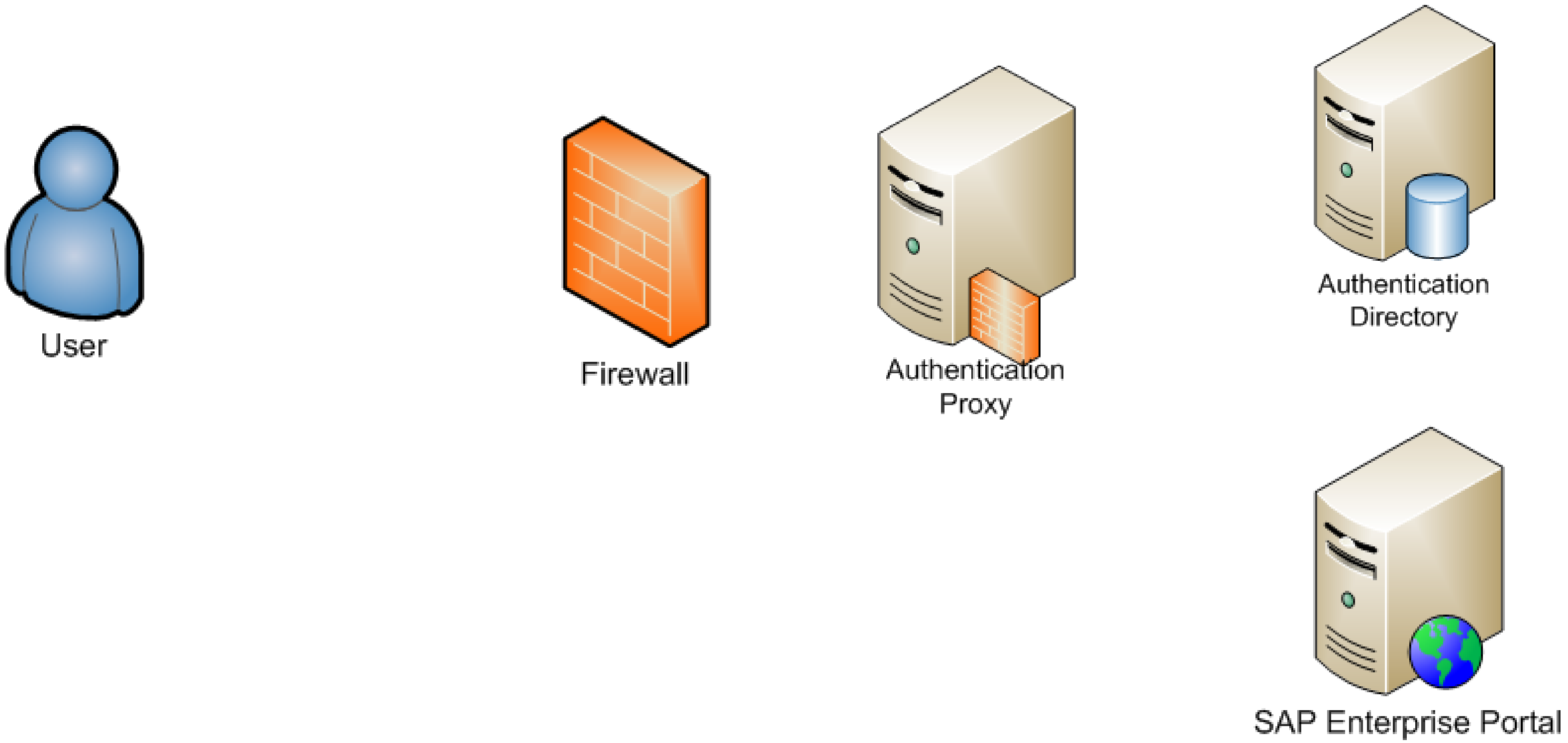
- **SAP Enterprise Portal supports different authentication mechanisms**, such as User & Password, X.509 Client Certificates, Logon Tickets, Kerberos, etc…
- The authentication is handled by the SAP J2EE Engine.

- Many organizations already have Web Access Management (WAM) solutions in place, providing two-factor authentication mechanisms.
- They use them to enable ***secured* access** to the systems (tokens, biometrics, etc) and Single-Sign On.
- **Some examples:**
  - RSA ClearTrust
  - CA SiteMinder
  - Oracle Oblix
  - Entrust GetAccess
  - Microsoft Integrated Windows Authentication (now deprecated)

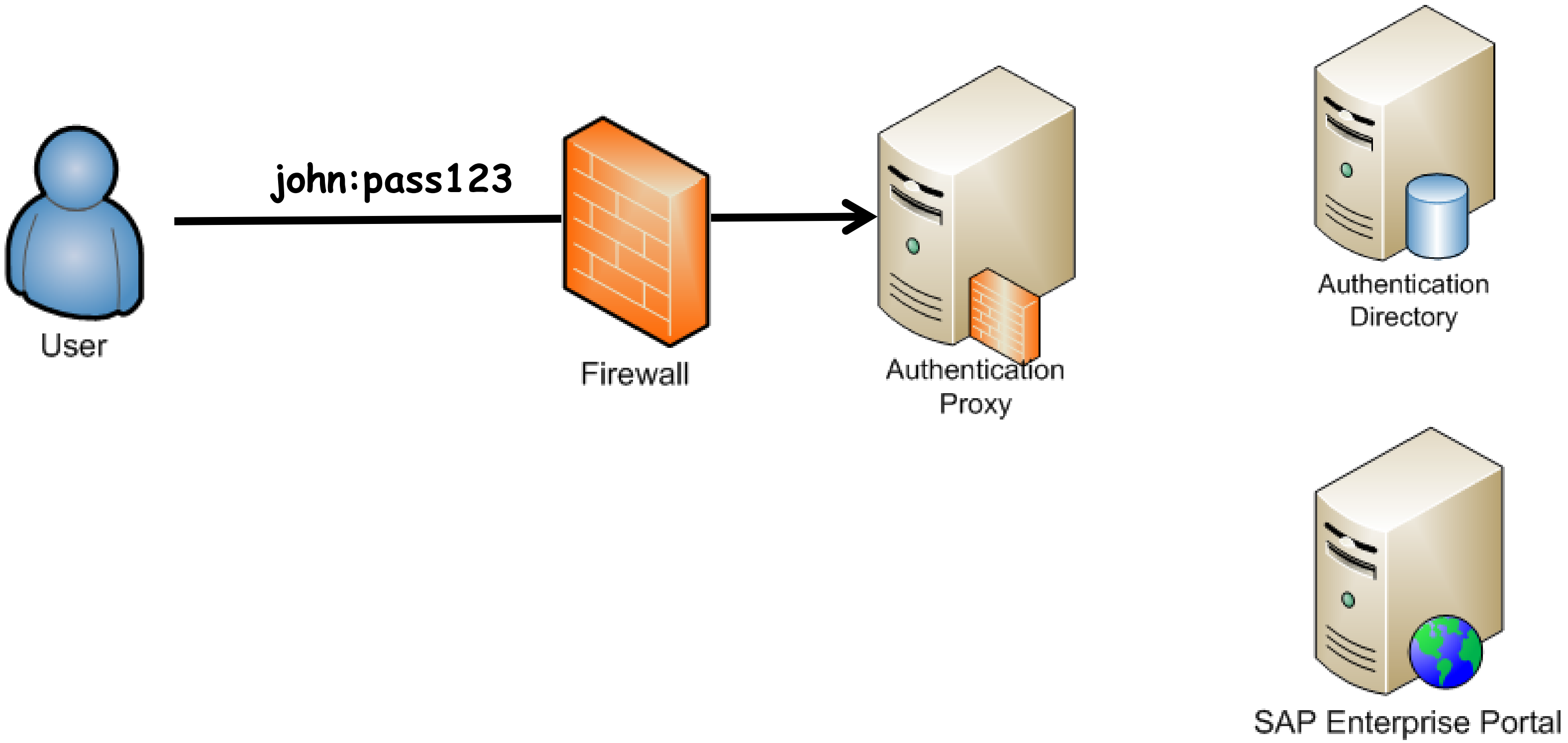
A Special Authentication Scheme

- The Portal is integrated with these solutions, by using the Header Variables Login Module.
- In these scenarios, the authentication procedure works a follow:
    1. The user provides authentication information to the EAM/WAM solution.
    2. The solution checks provided credentials.
    3. If successful, connects to the Enterprise Portal and sends the user to authenticate in a HTTP header.
    4. The Enterprise Portal verifies that the user is valid (it exists), and returns an SAP SSO logon ticket to the user.
    5. The user is authenticated.

The Header Authentication Scheme

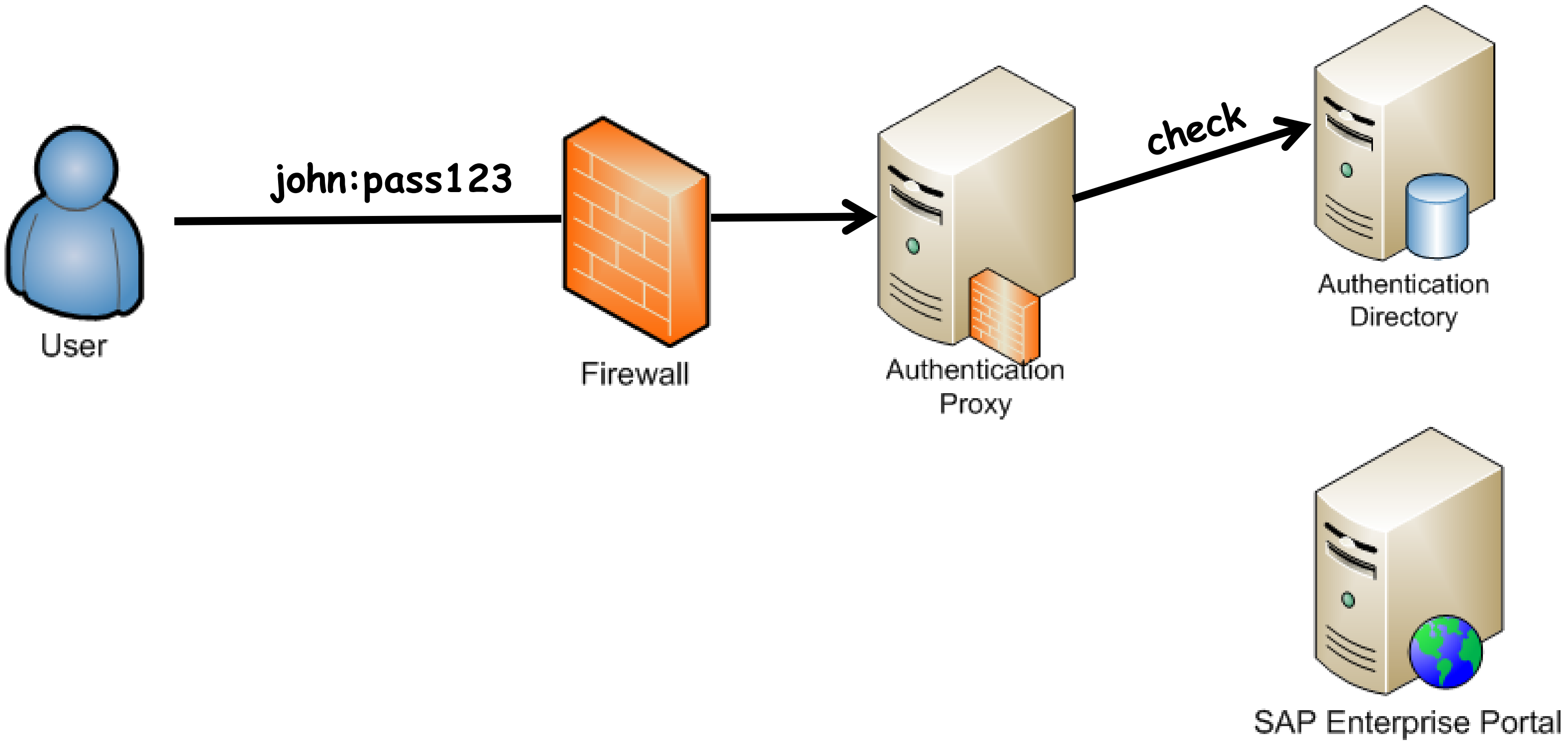


The Header Authentication Scheme



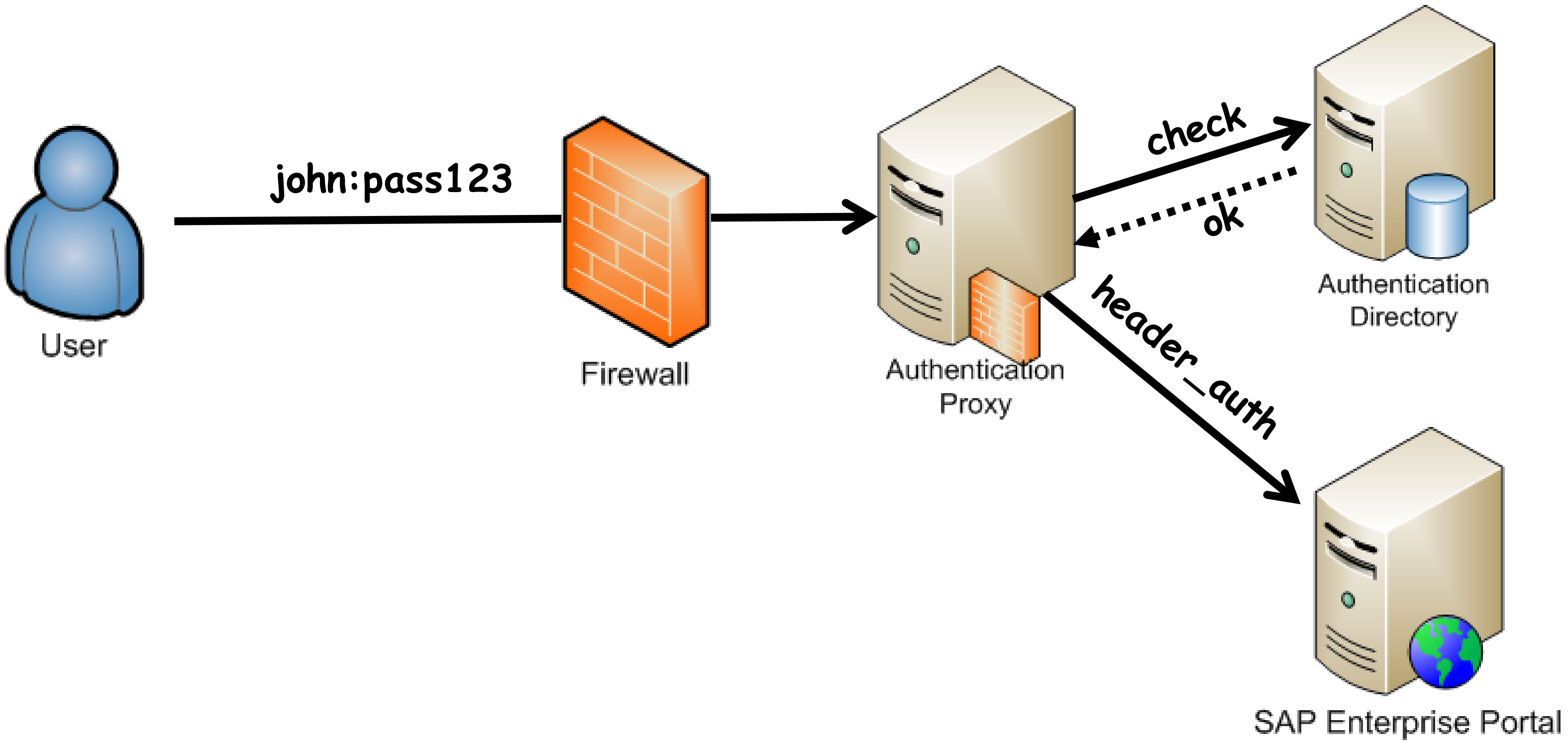
1. The user provides authentication information to the EAM/WAM solution.

The Header Authentication Scheme



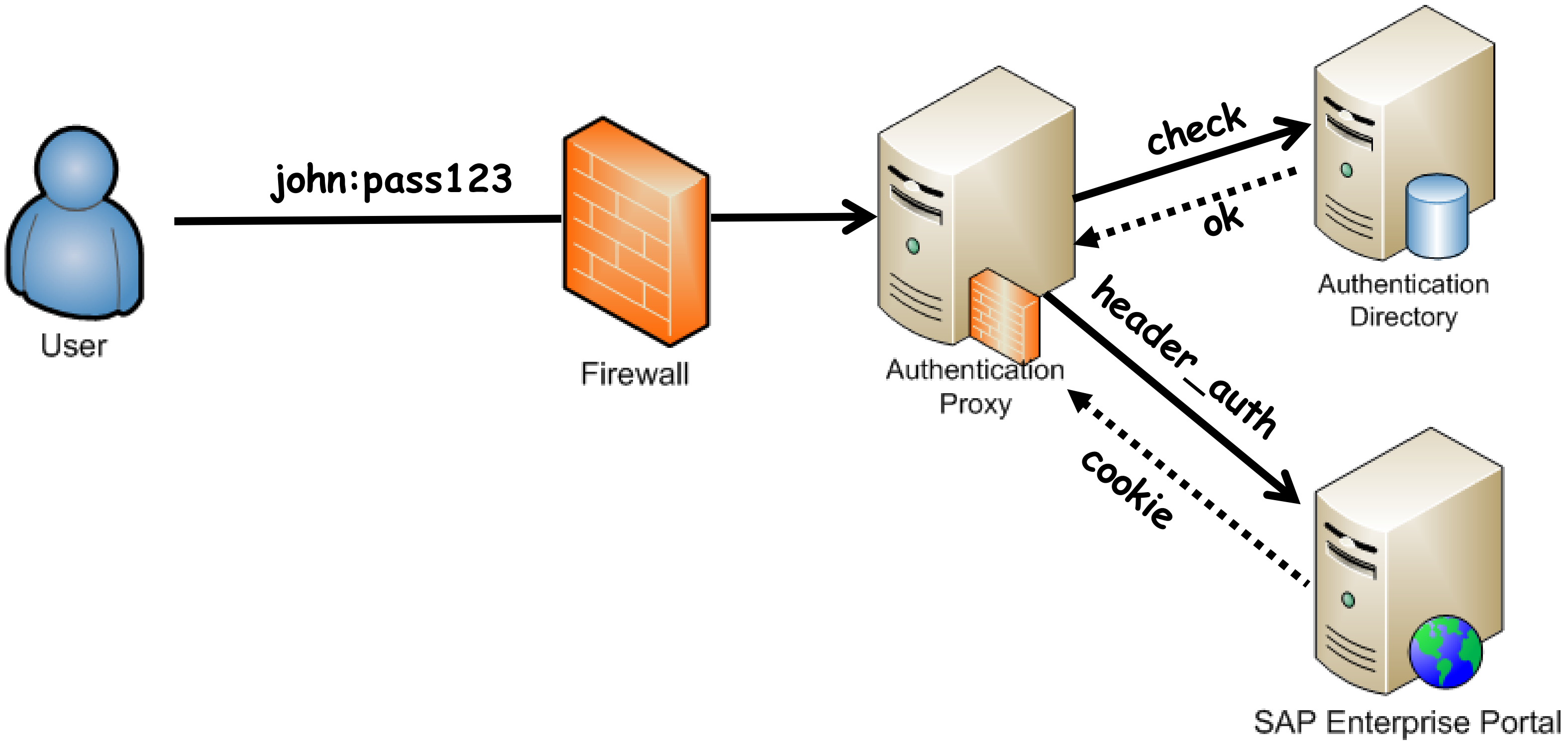
2. The solution checks provided credentials.

The Header Authentication Scheme



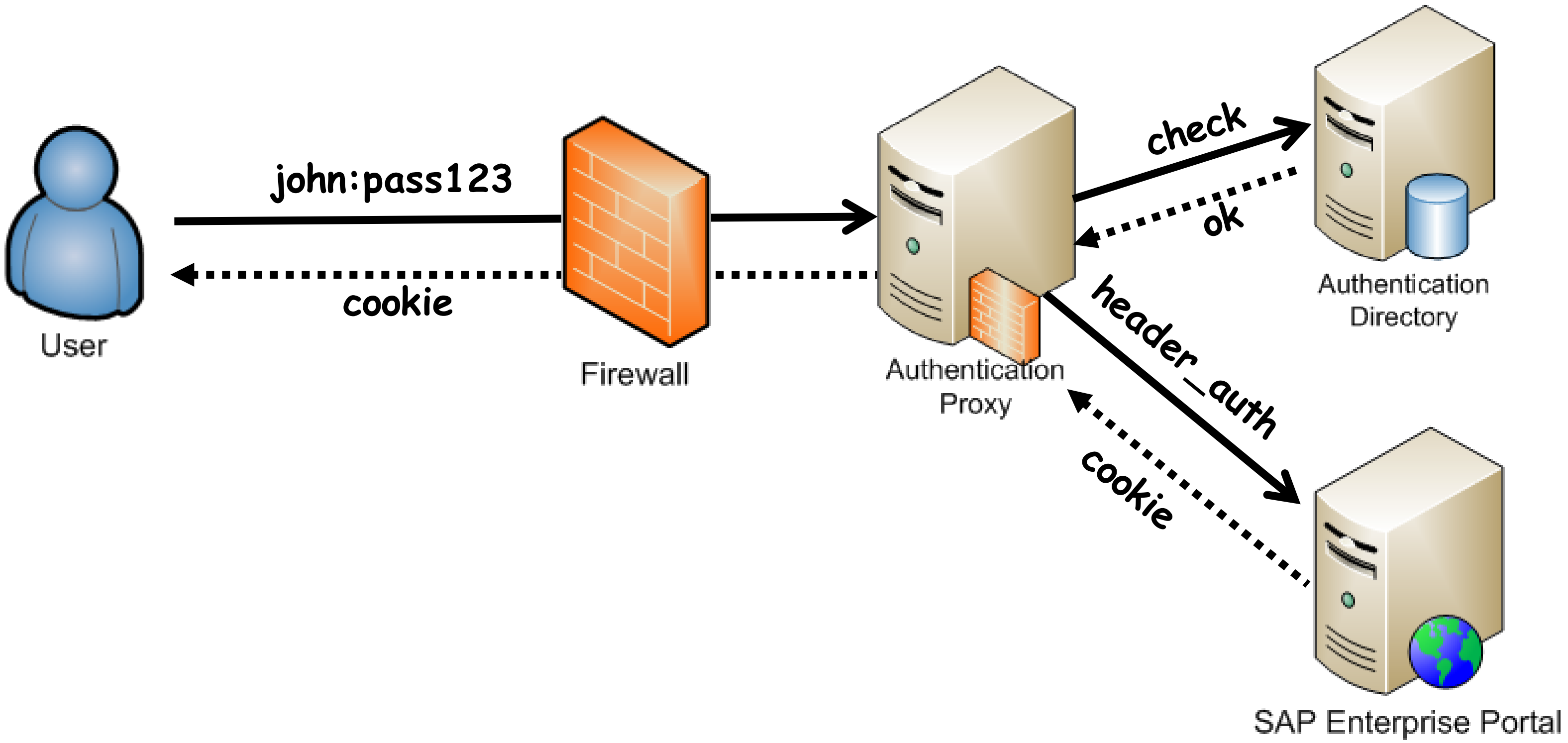
3. If successful, connects to the Enterprise Portal and sends the user to authenticate in a HTTP header.

The Header Authentication Scheme



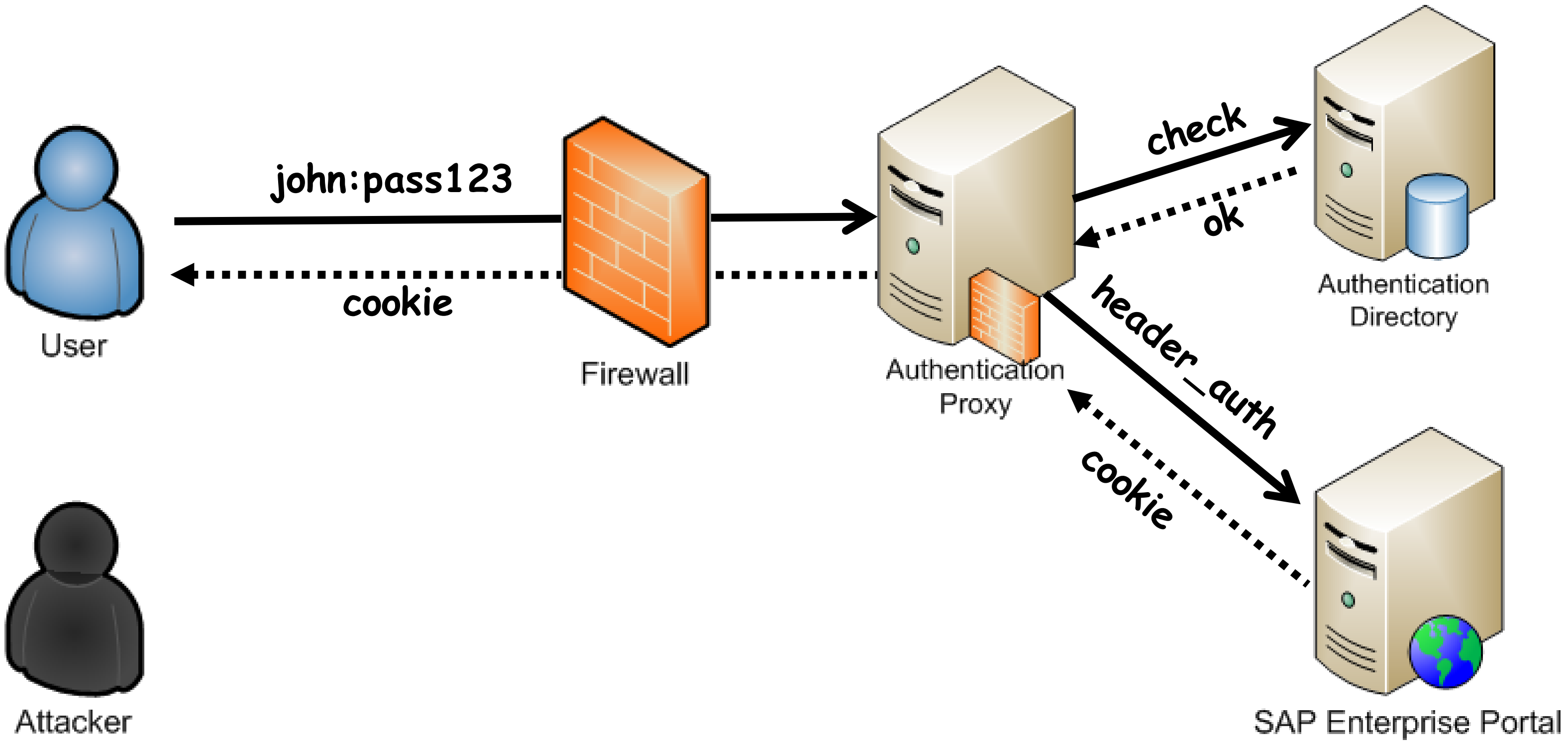
4. The Enterprise Portal verifies that the user is valid (it exists), and returns an SAP SSO logon ticket to the user.

The Header Authentication Scheme



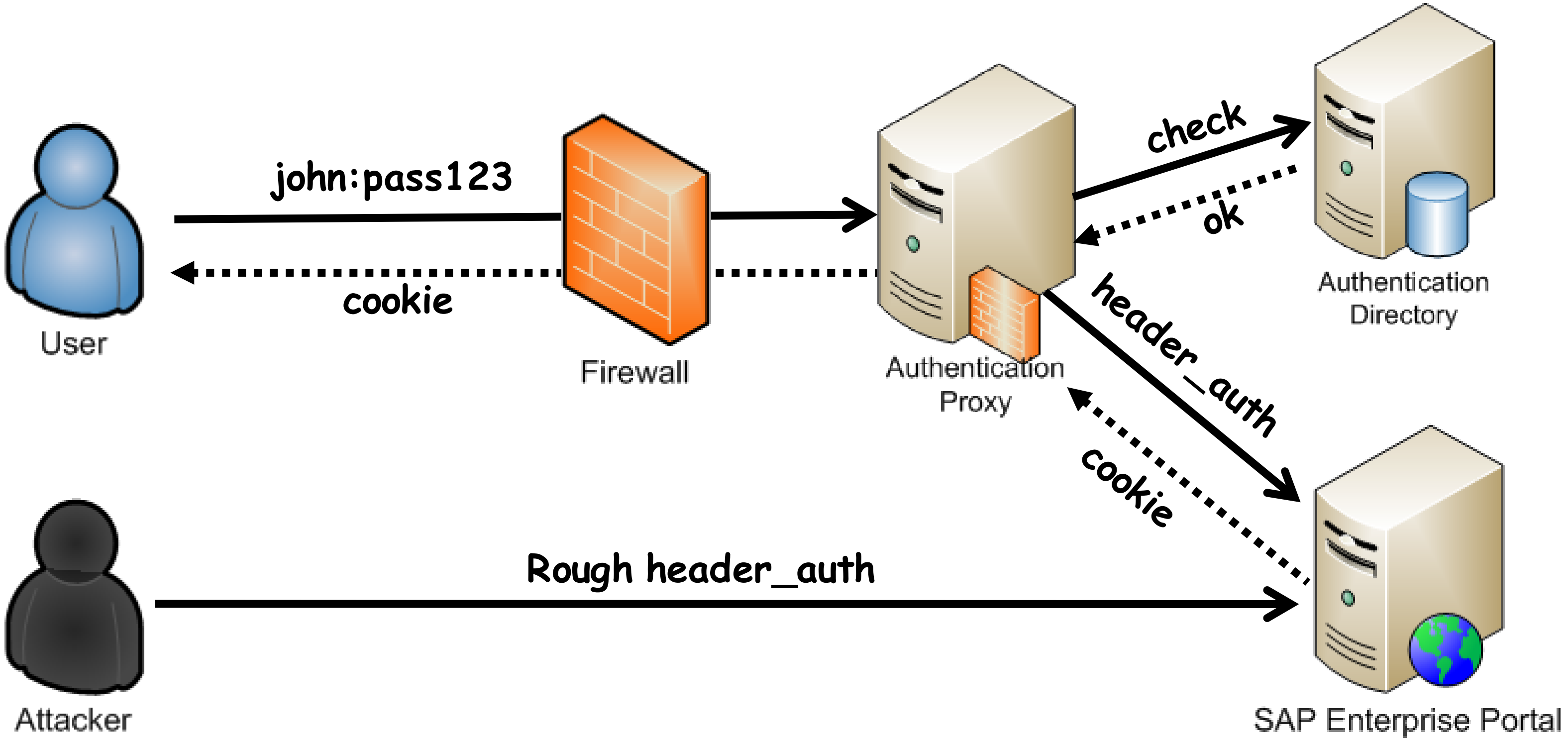
5. The user is authenticated.

The Attack



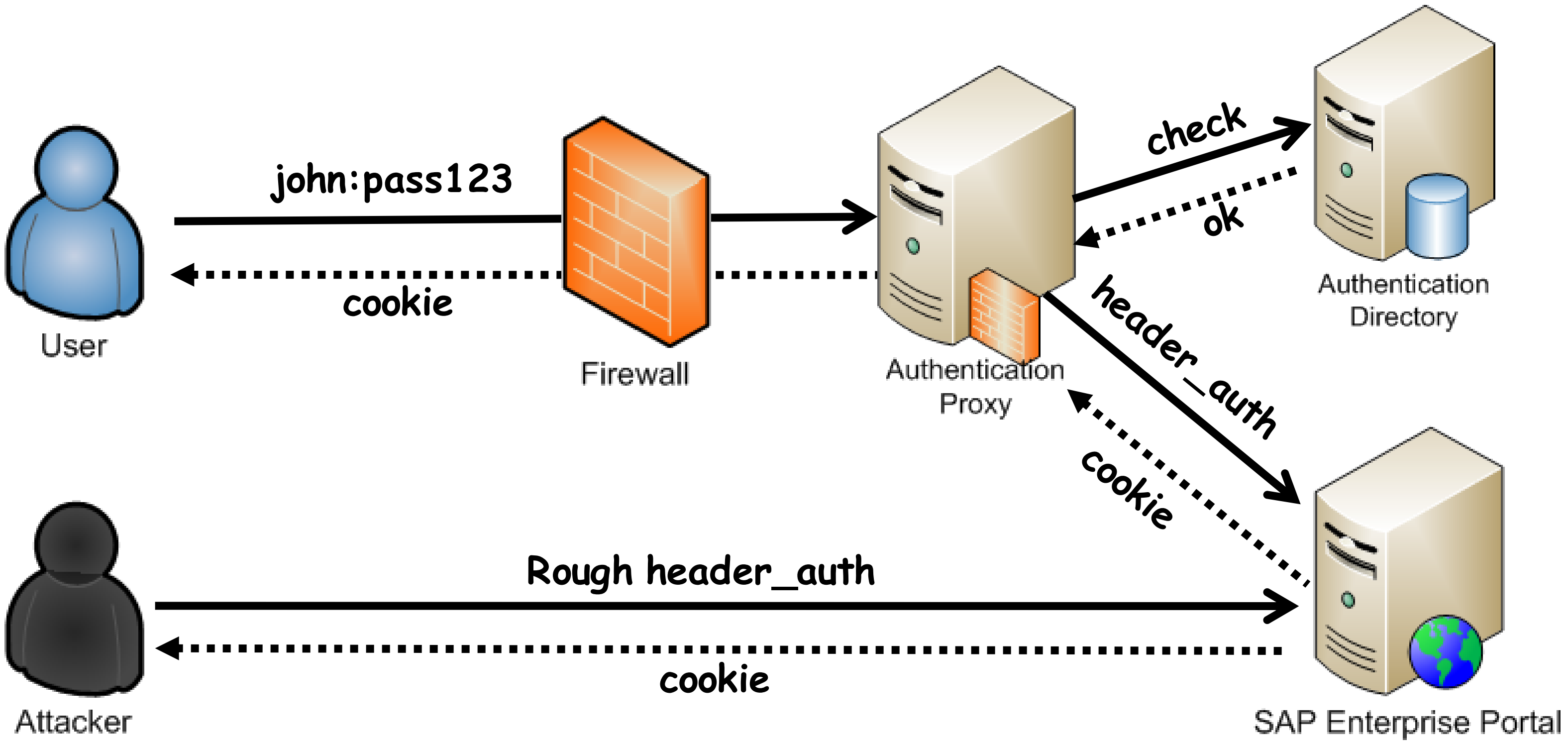
If the attacker can connect directly with the SAP Enterprise Portal, nothing prevents him from impersonation the EAM/WAM solution!

The Attack



If the attacker can connect directly with the SAP Enterprise Portal, nothing prevents him from impersonation the EAM/WAM solution!

The Attack



After my research and discovery, I found out this was documented since 2006 (!)

Live demo #5

Bypass of “secured” SAP Portal authentication

One HTTP header to rule them all

Protection / Countermeasure

- Implement proper network filters to avoid direct connections to the SAP J2EE Engine.
- If using it for Windows authentication, switch to the *SPNegoLoginModule*.
- Check [7].

Post-exploitation: SAPPortalShell

- **After the attacker has compromised the SAP Enterprise Portal**, he would try to install a backdoor to secure future access or expand influence.
- The Enterprise Portal's core is the Portal Runtime (PRT).
- The PRT serves Portal Applications, composed of:
  - Portal Components
  - Portal Services

- A Portal Application is packaged into a PAR file and deployed to the server.
- **If the attacker has full control over the system, nothing prevents him from deploying his own PAR files.**

Live demo #6

SAP Enterprise Portal Backdoors

The SAPPortalShell

Other Attacks

- Beyond the described attacks, **several other vulnerabilities** have been discovered in Web components and **can be exploited if not patched/protected**:
    - FX's exploits affecting old ITS versions (great Unicode payload)
    - Alexander Polyakov and guys from DSecRG (XSS, ActiveX, DoS and a BoF)
    - Onapsis Research Labs (BoF, DoS, Path Traversals, XSS, Open Redirects)

- More dangerous ICF services not covered in this talk (time constrains).
- Many other Web security vulnerabilities reported by us. Waiting for patches to be ready.

Conclusions

Wrapping Up

- Driven by modern business requirements, **many SAP systems are** nowadays **connected to the Internet** and untrusted networks (vendors, partners, etc).

- This situation drastically **increases the risk**, as the universe of possible cyber attackers is widened and the chances to catch them, reduced.

- SAP has different kind of Web technologies, each of them comprising their own specific security architectures and features. **It's imperative to understand the internals of these components to know how to secure them**.

- **SAP is taking proactive steps into increasing the security of its customers' systems** (security guides, regular patches, new standards).

Wrapping Up

- **The attacks** described would be **successful only if the organization is not following SAP's security recommendations**.

- **SAP systems should never be directly connected to the Internet**. If you required Web access, implement a reverse proxy/WAF solution in front of it.

- **By exploiting vulnerabilities in SAP Web components, a remote anonymous attacker can get complete control of the internal SAP servers and perform espionage, sabotage and fraud attacks**.

- It's not possible to do proper **risk management** being unaware of the threats we are facing. The objective analysis of this problematic is **the only sustainable strategy to increase the security of business-critical systems**.

References

1. http://help.sap.com/saphelp_nw73/helpdata/en/55/4202bc3067492aa6887bcd97ed76a6/frameset.htm
2. http://help.sap.com/saphelp_nw73/helpdata/en/48/69efc9e8a607d6e10000000a42189c/frameset.htm
3. http://help.sap.com/saphelp_nw73/helpdata/en/48/45acaf43a64bb8e10000000a42189b/frameset.htm
4. http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/f0d2445f-509d-2d10-6fa7-9d3608950fee
5. http://help.sap.com/saphelp_nw70ehp2/helpdata/en/39/e11482b2d23a428e583a59bef07515/frameset.htm
6. http://help.sap.com/saphelp_nw70ehp2/helpdata/en/9f/fc5e900b62d94e8878eb94db5b986f/frameset.htm
7. http://help.sap.com/saphelp_nw70ehp2/helpdata/en/d0/a3d940c2653126e10000000a1550b0/frameset.htm
8. http://www.onapsis.com/x1

Questions?

mnunez@onapsis.com

Thank you!

www.onapsis.com

Follow us on Twitter! @onapsis