SAP Application Security

Your Crown Jewels Online: Further Attacks to SAP Web Applications

Mariano Nunez
CEO – Onapsis, Inc.

Session ID: HT2-301

Session Classification: Lightening Round

RSA CONFERENCE 2012

Agenda

- The evolution of the threats to SAP systems
- The different SAP Web Servers
- Attacks to SAP Web Applications
  - Attacks to the SAP Web Dispatcher
  - Live demo: Business data exfiltration
  - Live demo: Authentication bypass in Enterprise Portals
- Countermeasures

The evolution of the threats to SAP systems

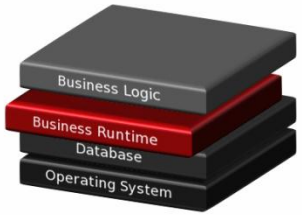
What is SAP?

- Largest provider of business management solutions in the world.

- Used by Fortune-500 world-wide companies, governmental organizations and defense facilities to **run their every-day business-critical processes.**

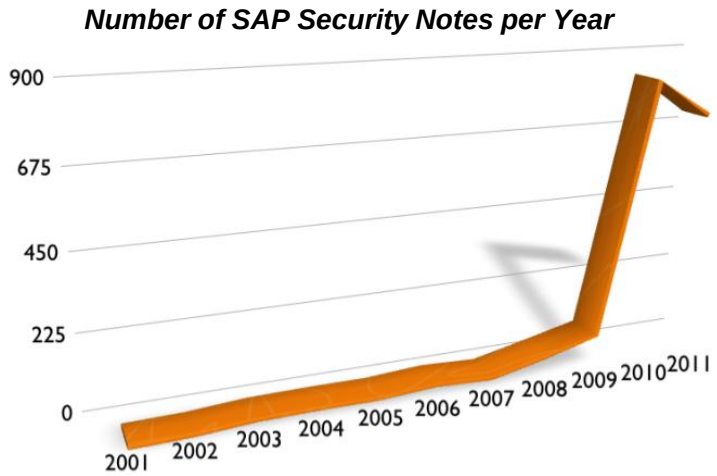
What does “SAP Security” means?

- SAP Security was traditionally regarded as a synonym of “Segregation of Duties controls”.
- But… **SoD controls are not enough!**
- The forgotten layer: The Business Infrastructure (NetWeaver/Basis).
  - Base framework in charge of critical tasks such as authentication, authorization, auditing, logging, etc
  - Can be susceptible of security vulnerabilities that, if exploited, can lead to **espionage, sabotage and fraud** attacks to the business information.



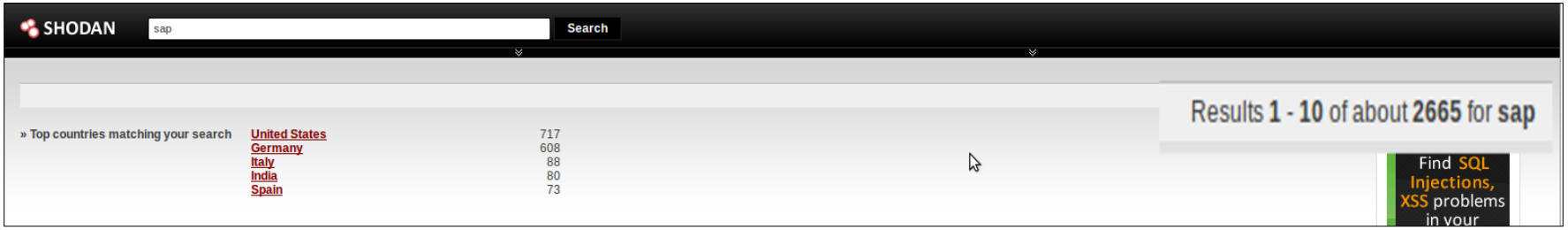
Attacks to the SAP technical layer

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



“My SAP system is only used internally”

- Could be true a decade ago, probably not anymore.
- Attackers can easily find SAP systems online.



The different SAP Web Application Servers

SAP Web Application Servers

- **SAP Internet Transaction Server (ITS)**
  - Released in 1996.
  - Middleware that translates SAP screens to HTML.
- **SAP Web Application Server (WebAS)**
  - The SAP kernel was enhanced to support HTTP(S).
  - Access provided by *ICF services.*
- **SAP Enterprise Portal (EP)**
  - Based in the SAP J2EE Engine.
  - Unique point of Web access to SAP systems.

The SAP Web Dispatcher

- Reverse-proxy mainly used for balancing the load to backend SAP Web servers.
- Based on the ICM framework.
- Features a Web Administration Interface.

If the SAP Web Dispatcher is exploited, all the backend systems can be ultimately compromised.

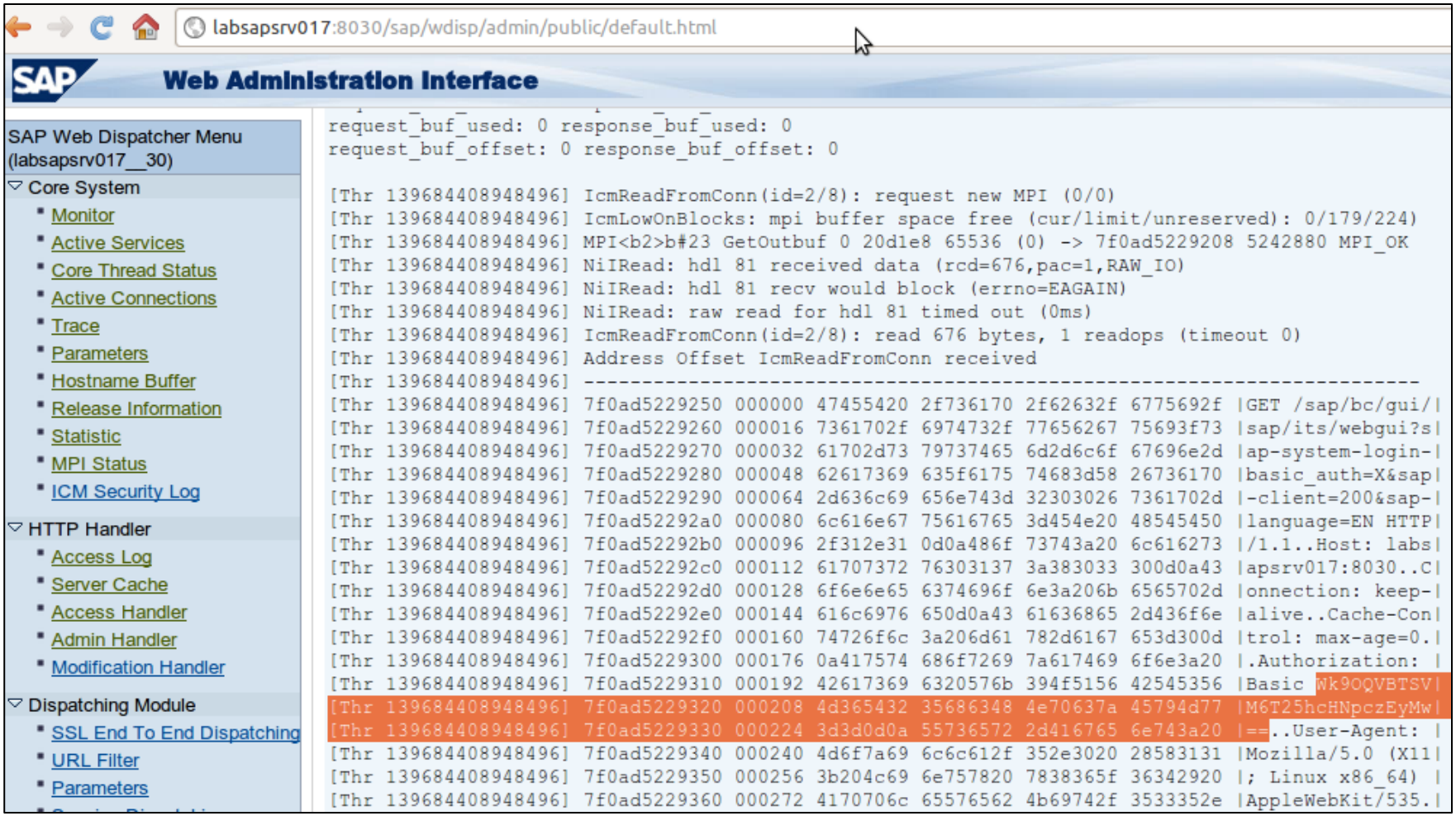
Attacks to SAP Web Applications

Attacks to the SAP Web Dispatcher

- It is possible to identify whether a Web Dispatcher is present by:
  - Analyzing returned HTTP headers
  - Sending specially-crafted requests that trigger error conditions.
  - Trying to access the Administration interface.

- Once compromised, an attacker may increase the *trace level* and obtain valid credentials/ cookies to access the backend systems.

Attacks to the SAP Web Dispatcher

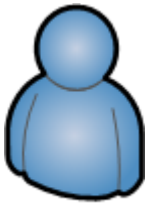


Attacks to the SAP Web Application Server - *Exploitation of RFC over the Internet*

- RFC is a proprietary protocol widely used by SAP. We presented threats and attack vectors in BlackHat 2007.
- This interface is (usually) only accessible internally.
- But… there is an ICF Service that can be used to perform RFC calls.

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

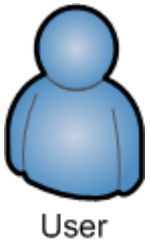
Attacks to the SOAP RFC Service

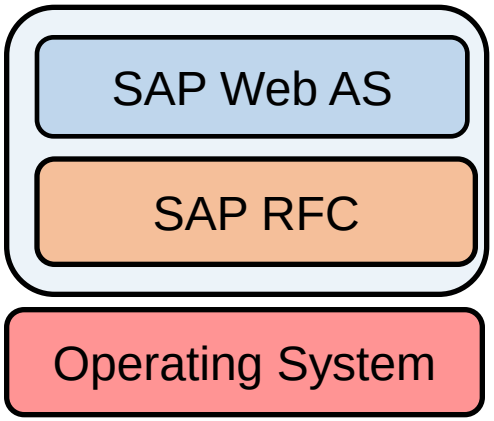


User

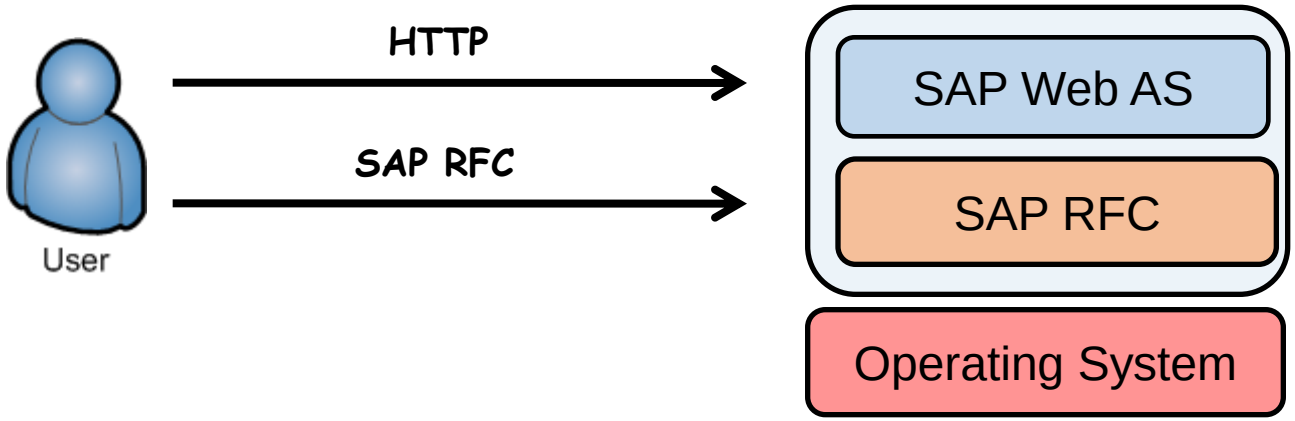
SAP Web
Application Server

Attacks to the SOAP RFC Service

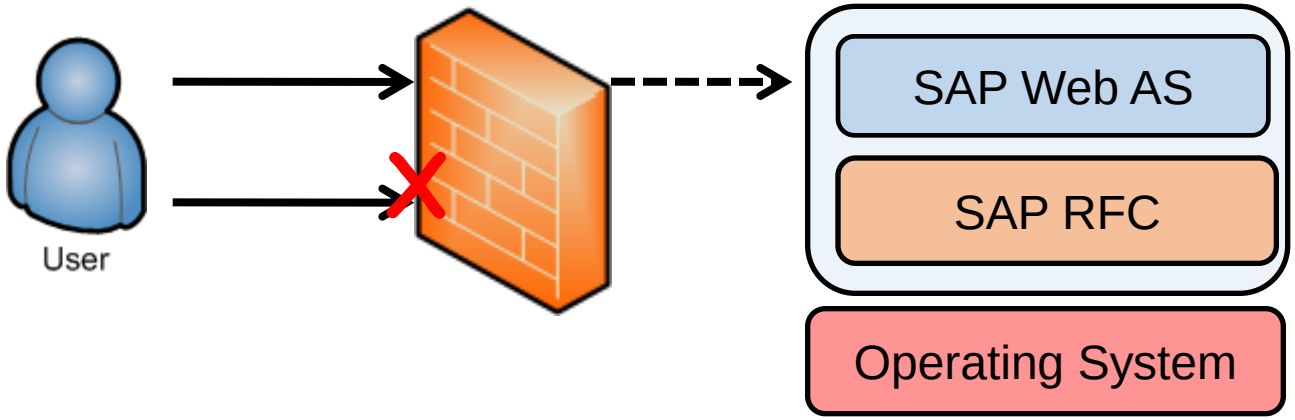




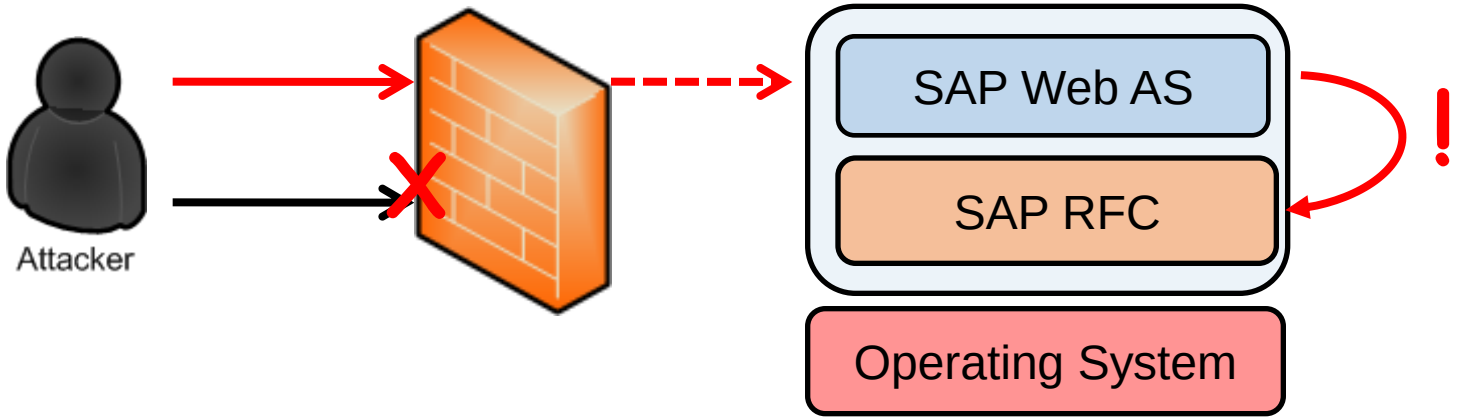
Attacks to the SOAP RFC Service



Attacks to the SOAP RFC Service



Attacks to the SOAP RFC Service



Live Demo: Business data exfiltration attacks through the Web

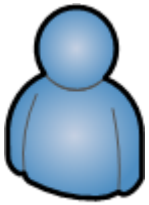
Authentication Bypass Attacks

- Many organizations currently have Web Access Management (WAM) solutions in place.

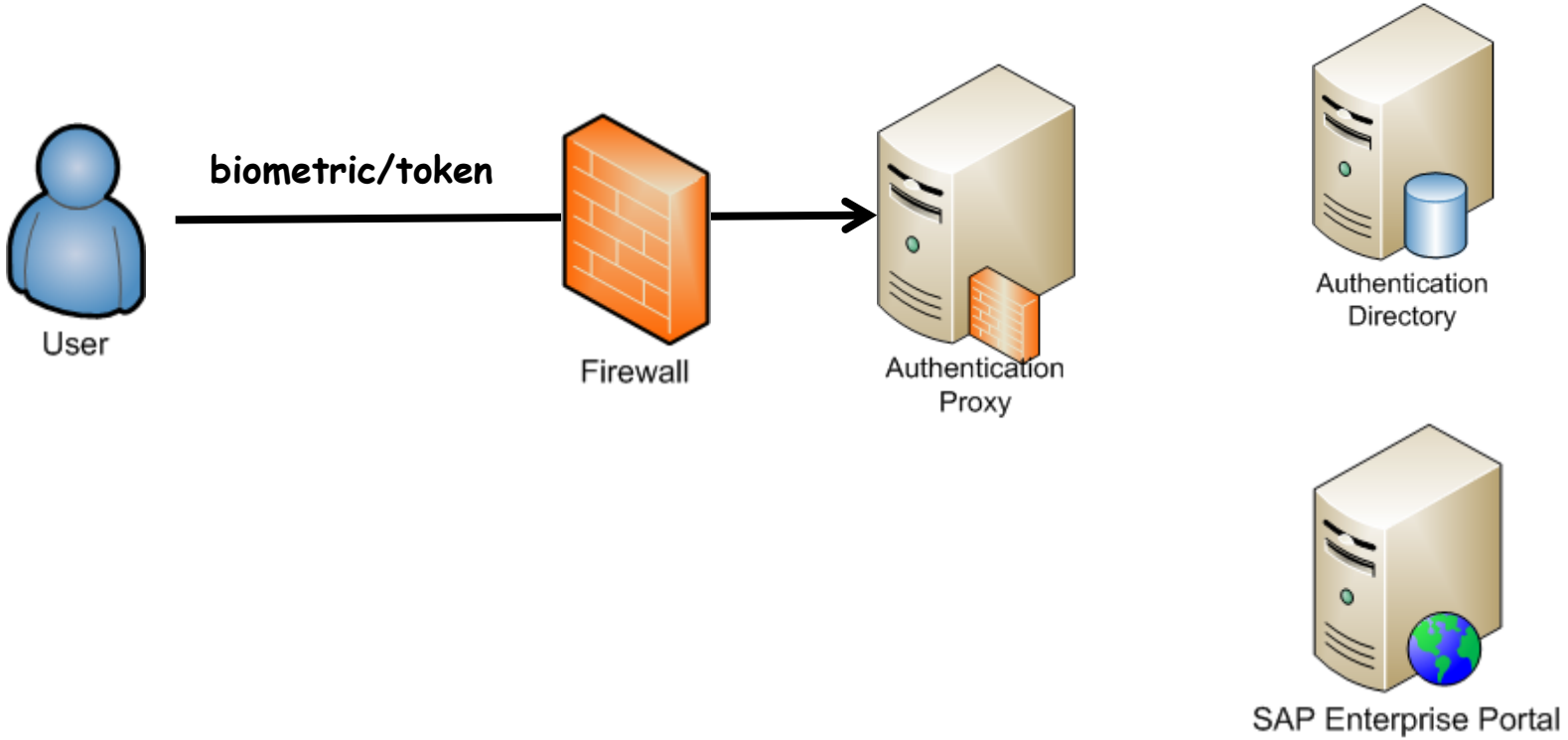
- They use them to enable secured access to the systems (tokens, biometrics, etc) and Single-Sign On.
  - RSA ClearTrust
  - CA SiteMinder
  - Oracle Oblix
  - Entrust GetAccess
  - Microsoft Integrated Windows Authentication

- The SAP J2EE Engine integrates with them using the *Header Variable Login Module…*

The Header Authentication Scheme

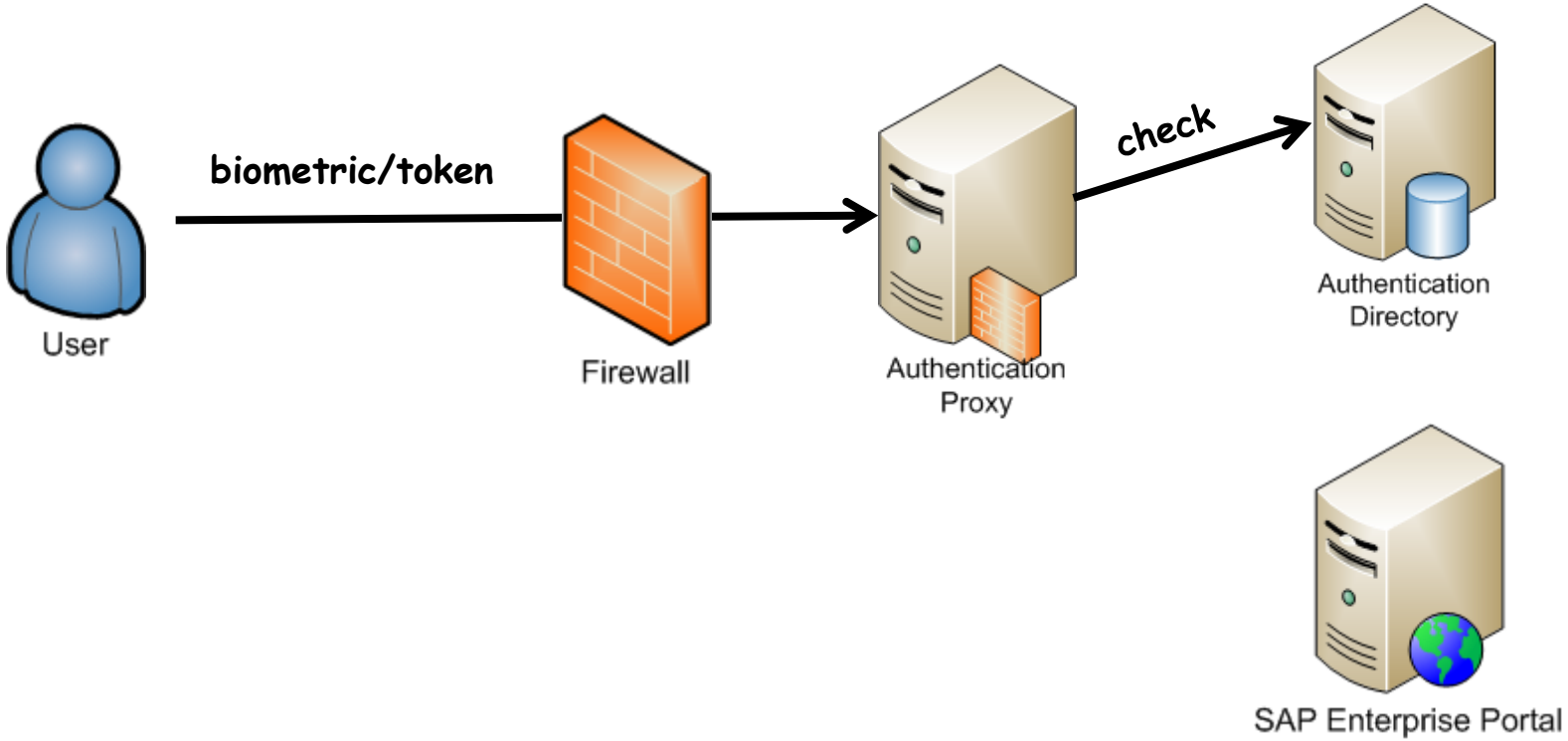


The Header Authentication Scheme



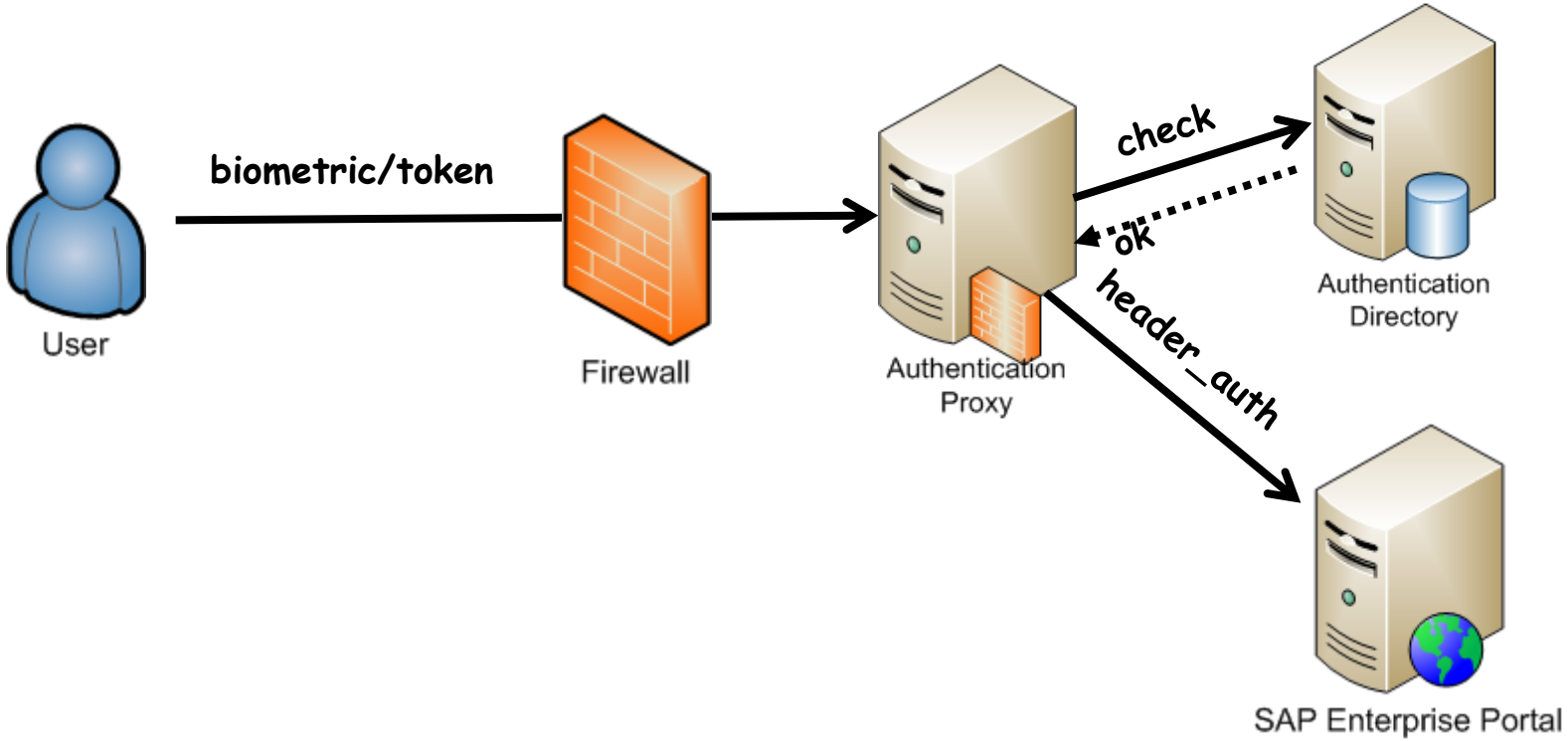
1. The user provides authentication information to the EAM/WAM solution.

The Header Authentication Scheme



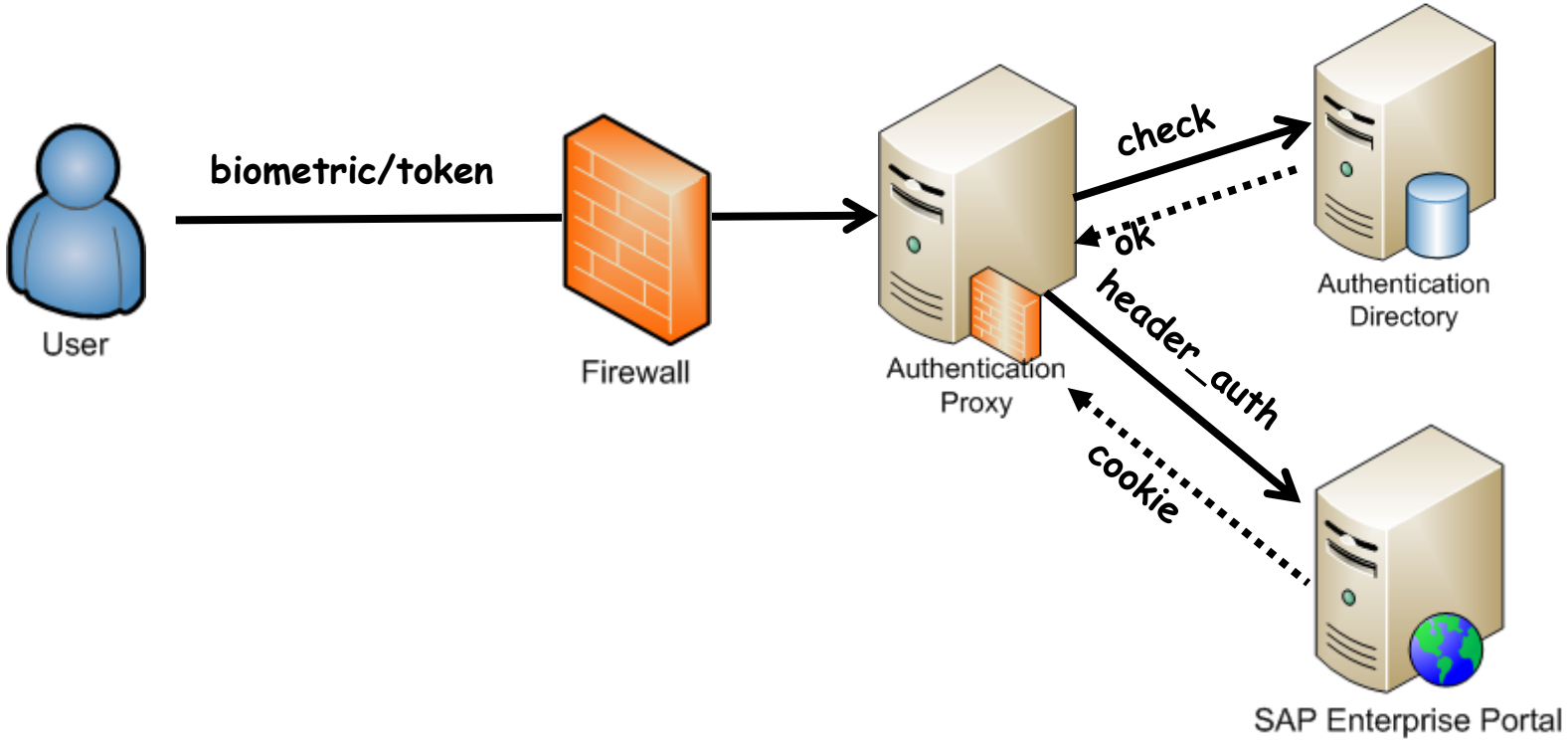
2. The solution checks provided credentials.

The Header Authentication Scheme



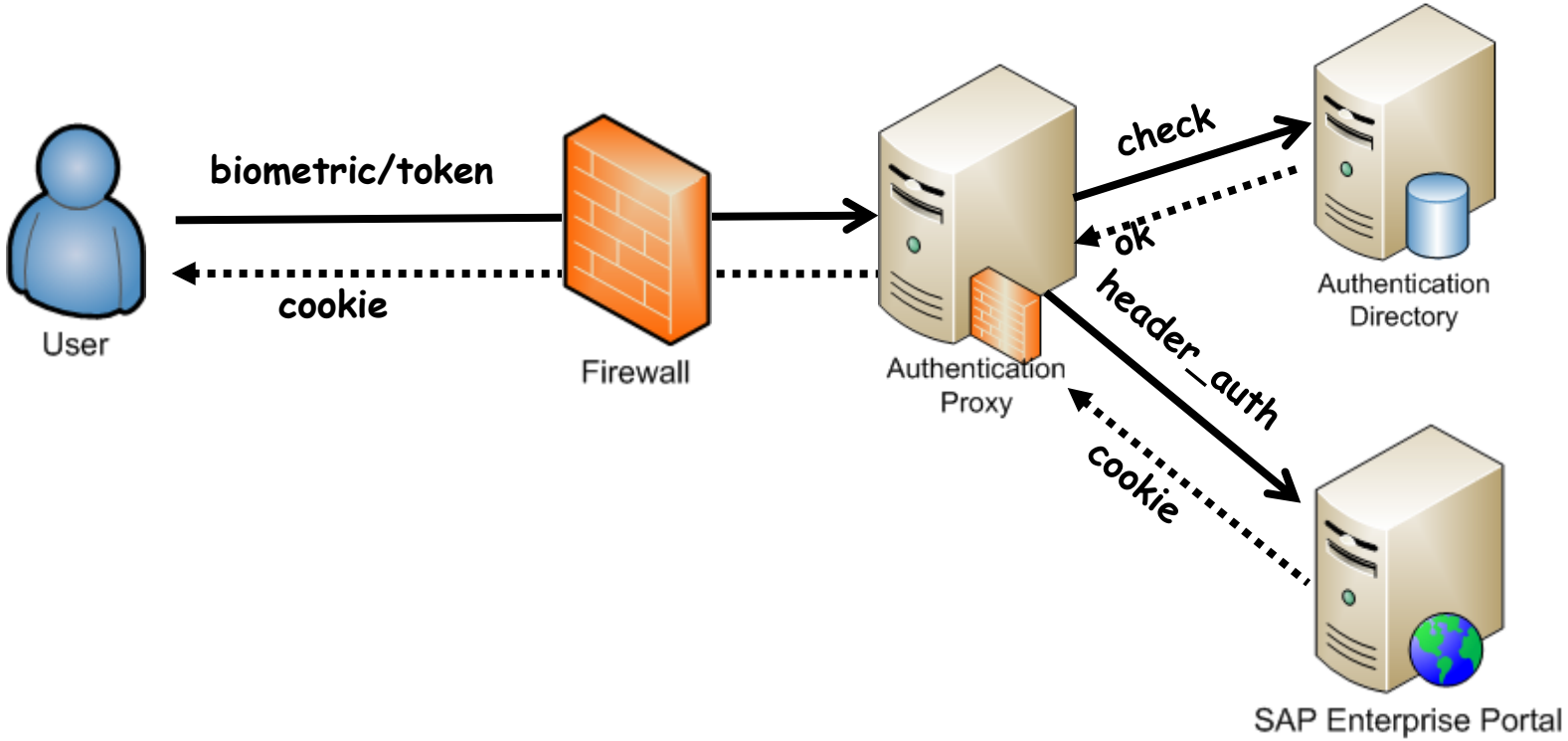
3. If successful, connects to the Enterprise Portal and sends the user to authenticate in a HTTP header.

The Header Authentication Scheme



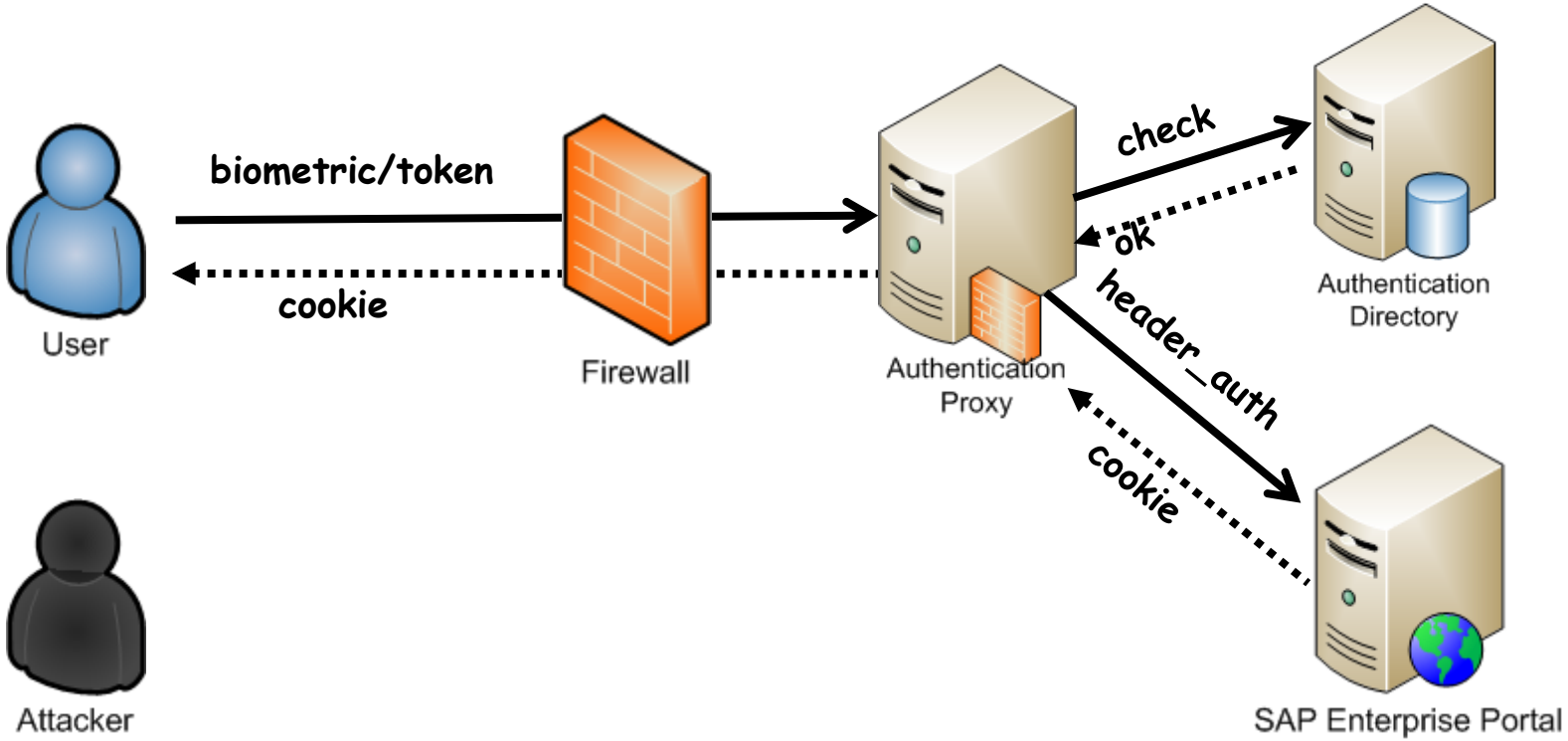
4. The Enterprise Portal verifies that the user is valid (it exists), and returns an SAP SSO logon ticket to the user.

The Header Authentication Scheme



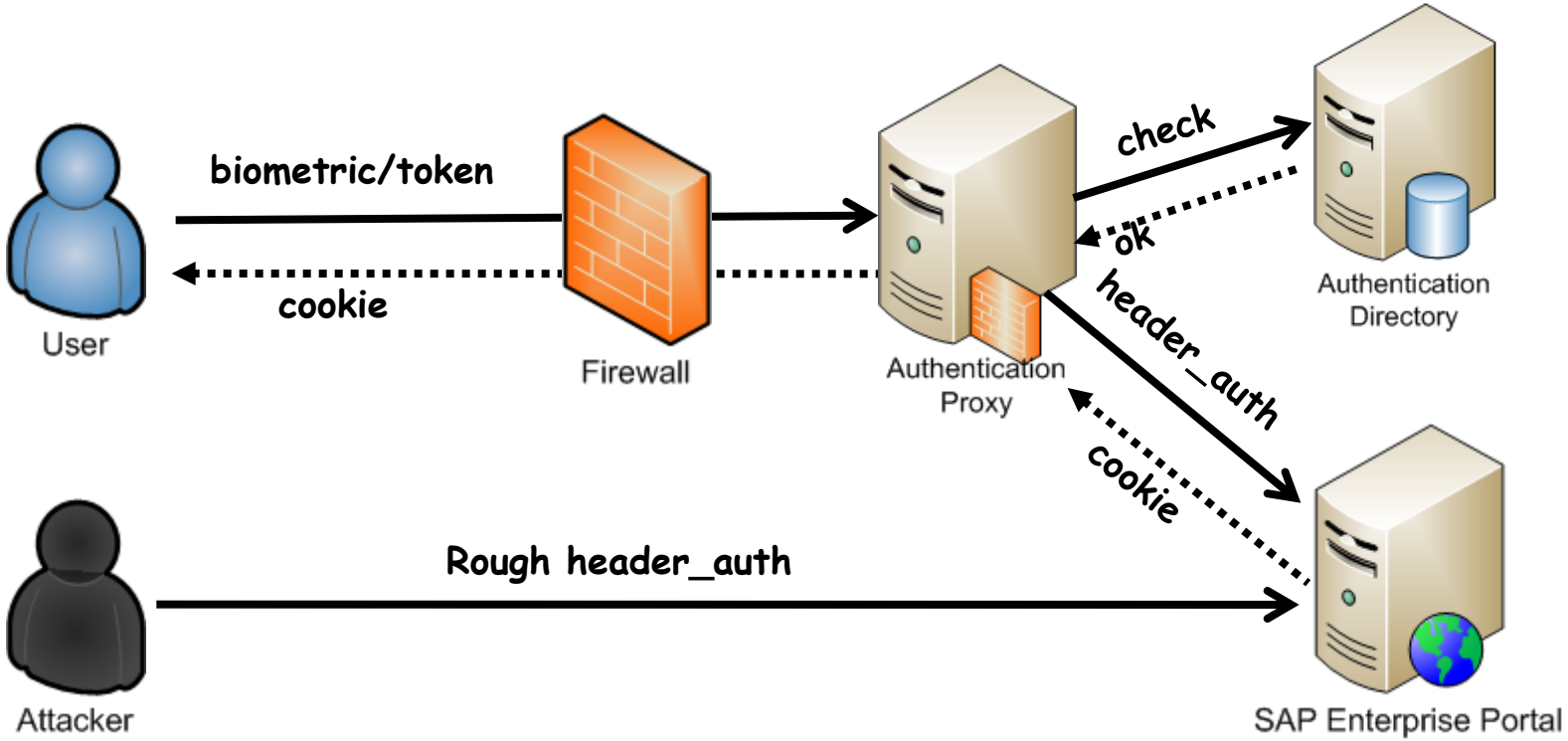
5. The user is authenticated.

The Attack



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

The Attack



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

Live Demo: Attacks to SAP Enterprise Portal Authentication

How to protect yourself from these attacks

- **Attacks to ICF Services:**
  - Disable any ICF service that is not enabled due to business requirements.
  - Check SAP Note 1498575 and [1].
  - Maintain ICF Authorization Data as described in [2] and [3].

- **Attacks to NetWeaver Portal authentication:**
  - Implement proper network filters to avoid direct connections to the SAP J2EE Engine.
  - If using it for Windows authentication, switch to the SPNegoLoginModule.
  - Check [4].

1. http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/f0d2445f-509d-2d10-6fa7-9d3608950fee
2. http://help.sap.com/saphelp_nw73ehp1/helpdata/en/39/e11482b2d23a428e583a59bef07515/frameset.htm
3. http://help.sap.com/saphelp_nw73ehp1/helpdata/en/9f/fc5e900b62d94e8878eb94db5b986f/frameset.htm
4. http://help.sap.com/saphelp_nw73ehp1/helpdata/en/d0/a3d940c2653126e10000000a1550b0/frameset.htm

Conclusions

- SAP systems are more and more connected to the Internet. Furthermore, few companies have internal DMZs for SAP servers.
- SAP Web Application Servers are highly complex and need to be fully understood to be able to secure them.
- By exploiting vulnerabilities in SAP Web components, an anonymous attacker can obtain complete control of the internal SAP servers and perform espionage, sabotage and fraud attacks.

Apply

- Find out which SAP Webapps you are using.
  - If not required, disable them.
  - If connected to the Internet, deploy WAF/IPS.
- Detect vulnerable Web services and configurations that could be exposing your business information and disable them.
- Evaluate ALL the systems (not just Production), at least after each SAP Security Patch Day.