VU University Amsterdam

# SAP Netweaver Application Server and Netweaver Portal Security

Author: Nick Kirtley

Supervisors: Abbas Shahim, Frank Hakkennes

Date: 28-09-2012

Organization: VU University Amsterdam, FEWEB

## Table of Contents


**1 Introduction ..... 4**

*1.1 Audience ..... 4*

*1.2 SAP and SAP AG ..... 4*

*1.3 SAP Components ..... 4*

*1.4 Information Security ..... 5*

1.4.1 SAP – An Information System ..... 5

1.4.2 Confidentiality, Integrity, Availability (CIA) ..... 5

1.4.3 An Example Business Process ..... 7

*1.5 Current SAP Security Approach ..... 7*

*1.6 Research Scope ..... 8*

*1.7 Research Goals ..... 9*

1.7.1 Problem Statement ..... 9

1.7.2 Research Questions ..... 10

*1.8 Proposed Solution ..... 10*

1.8.1 Testing Method ..... 11

*1.9 Approach ..... 11*

1.9.1 Initial Research ..... 11

1.9.2 SAP Security Workshop ..... 11

1.9.3 Literature Research ..... 11

1.9.4 Interviews ..... 11

1.9.5 Translating Knowledge Gained to Weaknesses, Desired State and Testing Methods ..... 12

*1.10 Limitations ..... 12*

*1.11 Overview ..... 12*

**2 Description of Netweaver Application Server and Netweaver Portal ..... 13**

*2.1 SAP Components ..... 13*

2.1.1 SAP ERP ..... 13

2.1.2 SAP Functional Modules ..... 13

2.1.3 SAP Netweaver Application Server ..... 13

2.1.3.1 Gateway ..... 14

2.1.3.2 Internet Communication Manager (ICM) ..... 14

2.1.3.3 Internet Connection Framework (ICF) ..... 15

2.1.3.4 Message Server ..... 15

2.1.4 Netweaver Portal ..... 15

2.1.5 SAP Web Dispatcher ..... 16

2.1.6 SAP GUI ..... 16

2.1.7 SAP Router ..... 16

*2.2 Security Patching ..... 16*

*2.3 Underlying Infrastructure ..... 17*

2.3.1 Operating System ..... 17

2.3.2 Database ..... 17
2.3.3 Network ..... 17
*2.4 Chapter Conclusion ..... 18*
**3 SAP Component Risks and Controls ..... 19**
*3.1 SAP Netweaver Application Server ..... 19*
3.1.1 Inadequate Authorization Definition for Netweaver AS Technical Administration ..... 19
3.1.2 Inadequate Authorization Definition for Java Applications ..... 21
3.1.3 Inadequate Authorization Definition for RFC Calls ..... 22
3.1.4 Inadequate SAP gateway configuration ..... 24
3.1.5 Lack of a central user authentication system ..... 24
3.1.6 Existence of default users with default passwords ..... 25
3.1.7 Operating System Access via the SAP Netweaver Application Server ..... 26
3.1.8 Lack of SAP Application Server Secure Configuration ..... 26
3.1.9 Unencrypted Communication ..... 27
3.1.10 Internet Services Available and Unrestricted ..... 29
3.1.11 Web Application Weaknesses ..... 30
3.1.12 Lack of Security Patching ..... 31
*3.2 SAP Netweaver Portal ..... 33*
3.2.1 Inadequate Authorization Definition for SAP Netweaver Portal ..... 33
3.2.2 Access to default pages ..... 34
3.2.3 Access to the SAP GUI via Netweaver Portal ..... 35
3.2.4 Availability of Anonymous Access ..... 36
3.2.5 Lack of Secure Network Architecture ..... 36
*3.3 Chapter Conclusion ..... 38*
**4 Conclusion and Future Work ..... 39**
*4.1 Conclusions ..... 39*
4.1.1 Overall Research Question ..... 39
4.1.2 First Research Question ..... 39
4.1.3 Second Research Question ..... 40
4.1.4 Third Research Question ..... 40
4.1.5 Fourth Research Question ..... 40
*4.2 Future Research ..... 41*
*4.3 Reflection on Research Performed ..... 41*
**Appendix A. Interview Questions ..... 44**
*Current Testing Methodology ..... 44*
*Impact on business in the event of an incident ..... 44*
*Incidents Related to SAP ..... 45*
**Appendix B. Interview Response ..... 46**
*Current Testing Methodology ..... 46*
*Impact on business in the event of an incident ..... 47*

*Incidents Related to SAP..... 47*

**Appendix C. Work Program..... 49**

**Abstract**

SAP is a major software vendor for ERP and business related software. SAP systems contain business critical information that is subject to security requirements. SAP security in the industry is mostly concerned with user authorization issues in the system. This thesis describes SAP security related to the commonly used Netweaver Application Server and Netweaver Portal components, such as hardening of services, secure configuration and user authorization issues specifically for those two components. This covers a broader range of security areas not usually covered by SAP security in industry, which commonly only deals with SAP ERP user authorization.

**Keywords:** SAP, infrastructure, hacking, hardening, secure configuration, Netweaver Application Server, Netweaver Portal.

# 1 Introduction

This chapter introduces the key concepts of the research problem to help understand the domain of the research problem. The domain of this research project is the security of the SAP Netweaver Application Server and Netweaver Portal components, which is an area of SAP security which receives less attention than SAP security domains such as user management.

The following sub-chapters will provide a brief introduction of SAP and how it's used, SAP security and security testing. The last part of the chapter will provide an overview of the remainder of the thesis document.

## 1.1 Audience

The intended audience of this thesis consists of technical IT auditors. A technical background is required because the reader should have a general understanding of business risks, technical risks, controls, control objectives and technical systems such as SAP and underlying infrastructure.

## 1.2 SAP and SAP AG

SAP, which is an acronym for Systems, Applications and Products in Data Processing, is an Enterprise Resource Planning (ERP) solution that helps businesses manage their (core) business processes. SAP is able to serve a broad range of business process including many financial areas, Customer Relationship Management (CRM), material management, project management, Supplier Relationship Management (SRM) and more. This allows a company that uses SAP to build an integrated solution for most conceivable business processes within a company. SAP has many industry specific solutions such as banking, telecommunications, healthcare, education and many more. This allows nearly all companies to use SAP, irrespective of their branch, while still benefiting from industry specific requirements. The broad support offered by SAP shows in SAP AG's customer portfolio. SAP AG is the parent company that owns and develops SAP software. SAP AG had roughly 109,000 customers in 2010 in over 120 countries, consisting of 75% small and midsize companies [1]. Revenue in 2010 consisted of roughly 5.5 billion Euros.

## 1.3 SAP Components

SAP in a technical sense consists of many products to provide the necessary services and functionality of a modern ERP solution that serve so many customers. The main components of SAP (and those most used) will be explained to provide the necessary background information for later sections in the thesis document. Further explanation of important SAP components and technology is given in chapter 2.

SAP ERP, which is also known as SAP Enterprise Central Component (ECC) and formerly known as R/3 (here after: SAP ERP), is the main system of SAP. It is the link responsible for direct communication with the database (server) that stores information. All information about the state of the application (and all business information) is stored within a single database. All other SAP components function upon the foundation of the central component (SAP ERP).

SAP Netweaver is a suite of tools that allow for integration of a wide range of services within the SAP environment. SAP Application Server (AS) is part of the Netweaver suite of tools. It acts as a web

server that offers services such as the SAP Graphical User Interface (GUI) and web services. These servers/services connect with other SAP Netweaver AS instances, with SAP ERP (backend), with clients. SAP Netweaver AS can be seen as an access channel to the SAP system. SAP Netweaver Portal is also part of the Netweaver suite of tools. It acts as a portal system for users to access SAP backend systems (most commonly SAP ERP) and other (third party) applications.

## 1.4 Information Security

This chapter will discuss a number of information security concepts that are relevant for SAP security and the subject of the thesis.

### 1.4.1 SAP – An Information System

When discussing security it is important to understand what should be secured. In the case of SAP security, the information contained within the SAP system should be secure because SAP is essentially an information system.

NIST describes an information system as the following [15]:

*A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.*

### 1.4.2 Confidentiality, Integrity, Availability (CIA)

When discussing information security it is important to understand key concepts. One such concept is CIA: Confidentiality, Integrity and Availability. The CIA concept consists of qualities or attributes of security, each with their own purpose.

**Confidentiality**

Confidentiality refers to keeping information confidential within a system. This means that confidential information should only be accessible to authorized individuals. Information systems usually have an authorization model to determine who should be able to access what information. SAP has multiple authorization models that can be used to ensure that only individuals can access information for which they are authorized.

The ISO 27000 standard definition for confidentiality [14]:

*Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.*

An example of confidentiality is an SAP system used by a multinational company whereby employees from an operating country can only be access their own data (from the same country) and not data from other countries where the multinational company operates.

An example of a loss of confidentiality in an SAP system is a low privileged employee that can access key company financial data that should only be accessible to senior management within the company.

**Integrity**

Integrity refers to information within a system set at an appropriate and intended value. This is achieved when data has not been modified without detection or proper authorization. Integrity can have further classification by timeliness, correctness and fullness (translated from Dutch words ‘tijdigheid’, ‘juistheid’ and ‘correctheid’) [13].

The ISO 27000 standard definition for integrity [14]:

*Property of protecting the accuracy and completeness of assets.*

An example of integrity in an SAP system is the values of financial information is the same as when the information was entered or modified with proper and authorized intention and with malicious intent.

An example of a loss of integrity in an SAP system is an unauthorized update of financial data due issues in the authorization mechanism.

**Availability**

Availability refers to information in a system being available when required. Availability can be affected by a range of technical factors.

The ISO 27000 standard definition for availability [14]:

*Property of being accessible and usable upon demand by an authorized entity.*

An example of availability in an SAP system is accessing the financial information when required for a certain time period.

An example of a loss of availability in an SAP system is the system not responding to a request for information due to a malicious attacker having changed critical configuration settings so that the system cannot function properly when required.

### 1.4.3 An Example Business Process

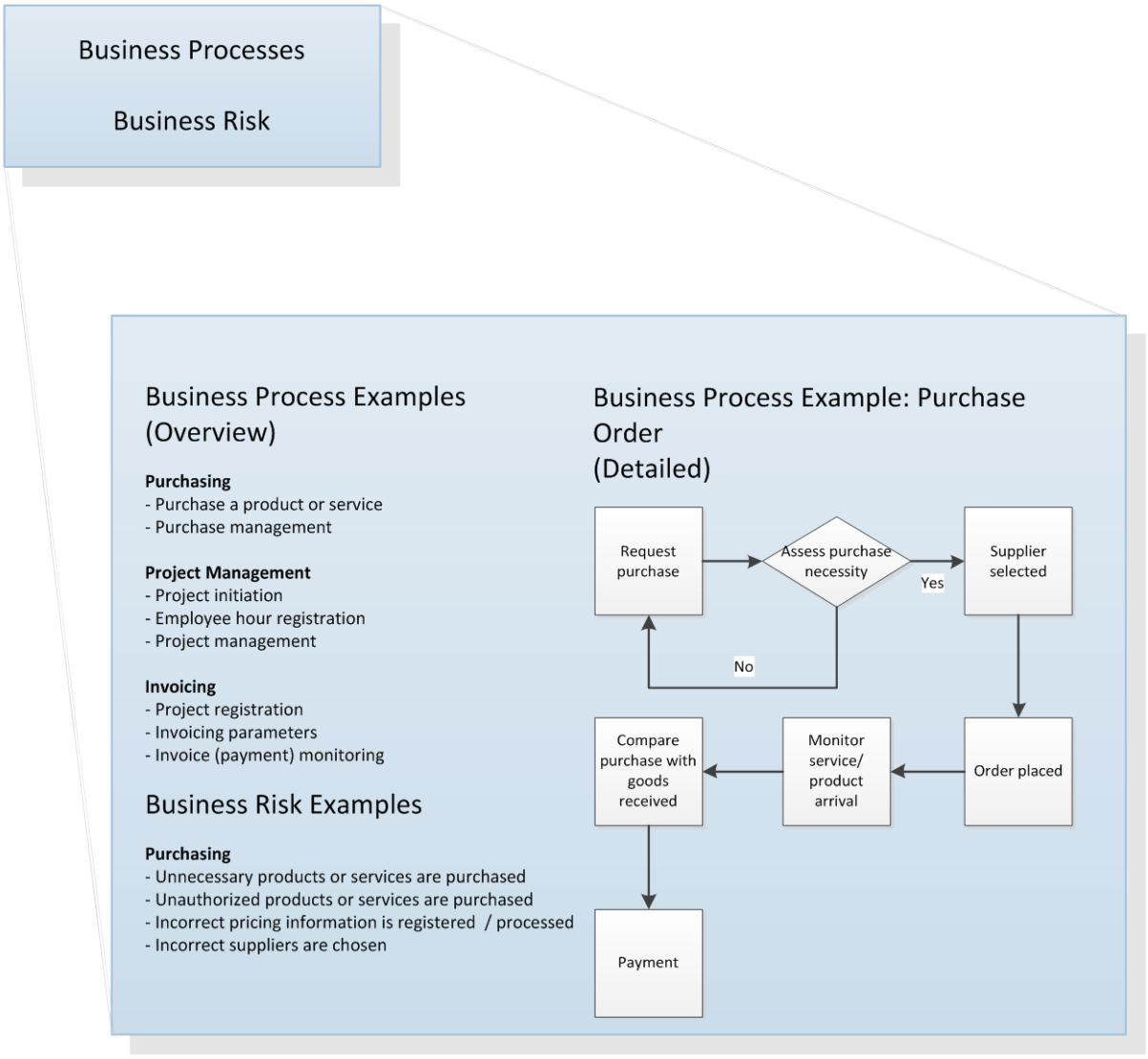


Figure 1: Business processes and business risks

Figure 1 shows a list of business process examples that are common in many businesses and a list of business risk examples specific to purchasing that should be secured with information security. Furthermore, a detailed process flow of a purchase order is also shown as an example.

The purpose of Figure 1 is to show an example overview of business processes and business risks. This is important because any weaknesses and associated risks identified in an SAP system should always relate to business risk because that is the final objective of SAP systems (to serve business). Information Security should mitigate those business risks.

## 1.5 Current SAP Security Approach

SAP security consists of securing the information stored within an SAP environment. This can be expressed in terms of CIA. Therefore, a secure SAP environment is one that can keep information confidential, maintain the integrity of information and to keep information available when required.

The common SAP security landscape currently focuses on authorization issues:

- Authorization issues, in the context of this research, consist of ensuring that only authorized individuals can access the SAP environment, and ensuring that the list of authorized individuals is authorized. Issues such as the least privilege principle, Segregation of Duties (SoD) and the four eyes principle are considered. Alignment with business and business processes are important considerations when assessing authorization issues.

The problem with this approach is that security of an information system should consist of more than merely authorization issues.

Security is about more than merely technology. Security management processes should be applied to provide sufficient security for an information system such as an SAP environment. Security management refers to the processes involved in providing a secure system that is used securely. Security management often works by the concept of people, processes and technology to provide a holistic security management offering. This research concentrates on the technology aspect, and in particular will only focus on the important infrastructure components Netweaver Application Server and Netweaver Portal (refer to 1.6 – Thesis Scope).

The SAP infrastructure implementation, consisting of Netweaver Application Server and Netweaver Portal should be included because weaknesses can be present in the system itself, which is not covered by a fully functioning authorization system. A simple example to illustrate the point:

Like any software system, SAP contains bugs and common security weaknesses. These are reported on a regular basis and can be accessed publically. These bugs and common weaknesses are fixed by SAP in updates and patches, secure configuration and implementation of important security concepts. If these updates and patches, secure configuration and implementation of important security concepts are not applied, an SAP system is vulnerable to known security weaknesses even though the authorization model is fully functional and effectively secured. This situation can lead to a loss of confidentiality, integrity and availability, depending on the types of common weaknesses in the SAP system of which Netweaver Application Server and Netweaver Portal are a part of.

## 1.6 Research Scope

This thesis will focus on the security of SAP Netweaver Application Server and Netweaver Portal.

The scope is defined as:

- Technical configuration of SAP Netweaver Application Server and its subcomponents
- Technical configuration of SAP Netweaver Portal

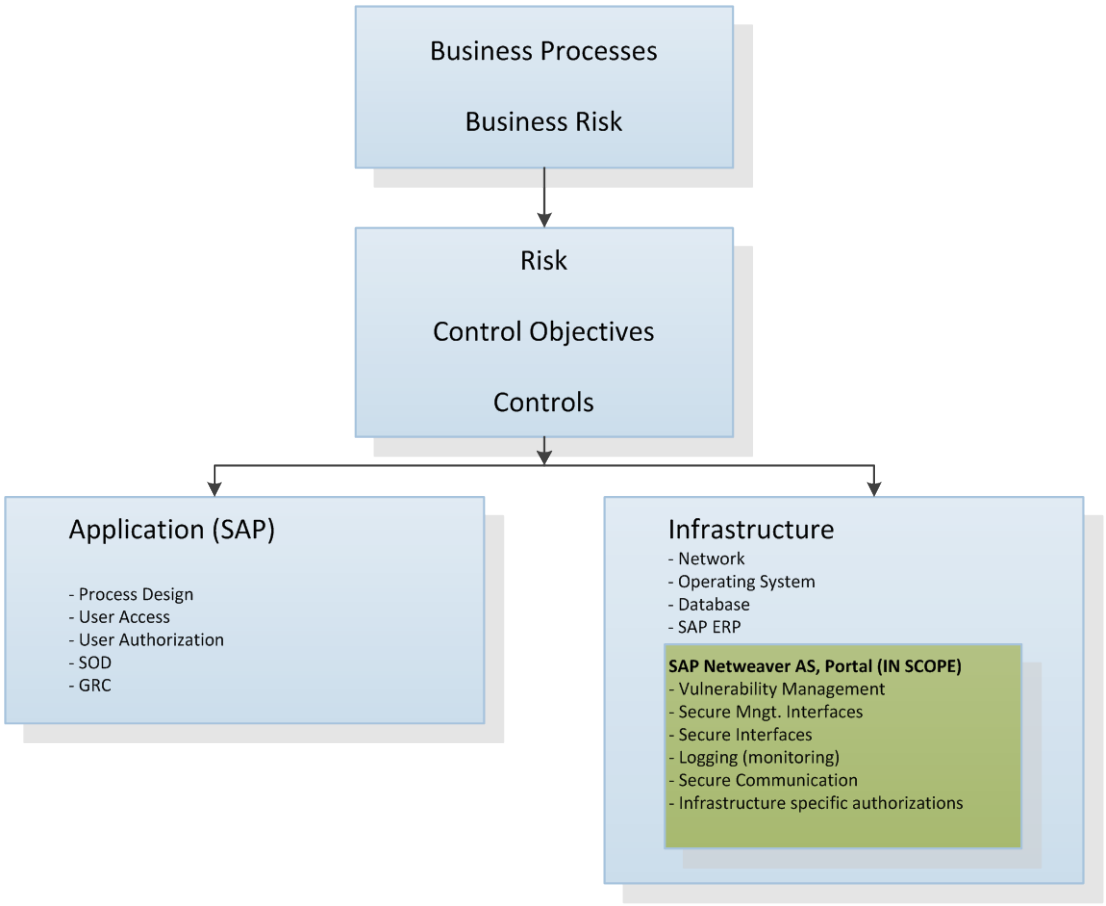


Figure 2: SAP Risk and Control Framework

Figure 2 shows an overview of the SAP risk and how a high level control framework could be conceived. The top object shows business processes and business risk. The middle object shows risks specific to the SAP (information) system, the control objectives and controls to mitigate the risks identified. The green area shows the scope of the thesis, which includes SAP specific components.

## 1.7 Research Goals

Currently SAP security mostly consists of evaluating authorization issues whereas weaknesses in Netweaver Application Server and Netweaver Portal are largely ignored. Therefore, SAP systems used by companies may contain security weaknesses that could negatively affect the confidentiality, integrity or availability of information stored on SAP systems.

The goal of this thesis is to research common weaknesses in Netweaver Application Server and Netweaver Portal. The security weaknesses should be understood, along with a control objective and a control testing method.

### 1.7.1 Problem Statement

The problem statement can be concisely described as follows:

*Industry currently does not seem to sufficiently understand the technical issues and risks involved in deploying an SAP implementation that serves business and contains critical business information. Therefore, management (within industry) would not seem able to take well informed actions to mitigate possible risks involved.*

### 1.7.2 Research Questions

The overall research question related to this thesis:

- *Which testing methods must an IT auditor use to assess weaknesses in critical SAP components Netweaver Application Server and Netweaver Portal?*

SAP systems provide the business with standard information system modules to manage common business processes. Security is an essential part of using SAP systems within a company to ensure that business information is secure. Netweaver Application Server and Netweaver Portal are essential in providing overall security.

1. *Describe Netweaver Application Server, Netweaver Portal and related components relevant to weaknesses described in the thesis.*

Weaknesses in SAP Netweaver Application Server and Netweaver Portal components are still prevalent in industry.

2. *Describe the weaknesses regarding the use of SAP Netweaver Application Server and Netweaver Portal.*

Security measures exist for weaknesses in SAP Netweaver Application Server and Netweaver Portal components.

3. *Describe the desired state that should be achieved related to weaknesses.*

The method of testing for weaknesses in Netweaver Application Server and Netweaver Portal are required to determine whether specific implementations are vulnerable.

4. *Develop a detailed approach to test weaknesses in Netweaver Application Server and Netweaver Portal.*

## 1.8 Proposed Solution

The proposed solution consists of developing a detailed understanding of SAP infrastructure security and translating that understanding into a risk, control and testing framework of SAP security, with a focus on infrastructure security.

The proposed solution will take the following into account:

- General security best practice
- Concrete testing steps and mitigating measures
- Weaknesses known by security experts

### 1.8.1 Testing Method

The testing methods described in this thesis will contain general descriptions describing how testing can be performed. A work program in the appendix describes testing in structured manner. Some weaknesses can have specific testing methods whereas others may require more broad descriptions due to the type of weakness and the fact that testing may vary depending on the specific situation. For example, the 'web application weaknesses' weakness described in chapter 3.1.11 is broad in nature and could have entire work programs devoted to the subject. Therefore, in this case a high level description and approach is given.

## 1.9 Approach

The research approach for this thesis consists of multiple phases. This has allowed for an extensive understanding of the subject matter with multiple perspectives.

### 1.9.1 Initial Research

The initial research consisted of awareness regarding SAP security and in particular Netweaver Application Server and Netweaver Portal. This mainly consisted of online research and discussions with SAP specialists. This initial research shows that there are security considerations that are currently not taken into account by industry and that this subject is of interest for further research.

### 1.9.2 SAP Security Workshop

The next step consisted of a one day SAP security workshop at the Troopers 12 security conference. A number of top SAP security specialists spoke about SAP security concepts that are not covered in normal SAP audits performed by industry.

The following subjects were discussed:

- SAP security trends
- Attack vectors that hackers may exploit in SAP
- Common technical misconfigurations and vulnerabilities
- ABAP code review results (common issues)
- Live demonstrations

This shows that the subject of SAP security is slowly evolving and of interest to industry.

### 1.9.3 Literature Research

The bulk of research consisted of literature research including reputable online resources such as the SAP support website. Two very important resources consisted of the 'SAP Security and Risk Management' book [2]. This book covers the Netweaver Application Server and Netweaver Portal components extensively. Furthermore, the security article 'Perfect Storm - The Brave New World of SAP Security [22]' provides subject matter that is up to date and relevant for this thesis. The literature research provides an extensive understanding of weaknesses that affect Netweaver Application Server and Netweaver Portal.

### 1.9.4 Interviews

Interviews were held with a number of SAP security industry professionals to provide information about the current SAP security state. The interview questions can be seen in Appendix A. The answers to the questions have been paraphrased in Appendix B. The interview questions have three main areas of interest:

- Current (SAP) testing methodology
- Impact on business in the event of an incident
- Incidents related to SAP

### 1.9.5 Translating Knowledge Gained to Weaknesses, Desired State and Testing Methods

This step consisted of converting the knowledge gained in previous steps to a coherent message regarding weaknesses, the desired states of weaknesses and testing methods of weaknesses that affect Netweaver Application Server and Netweaver Portal. Furthermore, knowledge gained from auditing and security experience was used to

## 1.10 Limitations

This thesis and the research performed are limited in the following manner:

- The weaknesses and control testing methods have not been tested in a practical environment or in a business setting.
- The weaknesses will not describe the resulting risk because this is dependent on business objectives and many other business parameters (i.e. specific to how business uses SAP and the information stored within it).
- Netweaver Application Server version 7 and Netweaver Portal 7. Therefore, older versions have not been verified (although they may have the same or similar weaknesses).

## 1.11 Overview

The rest of the document is used to describe the steps taken to investigate the problem statement and to answer the research questions.

Chapter 2 describes the SAP security landscape.

Chapter 3 describes security weaknesses, control objectives and controls.

Chapter 4 describes the conclusion and future work to further the research outlined in this thesis.

Appendix A and B include interview questions and answers.

Appendix C includes the work program.

# 2 Description of Netweaver Application Server and Netweaver Portal

The components in scope of this research will be described in this chapter including important sub-components that impact security. Related components are also described to help understand the technical working of Netweaver Application Server and Netweaver Portal.

## 2.1 SAP Components

The SAP components in scope, consisting of Netweaver Application Server (AS) and Netweaver Portal, and components closely associated with those components are discussed in this chapter. Netweaver AS and Netweaver Portal are often used in conjunction with SAP ERP, therefore, a short description of SAP ERP will also be provided.

### 2.1.1 SAP ERP

SAP ERP is the application environment for Enterprise Resource Planning (ERP). SAP ERP contains traditional ERP functionality, as described by [2]:

- Reporting
- Financial accounting and corporate governance
- Procurement and logistics execution
- Product development and manufacturing
- Sales and services
- Corporate services

SAP ERP contains much of the business critical information that requires protection in terms of CIA.

### 2.1.2 SAP Functional Modules

SAP has many functional systems, apart from SAP ERP, that can be used for increased functionality for common business processes. The definition of functional systems in this thesis includes:

- CRM
- SCM
- SRM
- PLM
- Business Objects
- Specific industry solutions

Each functional module contains business critical information just like SAP.

### 2.1.3 SAP Netweaver Application Server

The SAP Netweaver Application Server (AS) is the central component of the Netweaver product range. The Netweaver product range is essentially the range of products that provides various connectivity options to the SAP environment and crucially, the backend data. The main aim of the Netweaver Application Server is to offer robust and maintainable connectivity [2] [3]. The Netweaver AS contains various components and interfaces that offer connectivity (for example, via the SAP GUI,

or via an HTTP/HTTPS web interface). The various components will be described in later (sub) chapters. Netweaver AS has two main variants: an ABAP and a Java variant. The ABAP variant runs ABAP applications and the Java variant runs Java applications. The technology stack used in the variants differs, yet they offer the same (business) functionality.

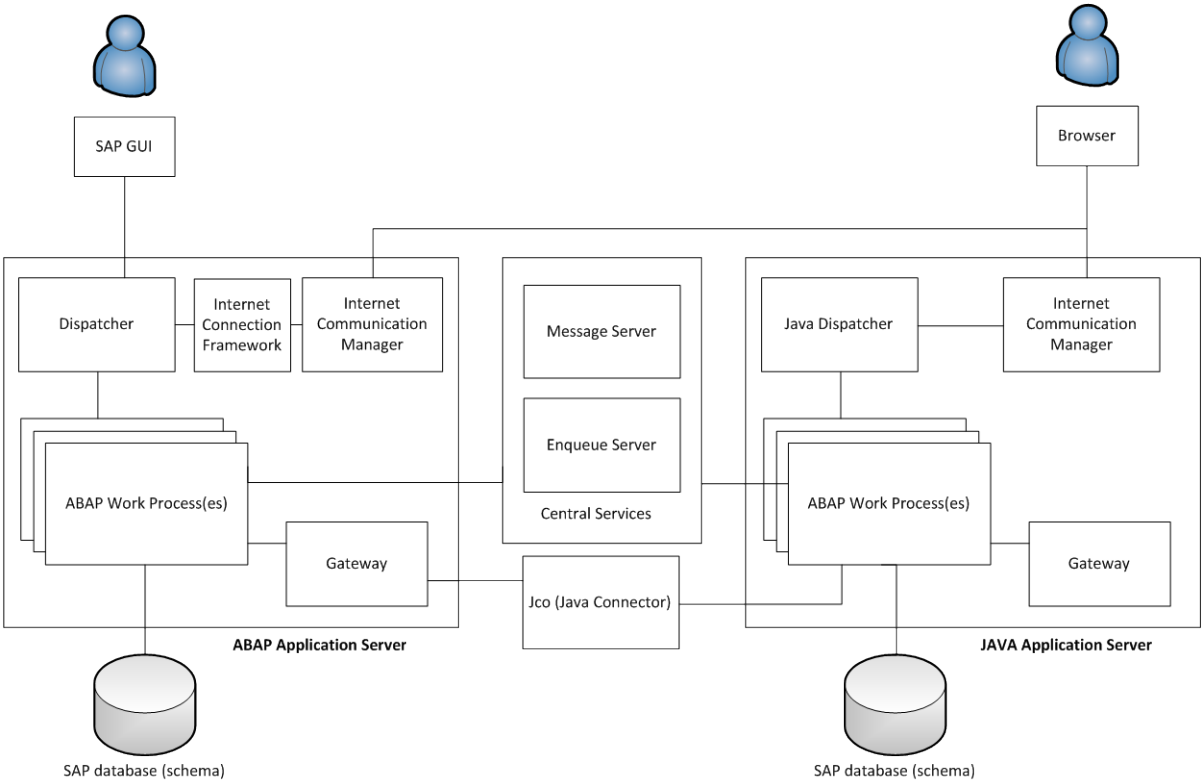


Figure 3: SAP Netweaver AS architecture [4]

Figure 3 shows a technical diagram of the Netweaver AS architecture split into the ABAP solution on the left and the Java solution on the right (Netweaver AS can consist of an ABAP solution, Java solution or both). Specifically, the components that make up the Netweaver AS are of interest because they show how the system works and the various external entry points. Many of the Netweaver AS components will be described in the following sub-chapters.

### 2.1.3.1 Gateway

The Netweaver AS Gateway is a communication interface between Netweaver Application Servers and between Netweaver AS and external applications. Each Netweaver AS has a gateway. The gateway is externally accessible and communicates via CPI-C (most commonly RFC) services. RFC consists of remote commands that can be performed by Netweaver AS on other Netweaver Application Servers, and by external applications on a Netweaver AS. The RFC services require associated authorizations, reference chapter 3.4.1.3 for more information.

### 2.1.3.2 Internet Communication Manager (ICM)

The Netweaver AS Internet Communication Module (ICM) is a communication interface for web requests that communicate via HTTP, HTTPS and SMTP. The ICM is externally accessible and is a layer above Netweaver AS ABAP and Java. The ICM receives requests and sends the request to a

relevant internal Netweaver AS handler. The ICM can differentiate requests that should be sent to the Netweaver ABAP AS and the Netweaver Java AS depending on the request requirements. The Netweaver Web Dispatcher monitors the performance of the ICM, reference chapter 3.1.3.5 for information about the Netweaver Web Dispatcher.

#### *2.1.3.3 Internet Connection Framework (ICF)*

The Netweaver Internet Connection Framework (ICF) is a communication interface for web requests to Netweaver AS ABAP [12], the ICM is the first layer which is called, which then sends requests to the ICF.

#### *2.1.3.4 Message Server*

The SAP Message Server is a messaging component that informs Netweaver Application Servers in the overall SAP system of their presence and status. The SAP Message Server can be called by clients to determine where to send subsequent requests (e.g. to determine where to login or to determine where to send RFC requests). Netweaver Application Servers, also known as instances, contact the SAP Message Server to announce available services.

### 2.1.4 Netweaver Portal

The Netweaver Portal component consists of providing a web based portal (user) interface that combines SAP and non-SAP systems. In technical terms Netweaver Portal is an application in itself that provides access methods that are user friendly for an end user. The Netweaver Portal is mostly accessible via a company internal network and in some cases even directly accessible from the Internet [2]. Figure 4 shows various components and connections related to Netweaver Portal.

The three main tasks of Netweaver Portal:

1. A single web application entry point that connects to other SAP components using modern web application interfaces.
2. Collaboration functionality including instant messaging, Email, forums, etc.
3. Connectivity for various types of devices such as normal web browsers (e.g. using Internet explorer or Mozilla Firefox) or mobile devices (e.g. Mobile Safari).

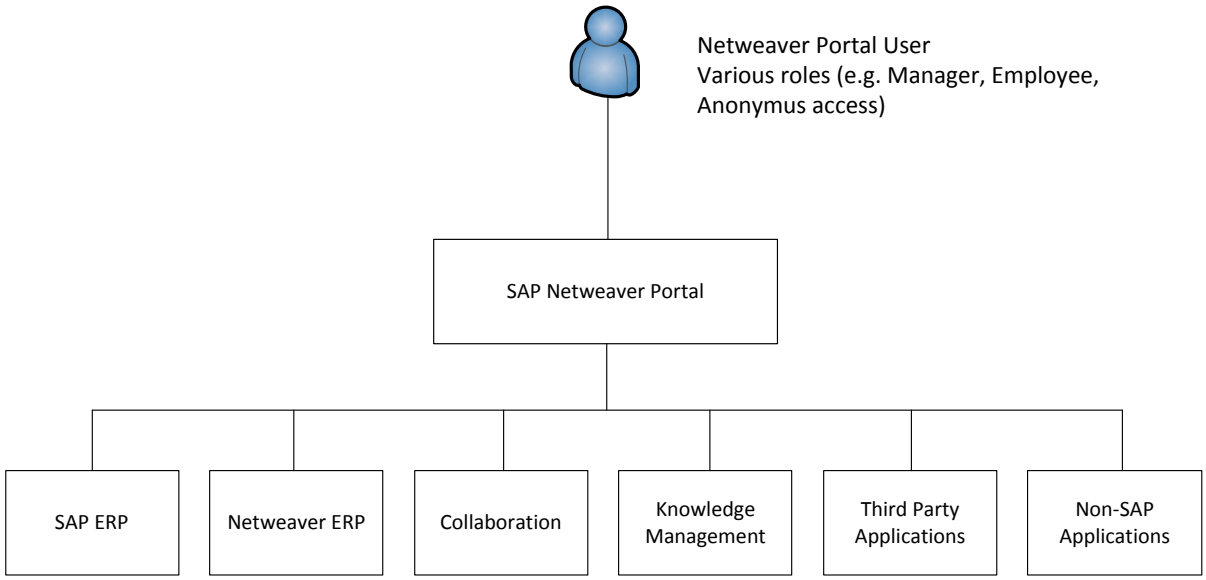


Figure 4: Netweaver Portal

### 2.1.5 SAP Web Dispatcher

The SAP Web Dispatcher is used in scenarios where the SAP system is exposed to the Internet [13]. It lies between the Internet and the SAP system, with an SAP system consisting of multiple Netweaver Application Servers. It is also referred to as a software switch because it can be used for load balancing. The SAP Web Dispatcher can handle ABAP and Java requests.

### 2.1.6 SAP GUI

SAP GUI provides a standard graphical interface for users as a native application running on common Operating Systems. For example, SAP GUI is available as a Windows application. It offers access to traditional SAP ABAP based applications.

### 2.1.7 SAP Router

SAP router is a software component that is used to segment internal and external networks. It works in conjunction with a firewall to ensure that only relevant SAP communication is allowed between network segments. SAP router is also required for remote support from SAP in Waldorf, Germany.

## 2.2 Security Patching

Security patching is an important aspect of any software application. Software contains security vulnerabilities due to architectural security design shortcomings or security shortcomings at the software code level (e.g. Errors made by software developers). Security shortcomings are detected by independent security researchers, or by the software vendor. Many security shortcomings may never even be discovered during the lifetime of a software product.

SAP software is also subject to security vulnerabilities and security patching. Table 1 shows the number of security patches that have been issued in the last decade. The large increase from 2007 to 2010 is attributed to the fact that SAP has taken security more seriously in recent years, and not because its software less secure in recent years.

| Year | Rough number of SAP security patches |
|---|---|
| 2011 | 700 |
| 2010 | 800 |

| | |
|---|---|
| 2009 | 300 |
| 2008 | 50 |
| 2002-2007 | 10 per year |

Table 1: Security Patches in the previous five years [11]

## 2.3 Underlying Infrastructure

SAP requires an underlying infrastructure to function just like any other information system. The systems involved include (but not limited to in cases where specialized installations are performed):

- (mandatory) Operating System(s)
- (mandatory) Database(s)
- (mandatory) Network
- (optional) User provisioning system (e.g. Active Directory)

Each system can contain weaknesses that could compromise the confidentiality, integrity or availability of information stored on the SAP system. The underlying infrastructure is not in scope of this thesis. However, references to underlying infrastructure security descriptions are given.

### 2.3.1 Operating System

An Operating System is required to host the SAP software as is the case with most software. The Operating System provides a wide range of services such as storage, connectivity, user interface and processing. Windows and Linux operating systems fully support SAP software, as in theory any operating system could. Hardening of the Operating System is required because it is part of the access path to business data stored within SAP systems.

The National Institute of Standards and Technology (NIST) Security Configuration Checklists Program provides hardening guidelines for many types of software [5]. Microsoft Windows based servers; such as Windows Server 2008 [6] and Linux based servers; such as Red Hat Enterprise Linux [7] NIST hardening guidelines are available.

### 2.3.2 Database

A database is required to store, manipulate, retrieve and delete data (that is required by SAP). All data used by SAP (and thus business information) is stored within the database.

SAP supports a wide range of databases including Oracle database, MS SQL and Max DB. This shows that SAP is database independent (as is the case with the Operating System). The database forms the backbone of data management. As described in the introduction, the data is the object of security and makes the database extremely important.

NIST hardening guidelines are available for Oracle databases; such as Oracle 10.2g [8] and Microsoft MS SQL databases; such as MS SQL 2005 [9].

### 2.3.3 Network

SAP is a distributed system which means that various components and users are distributed along technical (and even geographical) lines. This distribution is connected using a network and even multiple networks (in the case of communication via the Internet). This line of communication can present interception opportunities that could lead to issues regarding confidentiality, integrity and availability of data.

NIST hardening guidelines are available for networking devices; such as Cisco routers [10]. Network security is also subject to network architecture design decisions as well as individual network devices.

## 2.4 Chapter Conclusion

A description of Netweaver Application Server and Netweaver Portal has been given in this chapter. This includes the sub-components which are of particular importance to Netweaver Application Server due to the number of communication possibilities which can affect overall security. The descriptions of SAP components is required to fully understand the weakness described in the following chapters.

# 3 SAP Component Risks and Controls

This chapter will describe the Netweaver Application Server and Netweaver Portal weaknesses that have been identified as a result of research performed consisting of an SAP security workshop, literature research and interviews with SAP security industry professionals.

The weaknesses contain the following:

- Weakness description: a description of the weakness to understand the problem (research question 2).
- Control objective: a description of the desired state (i.e. how should the weakness be solved or mitigated) (research question 3).
- Control testing: a description of how to test whether a weakness is present in an SAP (Netweaver Application Server or Netweaver Portal) implementation (research question 4).

## 3.1 SAP Netweaver Application Server

Netweaver Application Server weaknesses, control objectives and control testing will described in this paragraph as outlined in chapter 3.

An overview of weaknesses for the Netweaver Application Server is given in Table 2. The first column shows the weakness identifier. The second column provides a descriptive title of the weakness and the third column shows the reference where the weakness is described in literature.

| Weakness ID | Weakness Description | Reference |
|---|---|---|
| 1.1 | Inadequate Authorization Definition for Netweaver AS Technical Administration | [2] |
| 1.2 | Inadequate Authorization Definition for Java Applications | [2] |
| 1.3 | Inadequate Authorization Definition for RFC Calls | [2] [22] |
| 1.4 | Inadequate SAP gateway configuration | [2] [22] |
| 1.5 | Lack of a central user authentication system | [2] |
| 1.6 | Existence of default users with default passwords | [2][22] |
| 1.7 | Operating System Access via the SAP Netweaver Application Server | [2] |
| 1.8 | Lack of SAP Application Server Secure Configuration | [2] |
| 1.9 | Unencrypted Communication | [2] |
| 1.10 | Internet Services Available and Unrestricted | [2] |
| 1.11 | Web Application Weaknesses | [2] |
| 1.12 | Lack of Security Patching | [23] |

Table 2: SAP Netweaver Application Server overview

### 3.1.1 Inadequate Authorization Definition for Netweaver AS Technical Administration

**Weakness Description**

Providing the right amount of access rights for administrators or high privileged users is a challenge in the IT industry as a whole and can be seen to affect many software systems and applications. Netweaver AS is no exception.

Excessive access rights for administrators are often a result of not implementing guidelines determining which administrators should have which rights (e.g. based on a role based model), and

instead providing administrators with an excessive amount of access rights. The underlying reason for this is a lack of IT governance at the organizational level of the company.

Netweaver AS provides task based roles. Special care should be taken to provide the right amount of task based roles to administrators based on potential risk in case the position is abused taking into account the likelihood and impact of such an event, which is very dependent on issues like the size of the company, the information stored by SAP and other organizational and process related issues.

Two examples of excessive administrator access [2]:

- An administrator is able to maintain roles and authorizations (i.e. defining what a role is able to perform) and the administration of users (i.e. assigning roles and authorizations to users). This would essentially allow an administrator to perform any task within SAP.
- A developer may have a developer role and a customizer role. This provides a developer with access to the development environment and the production environment.

The following technology related roles, and the corresponding activities exist in SAP:

- ALE developer: ALE is used for communication between SAP and non-SAP systems. This user role can develop ALE applications, manage ALE, customize ALE, etc.
- Auditor/reviser: This user role can view information, such as security logs, user authorizations, about the SAP system.
- Batch user in business departments: This user role can perform batches for business departments. This results in accessing and manipulating business information.
- Batch job operator: This user role can perform, monitor batch jobs across all environments.
- Authorization administrator (central control): This user can access and manipulate authorizations.
- Customizer: This user role can customize the SAP system in development and quality assurance environments, as well as view information in the production environment.
- Developer: This user role can customize the SAP system in development and quality assurance environments, as well as view information in the production environment.
- Help desk: This user can lock and unlock users, modify user passwords, etc.
- Operator: This user can perform technical administration such as accessing technical management functions and management of performance.
- Project coordinator: This user role can view information regarding development work, repository of developments and process definitions.
- Quality specialist: This user role can view development work, accept changes and release transports (moving changes from development to quality assurance and production).
- Administrator for security and user authorizations: This user role can make changes to user authorizations, user management, monitor information, administer audit information, and many more actions in a broad range of security related issues.
- System administrator for SAP data centre: This user role can make changes to clients, modify system configuration, administrating work processes, maintaining RFI connections, access to the security log, locking and unlocking transactions, and many more actions in a broad range of security related issues.
- Workflow developer: This user role can access and update workflow related issues.

- Central user administration: This user role can manage users including actions such as locking and unlocking users, change user passwords, assigning roles and authorizations, etc.

The list of roles is extensive and shows that the task of assigning the correct authorizations (i.e. no more and no less than is required) is difficult to administer.

**Control Objective**

The assignment of technical roles to users should be based on a least privilege principle and should only be given to the least amount of people required for technical administration of the SAP AS system. This requires the right combination of technical roles to technical individuals without assigning an unnecessary amount of technical roles that can be combined to perform actions that can lead to fraud or abuse.

In cases where an abundance of access rights are assigned to individuals, logging should be used to monitor actions that identify actions that could jeopardize the security of the SAP system or for fraud.

**Control Testing**

The allocation of technical roles can be tested by means of extracting user information from the user administration tables and determining which users have which access rights. The access rights can be analysed to determine if individual users have excessive authorizations. This process has to be performed in a case-by-case manner because the organizational structure, risk appetite of the company, size of the company, and type of business information that is stored within SAP all play a part in determining the kind of user authorizations that should be given to technical administrators.

*Note: The actual provisioning of users is an SAP level action and not specifically SAP AS. This is included in scope because of the importance of user administration in SAP AS. The user management of business related tasks, such as Segregation of Duties (SoD) for business functions is not described because it is out of scope.*

### 3.1.2 Inadequate Authorization Definition for Java Applications

**Weakness Description**

SAP AS can have Java applications run to perform a wide range of tasks. The Java applications are also subject to authorization levels to limit what can be performed by whoever uses the Java applications.

Netweaver AS can use either ABAP or Java. The Java authorizations only apply to the Java Netweaver AS variant. Two authorization concepts are supported by Netweaver AS. The two concepts are Java Authentication and Authorization Standard (JAAS) for J2EE and UME. The concepts are largely related to the technical structure of Enterprise Java Bean applications, which is an enterprise framework for Java applications.

The JAAS concept uses Principals, Roles and Permissions in EJB Java application objects. Principals are essentially users, roles essentially groups that are subject to permissions of actions that can or cannot be applied to objects and methods (comparable to actions). This allows for granular control by the developer and must be defined at the application level.

The JAAS concept is dependent on the developer implementation. This can lead to issues if the developer does not have a clear focus on authorization issues, is not subject to a rigorous code review process or if the developer is inexperienced. Furthermore, this can be difficult to analyse because authorization logic is defined in the Java source code.

The UME concept is used by Netweaver Portal and is therefore often extended to coincide with Netweaver Portal usage. Netweaver Portal can use its own authentication source (e.g. Active Directory).

The UME concept uses Permissions, Actions, UME roles and end users in EJB Java applications. The Permissions are associated with Actions and Actions are associated with UME roles and UME roles are associated with end users. The UME concept is higher level and defined in a single file for configuration. It is therefore less developer dependent and easier to review.

**Control Objective**

The Java applications that run in SAP AS are varied in their purpose. They can be programmed to perform a wide range of tasks, given that Java is general purpose programming language. The corresponding authorization requirements are therefore also broad. The security requirement regarding Java authorizations can therefore only consist of using the least privilege principle in providing the least amount of authorization for a given Java programming task to the least amount of SAP users required to perform a certain task.

**Control Testing**

The use of Java applications and its authorization structure can be tested using:

- Application security testing of the Java application: This method of testing can be performed by testing use and abuse cases using test accounts for all types of users defined in the Java application to try and perform actions that should not be allowed. For example, if a Java application is used to retrieve an employee's own salary information, the application security test can be performed to test whether a tester can view salary information from employees other than the employee that is logged in.
- Source code security review of the Java application: This method of testing can be performed by analysing source code and to determine if actions can be performed by users that should not be the case. The salary example given above also applies for the source code review.

The testing methods described above can be combined for increased effectiveness.

### 3.1.3 Inadequate Authorization Definition for RFC Calls

**Weakness Description**

SAP can be setup in a distributed manner, using multiple Netweaver Application Servers to facilitate multiple information inputs within a company. The distributed communication can be performed using RFC calls, which is a way for SAP transactions to execute remotely. There are two types of RFC calls:

- Untrusted; an RFC call is performed by an untrusted client, which could be a client Netweaver AS or a third party technology, using RFC user credentials for authentication, which are defined in the server Netweaver AS. Authorizations of the RFC user must be configured in the server.
- Trusted; an RFC call is performed by a trusted client. No credentials are required because the server Netweaver AS trusts the client, which could be a Netweaver AS or a third party technology. Authorizations of the trusted RFC user must be configured in the server.

**Control Objective**

The RFC services should be minimized to the minimum required for business and should only be accessible to systems or users that require access. In situations where the interaction between SAP AS systems or third systems is complicated, the configuration of RFC services can be misconfigured to allow for more functionality via RFC than required and possible unauthorized use.

The secure configuration of RFC, both trusted and untrusted, can be performed by:

- Ensuring use of untrusted RFC calls if possible.
- Ensuring use of strong authentication credentials for untrusted calls.
- Ensuring that the RFC can only perform the minimum necessary actions required for business.
- Ensuring that registry of (external) programs to the SAP gateway can only be added by authorized individuals.
- Ensuring that changes to the registry of (external) program to the SAP gateway is logged.
- Ensuring that the authentication credentials are not unnecessarily exposed to unauthorized individuals.
- Ensure use of logging and monitoring of RFC calls.

**Control Testing**

The use of RFC and secure authorization can be tested by mapping all RFC functions used in the entire SAP landscape and assessing whether the functions have minimum required functionality for their purpose and whether the associated authentication credentials are secure.

Untrusted RFC calls are defined on the caller side in the S_ICF object and require the authentication credentials that are defined in the system to be called. Access is granted by the called system based on the authorization rights associated with the user. The authorization credentials are defined in the S_RFC object on the called system.

Trusted RFC calls are defined on the caller side in the S_ICF object and do not require authentication credentials because the caller system is trusted. Access is granted by the called system based on using an authorization check in the S_RFCACL object. It checks whether the user that is active on the caller system can access the called system.

Use of RFC calls can be logged using transaction SM19. The log files can be analysed using transaction SM20. A process must be setup to perform actual analysis of the log files. This can inform on current usage of RFC functions.

Four RFC's are defined by [22] which are a good starting point to test the availability of RFC:

- RFC_PING: this function performs a ping that can be used to determine if RFC is available.
- RFC_SYSTEM_INFO: this function shows the kernel version, database engine, database host, SAP system ID and operating system. The technical version information can be used in further attacks.
- RFC_TRUSTED_SYSTEM_SECURITY: this function shows Windows domains, groups and user accounts on external servers.
- RFC_SET_REG_SERVER_PROPERTY: this function can lead to a DoS attack by claiming exclusive use.

### 3.1.4 Inadequate SAP gateway configuration

**Weakness Description**

The SAP gateway is used for communication between Netweaver Application Servers, primarily via RFC. The communication possibilities provide security issues if hardening steps are not taken. The possible issues include:

- A sideinfo file is available that contains possible RFC destinations (that can be called from the host). The RFC destinations in the sideinfo file can be used for abuse of outgoing RFC.
- Registrations in the SAP gateway can lead to RFC access rights to the host Netweaver AS. Therefore, the SAP gateway can be abused by adding unauthorized registrations. RFC registrations in the SAP gateway are made in the secinfo file.

**Control Objective**

Only authorized individuals must be able to add RFC definitions. The definitions are accessible in a number of manners:

- The sideinfo file is available at the operating system level (i.e. in a file accessible via the operating system).
- The transactions can be maintained via SAP using transaction SM59 and stored in table RFCDES.
- The registrations in the SAP gateway are stored in the secinfo file.

**Control Testing**

The RFC destinations can be tested by determining which individuals have access to the sideinfo file at the operating system level, this consists of individuals with access to the operating system instance in question, and access to the specific directory where the sideinfo file is stored based on the permissions of the directory and determining which individuals have access to perform transaction SM59.

The RFC registrations can be tested by determining which individuals have access to the secinfo file, which is available in a file at the operating system level.

### 3.1.5 Lack of a central user authentication system

**Weakness Description**

In a typical business environment many users require access to SAP systems. The users required to have access changes as employees join the company, move within the company and eventually leave the company. The SAP solution may also change, meaning that different groups require access than was previously the case. Such a situation requires clear insight into user access using a single user repository. However, this is not necessarily the case for SAP systems, which can complicate user management. In typical business situations, the SAP system itself may be the central user repository, or multiple repository systems may be used. This can complicate user management and lead to unnecessary user access with unnecessary authorizations.

**Control Objective**

A central user authentication system should be used to manage users, especially in cases where multiple Netweaver AS systems are used. The centralized user management system must be managed to take into account joiners, movers and leavers of employees and third parties and perform periodic reviews as is the case with generic software systems used by companies.

If a centralized user authentication system is not used then the user management should be performed directly in SAP and consideration should be taken that this may require more resources to keep up to date than use of a centralized authentication system.

**Control Testing**

This can be tested by assessing the method in which users are given access to SAP. If users are defined in LDAP or Microsoft Active Directory then a centralized user management system is used. If users are defined in SAP itself then no centralized user management system is used.

### 3.1.6 Existence of default users with default passwords

**Weakness Description**

SAP ERP, and therefore any access system to it, such as Netweaver AS contains multiple default users. The default passwords are available on the Internet. Therefore, the default passwords must be changed.

| Default User | Default Password |
|---|---|
| SAP* | 06071992 or pass depending on client |
| DDIC | 19920706 |
| EarlyWatch | Support |
| SAPCPIC | ADMIN=2E or admin |
| itsadmin | init |
| Administrator | manage |
| Developer | isdev |
| Replicator | iscopy |
| sap123 | Administrator |
| xmi_demo | sap123 |
| admin | axis2 |
| TMSADM | PASSWORD |

Table 3: Default SAP Users

Table 3 shows a list of default passwords that are available in SAP. The first three users are default users present in all SAP systems. The other users are present based on whether certain SAP systems are used. High access privileges can be gained if the default passwords are not changed.

**Control Objective**

The default users should have their default passwords changed to a non-default value. The passwords that are chosen should have a minimum length of 8 characters, should not use company names or common words and contain three of the four types of the following characters:

- Upper case character
- Low case character
- Number
- Special character

The SAP* user is required for certain administrative tasks that can only be performed using the SAP* user. The actions performed by the SAP* user should be logged and monitored to ensure that the SAP* user performs only authorized actions in the interest of the company.

**Control Testing**

The transaction SUIM or the Audit Information System can provide information about whether the default users have had their default passwords altered. These transactions should be used before a system is used by a company in a production environment and checked periodically.

### 3.1.7 Operating System Access via the SAP Netweaver Application Server

**Weakness Description**

There are transactions available in SAP ERP, transaction SM69 and transaction SM49, which allow users to execute Operating System commands, which is available for administration usage.

The SAP gateway also provides access to these commands using the sapxpg program. The sapxpg application could therefore be used to abuse the above mentioned transactions if the SAP gateway is configured incorrectly. The relevant configuration is made in the secinfo described earlier.

Access to the operating system via SAP could lead to unauthorized changes in the operating system. This could in turn lead to direct unauthorized access to the operating system.

**Control Objective**

Access to operating system commands via SAP should be limited to authorized administrators. The list of administrators should be known. Furthermore, use of operating system commands via SAP should be logged.

**Control Testing**

A mapping should be made of all users with access to transactions SM69 and SM49. The use of the sapxpg program can be limited via the secinfo file. The contents of the secinfo file must be analysed to determine who has access to the sapxpg program.

### 3.1.8 Lack of SAP Application Server Secure Configuration

**Weakness Description**

Netweaver AS contains general security parameters in a table that can be accessed via transaction RZ10. The areas of concern include password requirements and account management, RFC, the SAP gateway and Java AS.

The security parameters in RZ10 define the following:

- Minimum password length
- Password expiration time
- Maximum number of failed logins before user is locked and before user logon attempt is terminated
- Automatic unlocking of users
- Allow or disallow multiple simultaneous sessions
- Password difference (number of characters that must be different per password change)
- Number of days that an initial password is valid
- Number of days that a reset password is valid
- Allow or disallow RFC connections using expired passwords
- Location of the secinfo file (to secure the SAP gateway)
- Allow or disallow remote monitoring of the SAP gateway
- Allow or disallow remote tracing of the SAP gateway
- Enable or disable AS Java (should depend on whether Java is used on the AS)
- Enable or disable encryption of communication between the ICM and J2EE engine (which is essentially internal encryption)
- Java password rules

**Control Objective**

The security configuration should be secure to ensure that secure user management is performed, minimize service exposure and for use of encryption limited amount of internal communication (i.e. not all communication will be encrypted based on configuration from transaction RZ10).

**Control Testing**

The security settings from transaction RZ10 should be tested to determine whether they adhere to the best practice value, and whether they define the minimum required value given the services that are required for business operation.

### 3.1.9 Unencrypted Communication

**Weakness Description**

Due to the distributed nature of SAP implementations, consisting of users remotely accessing SAP systems and multiple SAP systems communicating with each other, either within an internal network, or with multiple networks and possibly even the Internet, unencrypted communication can lead to loss of confidentiality and integrity of information sent. Loss of confidentiality can include user and administrator credentials. Intercepted credentials can be used to perform unauthorized actions.

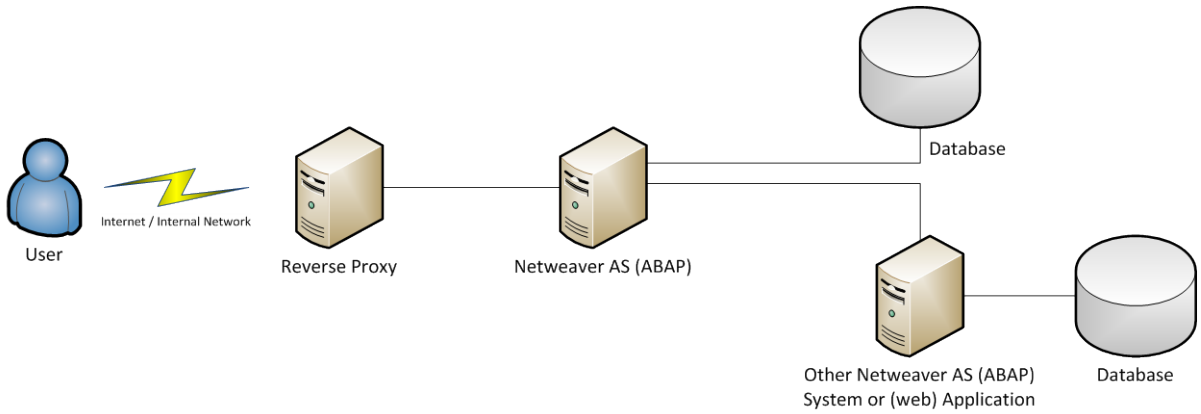


Figure 5: Communication via Internet and Internal Network

Figure 5 shows a typical setup using Netweaver AS within an internal network to show communication paths. Note that this diagram is high level and does not show important components such as firewalls. All lines of communication between the user and the various components can potentially be intercepted and modified. This risk is higher if communication is performed via the internet (which is an untrusted network), but is also present in an internal network. All lines of communications that use a network that cannot be fully trusted require encryption of data to prevent loss of confidentiality or integrity.

**Control Objective**

Encryption should be used for insecure communication paths. SAP provides encryption support via SSL and Secure Network Communications (SNC). Implementation of encryption should consider all communication paths (of which there can be many in a typical implementation as shown by Figure 3).

**Control Testing**

A mapping should be made of communication between users and systems. All lines of communication should be checked. The following lines of communication are possible:

- End user to Netweaver AS via HTTP(S) protocol
- End user (SAP GUI) to Netweaver AS ABAP via DIAG protocol
- Netweaver AS with central authentication system via LDAP
- Netweaver AS with other Netweaver AS systems or third party applications via RFC
- Netweaver AS with backend databases, SNC encryption cannot be applied

Not all lines of communication described above have a standard test procedure and will require custom testing methods based on specific testing situations.

The following standard test methods are available:

- Netweaver AS with other Netweaver AS systems, third party applications via RFC or SAP GUI using SNC. This is configured in the Personal Security Environment (PSE) which can be created using transaction STRUST. To setup an encrypted connection certificates are required for secure authentication. Furthermore, correct configuration is required to

activate the actual encryption of communication. Parameter ‘snc/enable’ is used to enable the use of encryption.

- Java services can be encrypted using the SAP Cryptographic Toolkit, it must be configured to ‘always’ use encryption. The certificates must be setup to enable encryption to work.

### 3.1.10 Internet Services Available and Unrestricted

**Weakness Description**

Netweaver AS offers multiple interfaces for administration purposes. These interfaces are not restricted by default and are therefore accessible via the local network or even the internet. Access to the administration pages could lead to information disclosure and alteration of configuration settings accessible via the administration interfaces.

The services available are offered via:

- ICF
- ICM
- Message Server
- SAP Web Dispatcher

**Control Objective**

Access to administration interfaces should be reduced to the absolute minimum required. The minimum required should consist of administrator employee access restricted to an internal management network (e.g. via VPN).

Access to the various administration interfaces can be disabled in SAP via configuration settings or blocked via a firewall.

Furthermore, logging can be enabled, where possible, of administration actions. The logging data can be monitored to check whether actions performed via administration interfaces are valid and authorized actions.

**Control Testing**

The availability of the administration interfaces can be tested by analysing the relevant configuration settings of each service or by testing whether the services are available at the standard locations via the local network or via the internet (i.e. manual testing).

The analysis of relevant security configuration settings consists of the following:

- ICF; checking whether services defined in the transaction SICF are actually required.
- ICM; checking whether the parameter ‘icm/HTTP/admin_<xx>’ has a value of a particular host, which limits access to that host.
- Message Server; checking whether the parameter ‘ms/admin_port’ has a value of ‘0’, which disables access via HTTP, that the parameter ‘ms/acl_info’ has a value, which enables the use of an access control list and that the parameter ‘rdisp/msserv_internal’ has a value of ‘0’, which disables the possibility of offering services via a different port.

Checking whether services exist can be achieved by using a list of standard locations of administration services (offered via ICF, ICM, Message Server and the SAP Web Dispatcher) and visiting the locations via the local network. E.g. the ICF is accessible via the following location:

- SAP install directory/sap/ with extensions of /bc or /bcm and many others.

### 3.1.11 Web Application Weaknesses

**Weakness Description**

It is possible to provide web applications via Netweaver AS using BSP, JSP, ABAP and Java as well as using Netweaver Portal which is described in the chapter Netweaver Portal. Web applications provide services to interact with SAP Netweaver data. Web applications can be accessible via the internal network and also the internet.

Web applications can contain weaknesses that can negatively affect the CIA of data that the web application can access, which is not necessarily all Netweaver AS data. This is common to all web applications and not just Netweaver AS or Netweaver Portal related web applications.

Examples of common vulnerabilities include SQL injection, Cross-Site Scripting and vertical/horizontal privilege escalation. OWASP has a top ten [16] of web application vulnerabilities that also affect web applications offered via Netweaver AS and Netweaver Portal. The OWASP top ten also includes methods of testing for top ten vulnerabilities and recommendations to solve the top ten vulnerabilities. There are also many other common vulnerabilities that affect web applications that could also affect Netweaver AS and Netweaver Portal web applications. Detailing all types of vulnerabilities is beyond the scope of this research. OWASP contains detailed testing methodology for web application security and testing of security [17].

Vulnerabilities in Netweaver AS and Netweaver Portal web applications can come from two sources: inherent vulnerabilities and custom vulnerabilities introduced by web application developers.

Inherent vulnerabilities come from Netweaver AS and Netweaver Portal. This will be described in chapter 2.4.1.12.

Vulnerabilities introduced by developers consist of extensions to basic functionality provided by Netweaver AS and Portal. The extensions can contain vulnerabilities such as those described in the OWASP top ten.

**Control Objective**

Web applications should operate securely and should not contain common web application vulnerabilities. Furthermore, the web application should only allow functionality that is explicitly required. For example, if a user should only be able to access a limited amount of information, the web application should not allow for manipulation to access other information that is not intended.

**Control Testing**

Web applications cannot be tested according to a standard check list of specific items. Therefore, the tests performed must be higher level. The types of tests that can detect vulnerabilities are:

- Manual and automatic code review
- Web application penetration testing

The definitions of these activities are described by OWASP [18] as:

Manual code review: *Review of the software source code to identify source code-level issues, which may enable an attacker to compromise an application, system, or business functionality. Web applications in particular are likely to have these vulnerabilities, as they are frequently developed quickly in an environment that does not allow for much security planning and testing. This should not be viewed as simply a generic software audit. Security-focused code reviews should be specifically tailored to find common vulnerabilities in applications.*

Automated source code analysis (automatic code review): Automated source code analysis involves the use of special software "tools" to conduct Static Code Analysis on software source code to identify potential vulnerabilities within the code.

Web application penetration testing (manual penetration testing): *Manual Penetration Testing involves application analysis performed by an experienced analyst, usually using a combination of open source automated utilities (either self-created or through security community) for performing task-specific functions and hands-on analysis to attempt to further 'hack' the application as an attacker.*

The three types of tests described above provide an auditor with insight regarding vulnerabilities that are present in a web application.

### 3.1.12 Lack of Security Patching

**Weakness Description**

Netweaver AS and Netweaver Portal contain inherent vulnerabilities as does all software. Inherent vulnerabilities in software exist in software due to programming weaknesses introduced by developers of the software.

Inherent vulnerabilities in software are detected by security researchers and users of software. SAP has a program whereby security researchers can submit identification of software vulnerabilities in exchange for recognition [21] which can help software researchers sell security software or with security consulting. SAP, and its software engineers, can also detect weaknesses. For example, this can be detected during testing of features that are already in production.

There are vulnerability databases available on the internet such as [19] [20] that describe known vulnerabilities of software such as SAP. These vulnerability databases also contain vulnerabilities related to Netweaver products including Netweaver AS and Netweaver Portal.

SAP provides security updates, known as patches or support packages, to secure vulnerabilities once they have been identified, but also to provide new functionality. Patches and support packages are provided periodically.

However, not all patches and support packages are installed by companies that use SAP Netweaver AS or Netweaver Portal. In fact, some companies may never install patches or support packages after the initial installation. This is a common problem that affects the entire IT industry.

If patches or support packages are not applied periodically, or immediately when they are made available by SAP the system can be at risk to vulnerabilities that have been detected.

Vulnerabilities can have various degrees of exposure, some vulnerabilities may have a full description on the internet, some vulnerabilities may not be known in detail except by SAP and the relevant security researcher that detected the vulnerability. Some vulnerabilities have associated exploits which allow someone to use the vulnerability with working examples or working code. Examples of vulnerabilities are available at [19] [20].

Furthermore, older versions of Netweaver Application Server and Netweaver Portal contain more insecure default configuration settings than newer versions. This means that possible vulnerabilities that exist in Netweaver Application Server and Netweaver Portal due to insecure configuration settings may be resolved by applying patches.

**Control Objective**

Netweaver AS and Netweaver Portal instances should have all security relevant patches and support packages installed. This will prevent exposure of known vulnerabilities.

Patches and support packages should be applied according to a patch management procedure. A patch management procedure should describe the requirements the organization places on software, which is usually described in an information security policy, and should outline what specific tasks should be taken to adhere to the high level requirements. A patch management procedure often includes the following steps:

- Registration of software used (such as instances of Netweaver AS and Netweaver Portal) including current version number and newest version available.
- Periodic installation of patches provided by the vendor (SAP).
- Periodic monitoring of vendor (SAP) information regarding release of patches and new vulnerabilities.

The precise implementation of patch management procedures can differ per organization based on information security policy requirements.

**Control Testing**

The current versions of Netweaver AS and Netweaver Portal should be determined. This value can be retrieved from the system by accessing the ‘Component Version’ menu via the ‘SAP System Data’ menu.

The current version of Netweaver AS and Netweaver Portal should be matched against the latest versions offered by SAP. This can be retrieved from the SAP support portal website.

The Netweaver component has the designation: SAPKB700xx. The xx value shows how recent the Netweaver AS and Netweaver Portal have been updated. The current (August 2012) version of Netweaver is at SAPKB70029.

## 3.2 SAP Netweaver Portal

Netweaver Portal weaknesses, control objectives and control testing will described in this paragraph as outlined in chapter 3.

An overview of risks for the Netweaver Portal is given in Table 4. The first column shows the weakness identifier. The second column provides the title of the weakness and the third column shows the reference where the weakness is described.

| Weakness ID | Weakness Description | Reference |
|---|---|---|
| 2.1 | Inadequate authorization definition for SAP Netweaver Portal | [2] |
| 2.2 | Access to default pages | [2] |
| 2.3 | Access to the SAP GUI via Netweaver Portal | [23] |
| 2.4 | Availability of Anonymous Access | [2] |
| 2.5 | Lack of Secure Network Architecture | [2] |

Table 4: SAP Netweaver Portal

### 3.2.1 Inadequate Authorization Definition for SAP Netweaver Portal

**Weakness Description**

Netweaver Portal does not inherit the ABAP security model used by Netweaver Application Server. Therefore, potential mismatches in authorizations could result in excessive authorizations in Netweaver Portal. Excessive access in Netweaver Portal could lead to excessive access of configuration pages (technical information) or certain business information depending on its connection with a backend system.

Netweaver Portal has the following objects:

- iViews; used to provide information to a user which can be linked to the backend (via Netweaver Application Server).
- Worksets; A workset group's iViews.
- Pages; A page group's worksets and iViews.

The objects can have three types of access:

- Administrator: allows for full access to a Netweaver Portal object.
- End User: allows for access to a Netweaver Portal object, based on the assigned authorizations which are checked at runtime.
- Role Assigner: allows for the assignment of access to Netweaver Portal objects.

An end user can have various access rights defined in ACL's to determine whether the user can access a certain object via the browser. The access rights consist of none, read only, write only, read/write, full access and owner.

**Control Objective**

Netweaver Portal user authorization definitions should be in line with the requirements of the user and the underlying SAP ERP system.

**Control Testing**

An overview must be made of access requirements of users in Netweaver Portal. This overview must include types of users and the relevant business information that they should be able to view. Furthermore, an overview should be made of Netweaver Portal pages, and the business information they are able to access. This may result in excessive access rights in Netweaver Portal. Care must be taken to determine the impact, it may mean that a page in Netweaver is accessible but that the backend business information is not available, which consists of a mismatch between Netweaver Portal and SAP ERP, or that a user is able to access backend business information which should not be the case.

The UME must be used to determine current access rights of users in Netweaver Portal. The assignment of access rights (ACL) should be matched with user groups.

The access rights of users can also be tested by logging in with users from all user groups available. This will allow a tester to see which access rights are available.

### 3.2.2 Access to default pages

**Weakness Description**

The portal contains many default pages that contain sensitive technical information. Only authorized technical administrators should have access to such pages. However, the default pages are not necessarily blocked for other user types, such as end users. This could result in the possibility of a broad group of users with read and possibly write access to technical configuration settings.

**Control Objective**

Access to default pages that contain technical information should be minimized to authorized technical administrators only.

**Control Testing**

There are many default configuration pages available. Many are documented by SAP and some may be available due to specific configuration or design decisions related to a specific Netweaver Portal implementation.

Therefore, default pages related specifically to Netweaver Portal should be tested using all types of users that should not have access and an understanding should be gained to determine if other types of default configuration pages are available, for example as a result of using a third party tool integrated into Netweaver Portal.

A list of default Netweaver Portal pages with technical information is provided:

- https://{URL}/sap/bc/webdynpro/sap/configure_application
- https://{URL}/sap/bc/webdynpro/sap/configure_component
- https://{URL}/sap/bc/webdynpro/sap/wd_analyze_config_appl
- https://{URL}/sap/bc/webdynpro/sap/wd_analyze_config_comp
- https://{URL}/sap/bc/webdynpro/sap/wd_analyze_config_user
- https://{URL}/sap/bc/soap/rfc
- https://{URL}/sap/bc/echo

- https://{URL}/sap/bc/FormToRfc
- https://{URL}/sap/bc/report
- https://{URL}/sap/bc/xrfc
- https://{URL}/sap/bc/xrfc_test
- https://{URL}/sap/bc/error
- https://{URL}/sap/bc/webrfc
- https://{URL}/sap/bc/bsp/sap/certreq
- https://{URL}/sap/bc/bsp/sap/certmap
- https://{URL}/sap/bc/gui/sap/its/CERTREQ
- https://{URL}/sap/bc/gui/sap/its/CERTMAP
- https://{URL}/sap/bc/bsp/sap/bsp_veri
- https://{URL}/sap/bc/bsp/sap/icf
- https://{URL}/sap/bc/IDoc_XML
- https://{URL}/sap/bc/srt/IDoc
- https://{URL}/sap/public/info

The pages listed above include technical configuration information that should not be accessible by normal end users.

### 3.2.3 Access to the SAP GUI via Netweaver Portal

**Weakness Description**

Netweaver Portal is used for providing access to SAP services via the web browser for easy access. This allows greater access to SAP services. However, providing greater access can have security implications because it increases exposure. SAP GUI is usually provided as a standard access mechanism. It can be used to login and perform SAP ERP actions. The possible actions are based on authorizations of a specific user, which can include technical administrators and super users. The SAP GUI is often accessible via the internal network only. The Netweaver Portal can increase SAP GUI access to other networks and the internet. This potentially allows users to access extremely sensitive functionality via the untrusted networks and the internet.

**Control Objective**

Exposure to critical functions in SAP should be limited. Therefore, SAP GUI access via Netweaver Portal using untrusted networks and the internet should not be possible.

**Control Testing**

The location of SAP GUI services via Netweaver Portal can vary. Therefore, testing should be broad, in search of a SAP GUI, or requires input from Netweaver Portal administrators.

A common location is the following:

- https://{URL}/sap/bc/gui/sap/its/webgui

If the SAP GUI is available via Netweaver Portal a risk assessment should be performed to assess whether exposure presents too high a risk and what the benefits of keeping the SAP GUI via Netweaver are.

### 3.2.4 Availability of Anonymous Access

**Weakness Description**

Netweaver Portal allows for anonymous access of web pages (and iViews which are web pages as well). This allows for anonymous access to provide information to customers, etc. The usage of such functionality can lead to unauthorized access of confidential information stored within anonymous pages due to allowing too much anonymous access or mis-configuration of anonymous access. This is especially the case for internet accessible Netweaver Portals.

**Control Objective**

Information made available on pages available anonymously should only consist of publically available information (i.e. not confidential information). All pages that are accessible anonymously should be assessed whether they contain confidential information.

**Control Testing**

Manual testing can be used to determine if pages are available anonymously. The following approaches can be performed:

- Visiting the home or login page of the Netweaver Portal and determining if anonymous pages are available
- Using tools to scan Netweaver Portal for common pages;
- Checking for availability of anonymous access via configuration settings; the UME properties that require assessment are:
    - ume.login.anonymous_user.mode = 1;
    - ume.login.guest_user.uniqueids = (list of unique users, which can be linked to pages that can be accessed);
    - iViews, pages and worksets that have a value of anonymous in the corresponding property value.

### 3.2.5 Lack of Secure Network Architecture

**Weakness Description**

Netweaver Portal can be exposed beyond the internal network to untrusted networks and the internet. This exposure requires secure network architecture to protect the Netweaver Portal, underlying SAP components and systems from external sources. Such a secure network architecture consists of providing services via defensive layers.

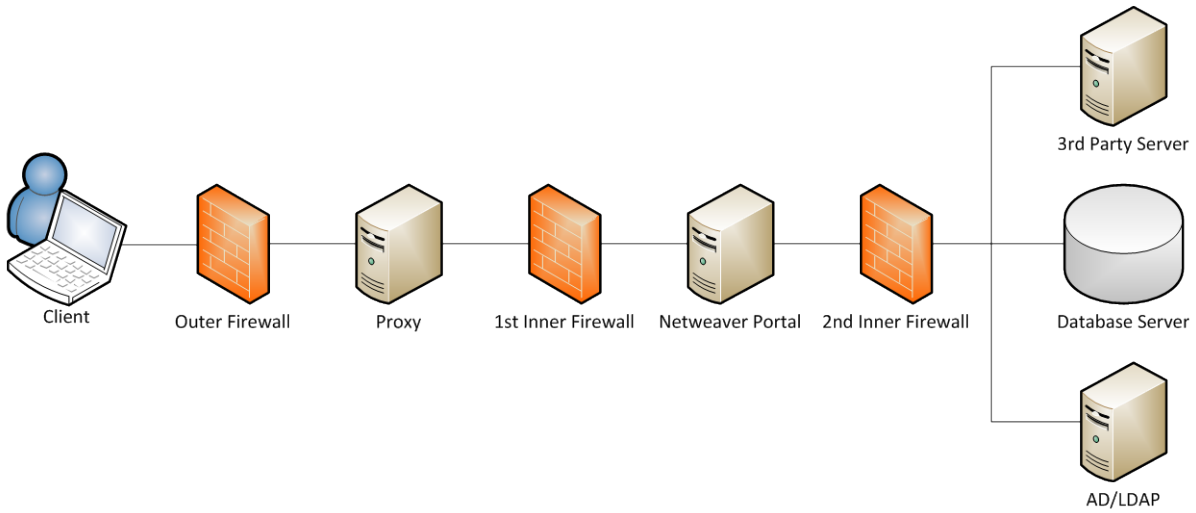


Figure 6: Secure Network Architecture

Figure 6 shows a secure architecture with multiple layers separated by a firewall at each layer. The layer between the outer firewall and the 1st inner firewall is essentially a DMZ. This layered approach ensures that Netweaver Portal and underlying data is protected by multiple firewalls. An attacker from an untrusted network or the internet would have to exploit weaknesses in the proxy, multiple firewalls and the Netweaver Portal to perform a meaningful attack that could access confidential company information.

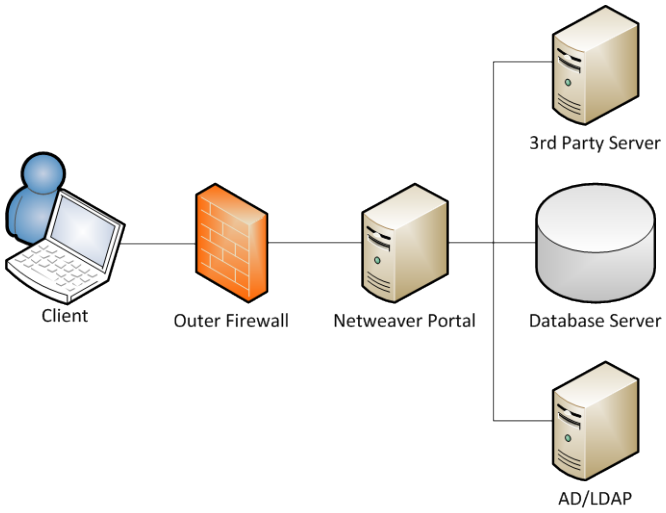


Figure 7: Insecure Network Architecture

Figure 7 shows an insecure network architecture. Such a network architecture is common in many companies. It shows a single firewall to protect the inner network from untrusted networks and the internet.

**Control Objective**

A multi-layered defensive network structure should be used to connect to untrusted networks or the internet. Such a multi-layered defensive network should have multiple layers separated by firewalls with a minimum type of network traffic allowed by each firewall.

**Control Testing**

The network structure must be understood based on analysis of network documentation and discussions with network engineers. The key questions surround the exposure of Netweaver Portal, and other infrastructure, towards untrusted networks and the internet. An attacker from an untrusted network or the internet would only have to compromise the Netweaver Portal and a single firewall to perform a meaningful attack that could access confidential company information.

## 3.3 Chapter Conclusion

This chapter described the following:

- Weaknesses that affect Netweaver Application Server and Netweaver Portal;
- Control objectives that can be used for control testing;
- Control testing methods to determine whether weaknesses are present in Netweaver Application Server and Netweaver Portal implementations.

The control testing methods are written as a general description and not a step-by-step testing guide. For a testing method in a structured manner refer to Appendix C.

# 4 Conclusion and Future Work

## 4.1 Conclusions

Conclusions are based directly on the research questions. Each research question will be discussed in the following sub-chapters.

### 4.1.1 Overall Research Question

*Which testing methods must an IT auditor use to assess weaknesses in critical SAP components Netweaver Application Server and Netweaver Portal?*

The research performed in this thesis shows that there are many technical steps involved in securing an SAP environment using Netweaver Application Server and Netweaver Portal. These steps are not trivial and therefore not necessarily performed by companies or tested during audits.

The impact of not performing steps outlined in the thesis varies and affects the CIA of information stored within SAP but also includes potential of indirect loss of CIA of business information. For example, technical information disclosure or the possibility to change specific configuration settings could subsequently allow an attacker to perform more serious attacks that affects CIA of business information.

Judging by the wide range of potential weaknesses and complicated methods of dealing with weaknesses related to Netweaver Application Server and Netweaver Portal and SAP ERP in general it shows that companies may not be dealing with these issues because they may not be understood. This is also shown by interview results.

The testing methods provided in this thesis show that clear identification of weaknesses in Netweaver Application Server and Netweaver Portal can be made to identify issues that could lead to loss of CIA of system and business information. The testing methods can be used test whether Netweaver Application Server and Netweaver Portal systems are subject to the weaknesses described.

### 4.1.2 First Research Question

*Describe Netweaver Application Server, Netweaver Portal and related components relevant to weaknesses described in the thesis.*

The Netweaver Application Server and Netweaver Portal components have been described in detail including important security related information (i.e. sub-components that can affect security). A technical overview was provided of both components. Furthermore, the underlying infrastructure used by SAP, consisting of Operating Systems, databases and networking was provided.

Chapter 2 shows that it is possible to determine the inner-workings of Netweaver Application Server and Netweaver Portal which is required to understand possible weaknesses that may affect the system and information stored within it.

### 4.1.3 Second Research Question

*Describe the weaknesses regarding the use of SAP Netweaver Application Server and Netweaver Portal.*

Twelve weaknesses were included for Netweaver Application Server and five weaknesses were included for Netweaver Portal. The following weaknesses were included:

- Inadequate Authorization Definition for Netweaver AS Technical Administration
- Inadequate Authorization Definition for Java Applications
- Inadequate Authorization Definition for RFC Calls
- Inadequate SAP gateway configuration
- Lack of a central user authentication system
- Existence of default users with default passwords
- Operating System Access via the SAP Netweaver Application Server
- Lack of SAP Application Server Secure Configuration
- Unencrypted Communication
- Internet Services Available and Unrestricted
- Web Application Weaknesses
- Lack of Security Patching
- Inadequate authorization definition for SAP Netweaver Portal
- Access to default pages
- Access to the SAP GUI via Netweaver Portal
- Availability of Anonymous Access
- Lack of Secure Network Architecture

The weaknesses show that there are technical, configuration and organizational challenges involved to secure Netweaver Application Server and Netweaver Portal. The weaknesses were described in detail in chapter 3.

### 4.1.4 Third Research Question

*Describe the desired state that should be achieved related to weaknesses.*

Essentially, the desired state is the state in which the weaknesses identified as a result of the research question 2 are not applicable or mitigated. The fact that ideal states are available for the weaknesses shows that solutions are available to mitigate these weaknesses. Each weakness identified has a respective desired state (or solution to solve the weakness). The desired state of the weakness was described in detail in chapter 3.

### 4.1.5 Fourth Research Question

*Develop a detailed approach to test weaknesses in Netweaver Application Server and Netweaver Portal.*

The control testing methods were included for all weaknesses. The level at which testing methods are described varies based on the issue at hand. For example, some configuration issues were described in great detail including parameters and their required settings whereas other testing methods are more high level with steps such as ‘perform a penetration test or perform a source

code review'. Such activities large tasks by themselves and have therefore not been described in greater detail.

The availability of detailed control testing shows that it is possible to have concrete and viable steps to mitigate weaknesses. The control testing methods were developed based on lessons learned from the SAP Security Workshop, literature research and interviews held with SAP security industry professionals. Furthermore, experience gained performing audit and security has helped in determining control testing methods.

The work program was developed using the understanding of weaknesses as a result of the research performed and using experience as an auditor and security specialist to convert into a structured manner including structured testing methods.

The control testing was described in general descriptive form in chapter 3 and in a structured manner in Appendix C.

## 4.2 Future Research

Future research could consist of validating the research conducted in this thesis within a test environment or customer implementation(s). Multiple tests on various test setups or customer locations are required as opposed to one, because the various configurations options and SAP components involved could have implications on security.

Furthermore, future research could broaden the scope of components within scope. This would broaden the lessons learned to include more types of SAP implementations.

## 4.3 Reflection on Research Performed

I have gained a great deal of insight in issues related to using Netweaver Application Server and Netweaver Portal. Although a risk assessment was not part of this research it is clear that there are direct and indirect threats to the CIA of business information that would most likely pose a risk to business. The research did not include validation of the weaknesses in a practical setting nor did it include a risk assessment of impact on business, which I think would be very interesting next step for further research. It would be interesting to see if businesses are indeed exposed to risks that are not widely understood by industry. The fact that industry is not widely aware of such potential risks is a problem, yet it may also be a blessing in the fact that attackers may also not be aware of such issues which decreases likelihood and therefore risk.

**References**


[1] SAP AG Annual Report, http://www.sapannualreport.com/2010/en/management-report.html, 2010

[2] Mario Linkies, Horst Karin, SAP Security and Risk Management, SAP Press, 2nd Edition, 2011

[3] SAP Netweaver AS, http://help.sap.com/saphelp_nw70/helpdata/en/84/54953fc405330ee10000000a114084/content.htm

[4] SAP Netweaver AS architecture, http://help.sap.com/saphelp_nw70/helpdata/en/84/54953fc405330ee10000000a114084/content.htm

[5] National Institute of Standards and Technology (NIST) Security Configuration Checklists Program, http://csrc.nist.gov/groups/SNS/checklists/

[6] NIST, Security Configuration Checklists Program, Windows Server 2008, http://benchmarks.cisecurity.org/tools2/windows/CIS_Windows_Server_2008_Benchmark_v1.1.0.pdf

[7] NIST, Security Configuration Checklists Program, Red Hat Enterprise Linux 5.1, http://benchmarks.cisecurity.org/tools2/linux/CIS_RHEL_5.0-5.1_Benchmark_v1.1.2.pdf

[8] NIST, Security Configuration Checklists Program, Oracle 10g, http://iase.disa.mil/stigs/downloads/zip/unclassified_oracle10_v8r1.8_checklist_20100827.zip

[9] NIST, Security Configuration Checklists Program, Microsoft SQL 2005, http://benchmarks.cisecurity.org/tools2/sqlserver/CIS_SQL2005_Benchmark_v1.2.0.pdf

[10] NIST, Security Configuration Checklists Program, Cisco iOS 12.4, http://www.nsa.gov/ia/_files/routers/I33-002R-06.pdf

[11] Onapsis, Black Hat Europe presentation, 2012, http://www.onapsis.com/slides/ONAPSIS-BlackHat-EU-2012_CyberAttacks_to_SAP_systems.pdf

[12] SAP Help, Internet Communication Framework (ICF), http://help.sap.com/saphelp_nw70ehp1/helpdata/en/72/c730e0c06511d4ad310000e83539c3/content.htm

[13] Succesvol Studeren Voor Biv/Ao / 1, 2nd Edition, 2001

[14] ISO 27000, Information security management systems — Overview and vocabulary, http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933_ISO_IEC_27000_2009.zip, 2009

[15] NIST, Information Security Terms, http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf, 2011

[16] OWASP top ten, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project, 2010

[17] OWASP, https://www.owasp.org/index.php/Main_Page, present

[18], OWASP definitions, https://www.owasp.org/index.php/Definition_for_Security_Assessment_Techniques, present

[19], National Vulnerability Database, http://nvd.nist.gov/, present

[20], Common Vulnerability and Exposures, http://cve.mitre.org/, present

[21], Archive for Acknowledgments to Security Researchers, http://www.sdn.sap.com/irj/scn/index?rid=/webcontent/uuid/50316177-762d-2f10-0993-a2206cc349b4, present

[22], Perfect Storm - The Brave New World of SAP Security, Layer Seven Security, http://www.isaca.org/Groups/Professional-English/sap-applications/GroupDocuments/Perfect%20Storm%20-%20The%20Brave%20New%20World%20of%20SAP%20Security%20v1.2.pdf, 2011

[23], Secure Configuration of SAP NetWeaver Application Server Using ABAP, SAP Press, 2012

# Appendix A. Interview Questions

The interview questions below were provided to industry professionals in the IT audit function (internal and external IT auditors).

## Current Testing Methodology

1. Describe the current testing methodology of SAP systems at your company or customer(s).

2. What focus areas are parts of the testing methodology? (e.g. authentication, authorization (user access rights, hardening, patch management)

3. What components are in scope of testing? (e.g. SAP ERP, Single-Sign On solutions, SAP Netweaver Application Server, SAP Netweaver Portal, Operating Systems, Databases, Networks)

4. Do you feel there are areas of concern/weakness regarding security that are not covered by current testing methods used by your company or audit/test team/clients?

5. If areas of SAP security are highlighted that are currently not part of your current testing methodology and could add security insight would you consider these areas of SAP security for future testing?

6. Have any specific measures been taken to increase the security of Netweaver Application Server or Netweaver Portal?

7. Have any specific measures been taken to increase the security measures related to Remote Function Calls (RFC), patching, Netweaver Application Server gateway, encryption, web application weaknesses, availability of unnecessary default pages or secure networking principles?

## Impact on business in the event of an incident

8. What impact would a loss of confidentiality of business information stored in SAP have on business? Please indicate on a scale of 1-5 (5 being highest) and include a description.
   Loss of personal/employee information:
   Loss of financial information:
   Loss of operational information:

9. What impact would a loss of integrity of business information stored in SAP have on business? Please indicate on a scale of 1-5 (5 being highest) and include a description.
   Loss of integrity of personal/employee information:
   Loss of integrity of financial information:
   Loss of integrity of operational information:

10. What impact would a loss of availability of business information stored in SAP have on business? Please indicate on a scale of 1-5 (5 being highest) and include a description.
    Loss of 1 hour:
    Loss of 4 hours:
    Loss of 1 day:
    More than 3 days:

## Incidents Related to SAP

11. Has your company or clients had any incidents regarding security of SAP systems. Describe the incident (if details are confidential please outline the issue).

12. What impact did incidents have on SAP systems? Did it include loss of confidentiality, integrity or availability of business information?

13. What weaknesses related to SAP were identified as a result of the incident? (E.g. authorization, configuration, patching, etc.)

# Appendix B. Interview Response

The interview responses have been paraphrased and anonymized by the author of the thesis. Answers that were provided multiple times have been minimized to one individual answer.

## Current Testing Methodology

1. Describe the current testing methodology of SAP systems at your company or customer(s).
   *Answer(s): Testing has been performed as part of SOX, external integrated audits and internal audit. Occasionally security tests in the form of penetration tests have been performed that also include SAP systems.*

2. What focus areas are parts of the testing methodology? (E.g. authentication, authorization (user access rights, hardening, and patch management)
   *Answer(s): Testing is primarily related to user management and authorization management. As part of general IT General Controls (ITGC) testing the full stack is taken into consideration: SAP ERP, operating systems, databases and networking. Specific tests for Netweaver Application Server and Netweaver Portal have not been performed thus far.*

3. What components are in scope of testing? (e.g. SAP ERP, User repositories (LDAP/AD), Single-Sign On solutions, SAP Netweaver Application Server, SAP Netweaver Portal, Operating Systems, Databases, Networks)
   *Answer(s): SAP ERP and authentication/user repository (e.g. LDAP/AD) is primarily the focus in terms of component scope. Layers such as OS, databases and networks are in scope of integrated audits.*

4. Do you feel there are areas of concern/weakness regarding SAP security that are not covered by current testing methods used by your company or audit/test team/clients?
   *Answer(s): Some respondents feel that SAP systems deal with security of its own systems and some respondents feel that they do not have enough specific knowledge about SAP systems inner workings (e.g. at configuration level) to confidently answer the question.*

5. If areas of SAP security are highlighted that are currently not part of your current testing methodology and could add security insight would you consider these areas of SAP security for future testing?
   *Answer(s): If the potential business impact can be described, respondents would be interested determining whether weaknesses exist in the systems that are not currently part of testing plans.*

6. Have any specific measures been taken to increase the security of Netweaver Application Server or Netweaver Portal?
   *Answer(s): Access to Netweaver Portal has been restricted to the internal network. Strict patching requirements exist for most respondents.*

7. Have any specific measures been taken to increase the security measures related to Remote Function Calls (RFC), patching, Netweaver Application Server gateway, encryption, web application weaknesses, availability of unnecessary default pages or secure networking principles?
   *Answer(s): Patching is a requirement for most respondents (however some have doubts whether this is performed properly for SAP specific systems, encryption is often not performed (however, this is an accepted risk). Other items are not part of specific requirements.*

## Impact on business in the event of an incident

*8.* What impact would a loss of confidentiality of business information stored in SAP have on business? Please indicate on a scale of 1-5 (5 being highest) and include a description.
Answer(s):
*Loss of personal/employee information: Most respondents indicate that loss of personal/employee information would be a serious problem for their company/client. This is mostly due to the willingness to protect employees, but also to prevent loss of reputation.*
*Loss of financial information: Most respondents indicate that a loss of financial information would be a serious issue for their company/client.*
*Loss of operational information: Most respondents indicate that operational information is critical when it includes financial information. One respondent indicated that industrial information (e.g. industrial process information) is not critical.*

9. What impact would a loss of integrity of business information stored in SAP have on business? Please indicate on a scale of 1-5 (5 being highest) and include a description.
*Loss of integrity of personal/employee information: Integrity of employee information is extremely important for one of the respondents due to business objectives related to employee satisfaction. Other respondents indicate that pay role related information is the most important.*
*Loss of integrity of financial information: Integrity of financial is considered critical.*
*Loss of integrity of operational information: Integrity of operational information is important, and critical for manufacturing.*

10. What impact would a loss of availability of business information stored in SAP have on business? Please indicate on a scale of 1-5 (5 being highest) and include a description.
*Loss of 1 hour: Most respondents indicate that 1 hour is acceptable. The manufacturing respondent indicated that 1 hour is unacceptable due to direct loss of manufacturing time.*
*Loss of 4 hours: Most respondents indicate that 4 hours is acceptable. The manufacturing respondent indicated that 4 hour is unacceptable due to direct loss of manufacturing time.*
*Loss of 1 day: Loss of 1 day is unacceptable for operational systems, except for personnel/employee information.*
More than 3 days: More than 3 days is considered unacceptable for all respondents.

## Incidents Related to SAP

11. Has your company or clients had any incidents regarding security of SAP systems. Describe the incident (if details are confidential please outline the issue).

*Answer(s): Most respondents indicate that they have not had specific incidents related to SAP. One respondent indicated that an incident was based on an insider threat by someone with privileged access to the SAP system. Another respondent indicated that loss of confidentiality was achieved via SQL system of a third party application that accessed SAP information.*

12. What impact did incidents have on SAP systems? Did it include loss of confidentiality, integrity or availability of business information?
    *Answer(s): One respondent indicated that an incident that led to loss of integrity of business information (employee details that affected salary information). Another respondent indicated that loss of confidentiality of SAP information has occurred, although the exact impact was never fully understood.*

13. What weaknesses related to SAP were identified as a result of the incident? (E.g. authorization, configuration, patching, etc.)
    *Answer(s): Authorization weaknesses were identified for the loss of integrity incident. The loss of confidentiality was related to weaknesses related to a third party application that accessed SAP information.*

# Appendix C. Work Program

The following table shows the work program that accompanies the thesis. The weaknesses, control objective and control testing are described in a structured manner. The weaknesses have a direct mapping to weaknesses described in the thesis.

| Nr. | Weakness | SAP Component | Control Objective | Control Testing |
|---|---|---|---|---|
| 1.1 | Inadequate Authorization Definition for Netweaver AS Technical Administration | Netweaver AS | The assignment of technical roles to users should be based on a least privilege principle and should only be given to the least amount of people required for technical administration of the SAP AS system. | 1. Obtain the design of user authorizations.<br>2. Obtain the list of users with their respective roles.<br>3. Obtain the technical implementation of user authorizations for role types: developers, customizers, batch jobs operators, IT Support (helpdesk, etc.), QA, system administrators, user administrators. This can be achieved by use of extraction tools, data analysis or direct analysis within SAP.<br>4. Examine the design of user authorizations and determine whether least privilege principle and Segregation of Duty is considered.<br>5. Examine the list of users and their authorizations and determine whether the provisioning of users and their access rights are justified. Consider the importance of the SAP system in question and impact on Netweaver AS and Netweaver Portal. |
| 1.2 | Inadequate Authorization Definition for Java Applications | Netweaver AS | The security requirement regarding Java authorizations can therefore only consist of using the least privilege principle in providing the least amount of authorization for a given Java programming task to the least amount of SAP users required to perform a certain task. | Two general testing methods:<br>a) Security testing of the Java application(s).<br>1. Obtain access to all types of users with access Netweaver AS.<br>2. Determine the purpose/functionality of Java applications and critical business/technical information involved.<br>3. Attempt abuse case testing to access critical business/technical information.<br><br>b) Source code review Java application(s).<br>1. Determine the purpose/functionality of Java applications and critical business/technical information involved.<br>2. Obtain the design documentation including user types and their associated authorizations.<br>3. Obtain the source code of the Java application(s).<br>4. Obtain the source code documentation.<br>5. Analyse the source code documentation and source code to determine the authorization models used (either JAAS or UME).<br>6. Determine whether access rights are in line with the design.<br>JAAS: Consider Principals, Roles and Permissions, implementation is developer specific and as such a custom analysis is required.<br>UME: Consider Permissions, Actions, UME roles, consider the roles and the actual access rights involved and compare with the design. |
| 1.3 | Inadequate Authorization Definition for RFC Calls | Netweaver AS | The RFC services should be minimized to the minimum required for business and should only be accessible to systems or users that require access. | 1. Obtain the design of RFC connections.<br>2. Obtain the actual list of RFC connections:<br>Untrusted RFC: use S_ICF and S_RFC.<br>Trusted RFC: S_ICF and S_RFCACL.<br>3. Obtain RFC logging information using SM19 and SM20.<br>4. Examine the design of RFC connections.<br>5. Examine the implementation of RFC and compare with the design.<br>6. Examine the implementation of RFC and determine whether strong credentials are used.<br>7. Examine the implementation of RFC and determine whether unnecessary RFC connections are defined (e.g. default or unused RFC).<br>8. Examine the logging information to determine that connections are in line with the design. |

| Nr. | Weakness | SAP Component | Control Objective | Control Testing |
|---|---|---|---|---|
| 1.4 | Inadequate SAP gateway configuration | Netweaver AS | Only authorized individuals must be able to add RFC definitions. | 1. Obtain the design of configuration settings (if available).<br>2. Determine the location of the sideinfo file. Determine which administrators/users can access the sideinfo file (at the file system level).<br>3. Determine the users with access to transaction SM69 and table RFCDES. |
| 1.5 | Lack of a central user authentication system | Netweaver AS | A central user authentication system should be used to manage users. | 1. Obtain design documentation of the user authentication system.<br>2. Obtain login credentials of an SAP end user, an SAP administrator, Netweaver AS and Netweaver Portal administrators<br>3. Determine whether a central user repository is used or whether users login users a SAP specific password. |
| 1.6 | Existence of default users with default passwords | Netweaver AS | The default users should have their default passwords changed to a non-default value. | 1. Obtain design documentation to show that default users are periodically checked for default passwords and their state (active/disabled).<br>2. Determine (in conjunction with the SAP administrators) that passwords have a minimum length of 8 characters and are complex.<br>3. Determine whether a user can login via SAP GUI and Netweaver Portal using the following default passwords:<br><br>SAP* / 06071992 or pass depending on usage<br>DDIC / 19920706<br>EarlyWatch / support<br>SAPCPIC / ADMIN=2E or admin<br>itsadmin / init<br>Administrator / manage<br>Developer / isdev<br>Replicator / iscopy<br>sap123 / Administrator<br>xmi_demo / sap123<br>admin / axis2<br>TMSADM / PASSWORD |
| 1.7 | Operating System Access via the SAP Netweaver Application Server | Netweaver AS | Access to operating system commands via SAP should be limited to authorized administrators. | 1. Obtain documentation to show that access to transactions SM49 and SM69 should be limited to authorized personnel.<br>2. Obtain documentation to show that access to the SAP gateway, and specifically the sapxpg program, is limited to authorized personnel.<br>3. Obtain the list of users with access to transactions SM49 and SM69.<br>4. Obtain the secinfo file.<br>5. Determine whether the list of users with access to SM49 and SM69 is appropriate.<br>6. Determine whether the secinfo file is configured to limit access to the operating system via the SAP gateway. |

| Nr. | Weakness | SAP Component | Control Objective | Control Testing |
|---|---|---|---|---|
| 1.8 | Lack of SAP Application Server Secure Configuration | Netweaver AS | The security configuration should be secure to ensure that secure user management is performed, minimize service exposure and for use of encryption limited amount of internal communication. | 1. Obtain documentation to show general security configuration parameters.<br>2. Obtain the general security configuration settings stored in RZ10.<br>3. Determine whether the following has been set in RZ10:<br><br>• Minimum password length (set to at least 8)<br>• Password expiration time (set to at least 90 days)<br>• Maximum number of failed logins before user is locked and before user logon attempt is terminated (set to at least 5 attempts)<br>• Automatic unlocking of users (set to true)<br>• Allow or disallow multiple simultaneous sessions (set to disabled)<br>• Password difference (number of characters that must be different per password change) (set to at least 12)<br>• Number of days that an initial password is valid (set to at most 3 days)<br>• Number of days that a reset password is valid (set to at most 3 days)<br>• Allow or disallow RFC connections using expired passwords (set to disallow)<br>• Location of the secinfo file (to secure the SAP gateway) (set to a secure location)<br>• Allow or disallow remote monitoring of the SAP gateway (set to disallow)<br>• Allow or disallow remote tracing of the SAP gateway (set to disallow)<br>• Enable or disable AS Java (should depend on whether Java is used on the AS)<br>• Enable or disable encryption of communication between the ICM and J2EE engine (which is essentially internal encryption) (set to true)<br>• Java password rules (set to strict password rules, see above) |
| 1.9 | Unencrypted Communication | Netweaver AS | Encryption should be used for insecure communication paths. | 1. Obtain SAP and network communication documentation.<br>2. Obtain system configuration settings from the Personal Security Environment (PSE), parameter 'snc/enable' and the SAP cryptographic Toolkit.<br>3. Discuss with the administrators whether encryption is covered at all levels (i.e. between end user and Netweaver AS/Netweaver Portal, between the various Netweaver AS systems, between Netweaver AS and backend systems such as the database).<br>4. Determine whether levels of encryption is sufficient. Also take into account network level encryption controls (such as segregation of networks). |
| 1.10 | Internet Services Available and Unrestricted | Netweaver AS | Access to administration interfaces should be reduced to the absolute minimum required. | 1. Obtain design documentation regarding restriction of administration interface access.<br>2. Obtain and determine whether the correct security settings are used:<br>• ICF; checking whether services defined in the transaction SICF are actually required.<br>• ICM; checking whether the parameter 'icm/HTTP/admin_<xx>' has a value of a particular host, which limits access to that host.<br>• Message Server; checking whether the parameter 'ms/admin_port' has a value of '0', which disables access via HTTP, that the parameter 'ms/acl_info' has a value, which enables the use of an access control list and that the parameter 'rdisp/msserv_internal' has a value of '0', which disables the possibility of offering services via a different port.<br>3. Perform manual testing to access administration interfaces. Access the Netweaver AS and Netweaver Portal pages via {SAP location}/sap, /bc, /bcm |

| Nr. | Weakness | SAP Component | Control Objective | Control Testing |
|---|---|---|---|---|
| 1.11 | Web Application Weaknesses | Netweaver AS | Web applications should operate securely and should not contain common web application vulnerabilities. | 1. Determine, in cooperation with SAP administrators, whether custom web application functionality has been incorporated/used.<br>2. Perform an analysis of information assets that are involved with the custom web application functionality.<br>3. Perform a web application penetration test. Note: official permission is required.<br>4. Obtain the source code of custom web application.<br>5. Perform a web application source code review. |
| 1.12 | Lack of Security Patching | Netweaver AS | Netweaver AS and Netweaver Portal instances should have all security relevant patches and support packages installed. | 1. Obtain the (SAP) patch management policy.<br>2. Obtain the current patch level from the 'Component Version' menu via the 'SAP System Data' menu.<br>3. Match the current patch levels with those from the SAP support website (http://scn.sap.com).<br>4. Determine whether all security patches have been applied. |
| 2.1 | Inadequate authorization definition for SAP Netweaver Portal | Netweaver Portal | Netweaver Portal user authorization definitions should be in line with the requirements of the user and the underlying SAP ERP system. | 1. Obtain design documentation of roles within Netweaver Portal.<br>2. Obtain current role definitions for Netweaver Portal from the UME.<br>3. Obtain user credentials for all types of users that can access Netweaver Portal<br>4. Determine the types of business information that users should be able to view in the Netweaver Portal.<br>5. Based on role definitions and access definitions determine whether access is appropriate.<br>6. Login to Netweaver Portal and test whether access is appropriate for all types of users. |
| 2.2 | Access to default pages | Netweaver Portal | Access to default pages that contain technical information should be minimized to authorized technical administrators only. | 1. Obtain the design documentation regarding removal of access to default Netweaver Portal pages.<br>2. Determine whether the following default pages are inaccessible to end users:<br>• https://{URL}/sap/bc/webdynpro/sap/configure_application<br>• https://{URL}/sap/bc/webdynpro/sap/configure_component<br>• https://{URL}/sap/bc/webdynpro/sap/wd_analyze_config_appl<br>• https://{URL}/sap/bc/webdynpro/sap/wd_analyze_config_comp<br>• https://{URL}/sap/bc/webdynpro/sap/wd_analyze_config_user<br>• https://{URL}/sap/bc/soap/rfc<br>• https://{URL}/sap/bc/echo<br>• https://{URL}/sap/bc/FormToRfc<br>• https://{URL}/sap/bc/report<br>• https://{URL}/sap/bc/xrfc<br>• https://{URL}/sap/bc/xrfc_test<br>• https://{URL}/sap/bc/error<br>• https://{URL}/sap/bc/webrfc<br>• https://{URL}/sap/bc/bsp/sap/certreq<br>• https://{URL}/sap/bc/bsp/sap/certmap<br>• https://{URL}/sap/bc/gui/sap/its/CERTREQ<br>• https://{URL}/sap/bc/gui/sap/its/CERTMAP<br>• https://{URL}/sap/bc/bsp/sap/bsp_veri<br>• https://{URL}/sap/bc/bsp/sap/icf<br>• https://{URL}/sap/bc/IDoc_XML<br>• https://{URL}/sap/bc/srt/IDoc<br>• https://{URL}/sap/public/info |
| 2.3 | Access to the SAP GUI via Netweaver Portal | Netweaver Portal | Exposure to critical functions in SAP should be limited. Therefore, SAP GUI access via Netweaver Portal using untrusted networks and the internet should not be possible. | 1. Determine, in collaboration with SAP administrators, the level of accessibility of the Netweaver Portal (i.e. within the internal network only, consider segmentation of the internal network, access via the internet).<br>2. Determine whether the SAP GUI is available via the Netweaver Portal and whether this is appropriate.<br><br>A common location is the following:<br>• https://{URL}/sap/bc/gui/sap/its/webgui |

| Nr. | Weakness | SAP Component | Control Objective | Control Testing |
|---|---|---|---|---|
| 2.4 | Availability of Anonymous Access | Netweaver Portal | Information made available on pages available anonymously should only consist of publically available information (i.e. not confidential information). All pages that are accessible anonymously should be assessed whether they contain confidential information. | 1. Obtain the design documentation regarding anonymous access.<br>2. Determine whether anonymous access to Netweaver Portal should be available.<br>3. Checking for availability of anonymous access via configuration settings; the UME properties that require assessment are:<br>o ume.login.anonymous_user.mode = 1;<br>o ume.login.guest_user.uniqueids = (list of unique users, which can be linked to pages that can be accessed);<br>o iViews, pages and worksets that have a value of anonymous in the corresponding property value.<br>4. Test whether Netweaver Portal pages are available without user credentials. |
| 2.5 | Secure Architecture | Netweaver Portal | A multi-layered defensive network structure should be used to connect to untrusted networks or the internet. | 1. Obtain SAP component diagrams and network diagrams.<br>2. Determine the exposure of SAP systems to the internal network and internet.<br>3. Determine whether multiple network layers are present. |