Risk Assessment in Online Banking System

K.V.D. Kiran[1], P.Sruthi[2], P.S. Neema[3], G.V.S. Manju Vani[4], Rishikesh Sahu[5]

(Computer Science and Engineering, K L E F University (KLU), India)

ABSTRACT- *With the development of information technology and the popular use of the information network system, the security of the information system becomes particularly important. To ensure the security of the information system, it is a key point to have risk assessment. This paper deals with the risk assessment in information security of distributed banking sector. The process of identification and analysis of various assets (both hardware and software), vulnerabilities, threats and risks in distributed banking sector has assumed utmost importance. This paper also presents collective information regarding various risk assessment methodologies like qualitative, quantitative and hybrid methods and tools such as OCTAVE and IRAM that are being employed in order to perform risk assessment in information security.*

Keywords- *assets, authentication, concurrency, distributed computing, quantitative and qualitative methodologies, risk assessment, security, threat, vulnerabilities.*

1. Introduction

Distributed computing is a field of computer science that studies distributed systems. A distributed system is a software system in which components located on networked computers communicate and coordinate their actions by passing messages. Banking sector is one of the main applications of distributed systems. The process of risk assessment in information security mainly deals with identification of the cause of a particular risk. The presence of various vulnerabilities that pose threat to entire system generally results in risk. Proper identification of various software and hardware assets plays an important role in identification of these vulnerabilities and threats. A proper risk assessment methodology like quantitative, qualitative or hybrid can be applied as per requirement.

2. Terminology, Meaning and Description

2.1 Banking System

It is a structural network of institutions that offer financial services within a county. The members of the banking system and the functions they typically perform include:

- commercial banks that take deposits and make loans,
- investment banks which specialize in capital market issues and trading, and
- National central banks that issue currency and set monetary policy.

2.2 Distributed System

A distributed system consists of a collection of autonomous computers, connected through a network and distribution middleware, which enables computers to coordinate their activities and to share the resources of the system, so that users perceive the system as a single, integrated computing facility.

It is a piece of software which ensures that a collection of independent computers that appears to its users as a single coherent system.

2.3 Transaction

It is collection of series of events which change a database from one consistent state to other. Distributed transactions are transactions against multiple applications or hosts.

2.4 Resource Sharing

It is the ability to use any hardware, software or data anywhere in the system. It describing how

- Resources are provided,
- They are used and
- Provider and user interact with each other

2.5 Concurrency

Components in distributed systems are executed in concurrent processes. Components access and update shared resources (e.g. variables, databases, device drivers).

2.6 Fault Tolerance

Hardware, software and networks fail. Distributed systems must maintain availability even at low levels of hardware/software/network reliability. Fault tolerance is achieved by recovery and redundancy.

2.7 Transparency

Distributed systems should be perceived by users and application programmers as a whole rather than as a collection of cooperating components. Transparency has different dimensions that were identified by ANSA. These represent various properties that distributed systems should have.

2.8 Load scalability

The ease with which a system or component can be modified, added or removed, to accommodate changing load.

2.9 Reliability

It is the ability of an item to perform a required function under stated conditions for a specific period of time.

2.10Redundancy

Several machines can provide the same services, so if one is unavailable, work does not stop. Additionally, because many smaller machines can be used, this redundancy does not need to be prohibitively expensive.

2.11Methods of communications

- message passing - send and receive primitives
- synchronous or asynchronous
- blocking or non-blocking
- mechanisms of message passing - channels, sockets, ports
- client-server communication model
- group multicast communication model

2.12Asset

Anything which has some value is termed as an asset. It is further explained as a resource with economic value that an individual, corporation or country owns or controls with the expectation that it will provide future benefit.

2.13Risk

Risk is the potential of losing something of value, weighed against the potential to gain something of value.

2.14Vulnerability

Vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

3. Software Assets and Vulnerabilities

Various Software Assets

Some software assets taken into consideration are

- IBM z/OS
- IBM AIX
- IBM DB2
- Microsoft sql server
- Oracle sun Solaris
- Linux
- Windows Server 2000/‘03/‘08
- Finacle Lite
- Microsoft Azure platform
- HP UX

3.1 IBM Z/OS

Vulnerability Details

- *CVE-2013-5385* : The OSPF implementation in IBM i 6.1 and 7.1, in z/OS on zSeries servers, and in Networking Operating System (aka NOS, formerly BLADE Operating System) does not properly validate Link State Advertisement (LSA) type 1 packets before performing operations on the LSA database, which allows remote attackers to cause a denial of service (routing disruption) or obtain sensitive packet information via a crafted LSA packet, a related issue to CVE-2013-0149.

3.2 IBM AIX

Vulnerability Details

- *CVE-2013-5419* : Multiple buffer overflows in (1) mkque and (2) mkquedev in bos.rte.printers in IBM AIX 6.1 and 7.1 allow local users to gain privileges by leveraging printq group membership.
- CVE-2012-4845 : The FTP client in IBM AIX 6.1 and 7.1, and VIOS 2.2.1.4-FP-25 SP-02, does not properly manage privileges in an RBAC environment, which allows attackers to bypass intended file-read restrictions by leveraging the setuid installation of the ftp executable file.

3.3 IBM DB2

Vulnerability details

- CVE-2013-6717 : The OLAP query engine in IBM DB2 and DB2 Connect 9.7 through FP9, 9.8 through FP5, 10.1 through FP3, and 10.5 through FP2, and the DB2 pureScale Feature 9.8 for Enterprise Server Edition, allows remote authenticated users to cause a denial of service (database outage and deactivation) via unspecified vectors.
- CVE-2013-4033 : IBM DB2 and DB2 Connect 9.7 through FP8, 9.8 through FP5, 10.1 through FP2, and 10.5 through FP1 allow remote authenticated users to execute DML statements by leveraging EXPLAIN authority.

3.4 Microsoft SQl Server

Vulnerability details

- CVE-2012-2552 : Cross-site scripting (XSS) vulnerability in the SQL Server Report Manager in Microsoft SQL Server 2000 Reporting Services SP2 and SQL Server 2005 SP4, 2008 SP2 and SP3, 2008 R2 SP1, and 2012 allows remote attackers to inject arbitrary web script or HTML via an unspecified parameter, aka "Reflected XSS Vulnerability."
- CVE-2012-1856 : The TabStrip ActiveX control in the Common Controls in MSCOMCTL.OCX in Microsoft Office 2003 SP3, Office 2003 Web Components SP3, Office 2007 SP2 and SP3, Office 2010 SP1, SQL Server 2000 SP4, SQL Server 2005 SP4, SQL Server 2008 SP2, SP3, R2, R2 SP1, and R2 SP2, Commerce Server 2002 SP4, Commerce Server 2007 SP2, Commerce Server 2009 Gold and R2, Host Integration Server 2004 SP1, Visual FoxPro 8.0 SP1, Visual FoxPro 9.0 SP2, and Visual Basic 6.0 Runtime allows remote attackers to execute arbitrary code via a crafted (1) document or (2) web page that triggers system-state corruption, aka "MSCOMCTL.OCX RCE Vulnerability."

3.5 Linux

Vulnerability details

- CVE-2013-6368 : The KVM subsystem in the Linux kernel through 3.12.5 allows local users to gain privileges or cause a denial of service (system crash) via a VAPIC synchronization operation involving a page-end address.
- CVE-2013-4854 : The RFC 5011 implementation in rdata.c in ISC BIND 9.7.x and 9.8.x before 9.8.5-P2, 9.8.6b1, 9.9.x before 9.9.3-P2, and 9.9.4b1, and DNSco BIND 9.9.3-S1 before 9.9.3-S1-P1 and 9.9.4-S1b1, allows remote attackers to cause a denial of service (assertion failure and named daemon exit) via a query with a malformed RDATA section that is not properly handled during construction of a log message, as exploited in the wild in July 2013.

3.6 Windows server 2008

Vulnerability details

- CVE-2013-6999 : The IsHandleEntrySecure function in win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2008 SP2 does not properly validate the tagPROCESSINFO pW32Job field, which allows local users to cause a denial of service (NULL pointer dereference and system crash) via a crafted NtUserValidateHandleSecure call for an owned object. NOTE: the vendor reportedly disputes the significance of this report, stating that "it appears to be a local DOS ... we don't consider it security vulnerability." CVSS score : 4.0
- CVE-2013-5058 : Integer overflow in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allow local users to gain privileges via a crafted application, aka "Win32k Integer Overflow Vulnerability." CVSS score : 4.9

3.7 Microsoft windows azure platform

Vulnerability details

- *CVE-2011-1068* : Microsoft Windows Azure Software Development Kit (SDK) 1.3.x before 1.3.20121.1237, when Full IIS and a Web Role are used with an ASP.NET application, does not properly support the use of cookies for maintaining state, which allows remote attackers to obtain potentially sensitive information by reading an encrypted cookie and performing unspecified other steps. CVSS score : 2.6

3.8 HP UX

Vulnerability details

- *CVE-2012-0126:* Unspecified vulnerability in the WBEM implementation in HP HP-UX 11.11 and 11.23 allows remote attackers to obtain access to diagnostic information via unknown vectors, a related issue to CVE-2012-0125. CVSS score : 5.8
- *CVE-2006-4188:* Unspecified vulnerability in the LP subsystem in HP-UX B.11.00, B.11.04, B.11.11, and B.11.23 allows remote attackers to cause a denial of service via unknown vectors. CVSS score : 5.0
- *CVE-2005-1192* : Unknown vulnerability in HP-UX B.11.00, B.11.04, B.11.11, B.11.22, and B.11.23, when running TCP/IP on IPv4, allows remote attackers to cause a denial of service via certain packets, related to the PMTU, a different vulnerability than CVE-2004-1060. CVSS score : 5.0

4. Hardware Assets

Various types of hardware assets:

- HP Unix Server(Superdome)
- Oracle / Sun Server
- Sybase Adaptive Server Enterprise
- SPARC Enterprise M Server
- Sun Fire 6800 Server
- Redhat Enterprise Linux

Vulnerabilities of hardware assets

4.1 HP Unix Servers(Superdome)

Unspecified vulnerability in the WBEM implementation in HP HP-UX 11.11 and 11.23 allows remote attackers to obtain access to diagnostic information via unknown vectors.

CVSS Scores and Vulnerability Types

CVSS Score	5.8
Confidentiality Impact	Partial(There is considerable Information disclosure.)
Integrity Impact	Partial(Modification of some System files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	None(There is no impact to the availability of the system.)
Access Complexity	ewhat specialized exploit.)
Authentication	Not required(Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type	Obtain Information
CWE ID	CWE id is not defined for this vulnerability

Unspecified vulnerability in the LP subsystem in HP-UX B.11.00, B.11.04, B.11.11, and B.11.23 allows remote attackers to cause a denial of service via unknown vectors.

CVSS Scores and Vulnerability Types

CVSS Score	5.0
Confidentiality Impact	None(There is no impact to the confidentiality of the system.)
Integrity Impact	None(There is no impact to the integrity of the system.)
Availability Impact	Partial(There is reduced Performance or interruptions in resource availability.)
Access Complexity	Low(Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required(Authentication is not required to exploit the vulnerability.)
Gained Access	None.
Vulnerability Type(s)	Denial of Service
CWE ID	CWE id is not defined for this vulnerability

Unknown vulnerability in BIND 9.2.0 in HP-UX B.11.00, B.11. -11, and B.11.23 allows remote attackers to cause a denial of service.

CVSS Scores and Vulnerability Types

CVSS Score	5.0
Confidentiality Impact	None(There is no impact to the confidentiality of the system.)
Integrity Impact	None(There is no impact to the integrity of the system.)
Availability Impact	Partial(There is reduced Performance or interruptions in resource availability.)
Access Complexity	Low(Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required(Authentication is not required to exploit the Vulnerability.
Gained Access	None
Vulnerability Type(s)	Denial of Service
CWE ID	CWE id is not defined for this vulnerability.

4.2 Oracle / Sun servers

Unspecified vulnerability in the Sun Storage Common (CAM) component in Oracle Sun Products Suite 6.9.0 allows remote attackers to affect confidentiality, related to Fault Management System (FMS).

CVSS Scores and Vulnerability Types

CVSS Score	5.0
Confidentiality Impact	Partial(There is considerable Informational disclosure.)
Integrity Impact	None(There is no impact to the integrity of the system.)
Availability Impact	None(There is no impact to the availability of the system.)
Access Complexity	Low(Specialized access Conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required(Authentication is not required to exploit the vulnerability.)
Gained Access	None
CWE ID	CWE id is not defined for this vulnerability.

4.3 Sybase Adaptive Server Enterprise

Unspecified vulnerability in SAP Sybase Adaptive Server Enterprise(ASE) 15.7 before 15.7 SP50 or 15.7 SP100 allows remote attackers to cause a denial of service via unspecified vectors.

CVSS Scores & Vulnerability Types

CVSS Score	7.1
Confidentiality Impact	None(There is no impact to the confidentiality of the system.)
Integrity Impact	None(There is no impact to the integrity of the system.)
Availability Impact	Complete(There is a total Shutdown of the affected resource. The attacker can render the resource completely unavailable.

Access Complexity	Medium(The access conditions are somewhat Specialized. Some preconditions must be satisfied to exploit.)
Authentication	Not required (Authentication is not required to exploit the Vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial of service
CWE ID	CWE id is not defined for this Vulnerability.

4.4 SPARC Enterprise MServer

Unspecified vulnerability in the SPARC Enterprise M Series Servers component in Oracle and Sun Systems Products Suite XCP 1114 and earlier allows remote attackers to affect availability via related to XSCF Control Package (XCP).

CVSS Scores and Vulnerability Types

CVSS Score	5.0
Confidentiality Impact	None(There is no impact to the Confidentiality of the system.)
Integrity Impact	None(There is no impact to the Integrity of the system.)
Availability Impact	Partial(There is reduced performance or interruptions in resource availability.)
Access Complexity	Low(Specialized access Conditions or extenuating circumstances do not exist. Very little Knowledge or skill is required to exploit.)
Authentication	Not required(Authentication is not required to exploit the Vulnerability.)
Gained Access	None
CWE ID	CWE id not defined for this vulnerability.

Unspecified vulnerability in Oracle SPARC Enterprise M Series Servers XCP 1110 and earlier allows local users to affect confidentiality, related to XSCF Control Package (XCP).

CVSS Scores and Vulnerability Types

CVSS Score	2.1
Confidentiality Impact	Partial(There isconsiderable informational disclosure.)
Integrity Impact	None(There is no impact to the integrity of the system.)
Availability Impact	None(There is no impact to the availability of the system.)
Access Complexity	Low(Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required(Authentication is not required to exploit the vulnerability.)
CWE ID	CWE id is not defined for this Vulnerability.

4.5 Redhat Enterprise Linux

mod_nss1.0.8 and earlier, when NSSVerifyClient is set to none for the server / vhost context, does not enforce the NSSVerifyClient setting in the directory context, which allows remote attackers to bypass intended access restrictions.

CVSS Scores and Vulnerability Types

CVSS Score	4.0
Confidentiality Impact	Partial(There is considerable Informational disclosure.)
Integrity Impact	Partial(Modification of some System files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	None(There is no impact to

	the Availability of the system.)
Access Complexity	High(Specialized access Conditions exist. It is hard to exploit and several special conditions must be satisfied to exploit.)
Authentication	Not required(Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type	Bypass a restriction or similar
CWE ID	264

389 Directory Server 1.2.11.15(aka Red Hat Directory Server before 8.2.11-14) allows remote authenticated users to cause a denial of service(crash) via multiple @ characters in a GER attribute list in a search request.

CVSS Scores and Vulnerability Types

CVSS Score	4.0
Confidentiality Impact	None(There is no impact to the confidentiality of the system.)
Integrity Impact	None(There is no impact to the integrity of the system.)
Availability Impact	Partial(There is reduced Performance or interruptions In resource availability.)
Access Complexity	Low(Specialized access Conditions or extenuating circumstances do not exist. Very Little knowledge or skill is required to exploit.)
Gained Access	None
Vulnerability Type	Denial Of Service
CWE ID	20

5. Qualitative and Quantitative Methodology

Qualitative analysis deals with collecting, analyzing, and interpreting data by observing what people do and say. It refers to the meanings, concepts, definitions, characteristics, metaphors, symbols, and descriptions of things. It is subjective in nature, and methods of collecting information, mainly individual, in-depth interviews and focus groups. It is an exploration of what is assumed to be a dynamic reality. It does not claim that what is discovered in the process is universal, and thus, replicable. The results are interpretive.

Quantitative analysis refers to counts and measures of things. It is objective in nature. It seeks explanatory laws and aims at in-depth description. The results are measurable.

The hybrid of these two methods is obtained by combining the subjectivity and the objectivity concepts. The entropy theory used in order to calculate the weight vectors of the risk factors such as risk probability, impact severity and uncontrollability combines the subjectivity with objectivity and thus provides a hybrid methodology for risk assessment of information security.

6. Risk Assessment Methodologies

6.1 Octave

6.1.1 Description

OCTAVE is an asset-driven evaluation approach. OCTAVE requires the analysis team to consider the relationships among critical assets, the threats to those assets, and vulnerabilities (both organizational and technological) that can expose assets to threats. It identifies information-related assets (e.g., information and systems) that are important to the organization and focus risk analysis activities on those assets judged to be most critical to the organization (focus on the few critical assets, no more than five). OCTAVE is mainly a self-directed information security risk evaluation. This core concept of OCTAVE is defined as a situation where people from an organization manage and direct an information security risk evaluation for their organization. There are different OCTAVE methods based on OCTAVE Criteria. OCTAVE, OCTAVE-S and OCTAVE Allegro.

6.1.2 Target Organizations

- OCTAVE Method - large organizations
- OCTAVE-S - small and medium organizations (manufacturing companies with 100 people or less)
- OCTAVE Allegro – All organizations

6.1.3 Approach

The OCTAVE method currently has three different approaches (OCTAVE, OCTAVE-S and OCTAVE Allegro). Since all approaches are based on the same framework, only one of them was considered for this study. The one chosen was OCTAVE Allegro, the more recent of the approaches. This approach differs from previous OCTAVE approaches by focusing primarily on information assets in the context of how they are used, where they are stored, transported, and processed, and how they are exposed to threats, vulnerabilities, and disruptions as a result. Like previous methods, OCTAVE Allegro can be performed in a workshop-style, collaborative setting and is supported with guidance, worksheets, and questionnaires, which are included in the model. However, OCTAVE Allegro is also well suited for use by individuals who want to perform risk assessment without extensive organizational involvement, expertise, or input.

6.2 *IRAM*

6.2.1 Description

IRAM is the ISF's information risk analysis methodology. Structured and rigorous yet practical, flexible and above-all easy-to-use, IRAM has been developed to meet the demanding needs of information risk analysts in modern risk oriented organizations. It helps to determine the criticality / importance of information systems by conducting a full risk analysis on those systems.

6.2.2 Target Organizations: All

6.2.3 Approach: IRAM, the ISF's next generation information risk analysis approach, has three main components-

- Business Impact Assessment
- Threat and Vulnerability Assessment
- Control Selection.

7. CONCLUSION

Risk Assessment plays an important role in providing information security. Banking sector is one of the main applications of distributed systems. Various assets and vulnerabilities involved in distributed banking application are identified. Risk assessment methodologies and tools employed also plays an important role in assessing risk in information security.

References

[1] http://www.cs.ucl.ac.uk/staff/ucacwxe/lectures/ds98-99/dsee3.pdf

[2] http://www.csc.villanova.edu/~schragge/CSC8530/Intro. html

[3] http://www.icoe.org/webfm_send/1936

[4] http://secunia.com/advisories/21499

[5] http://securitytracker.com/alerts/2006/Aug/1016698. html

[6] http://www.frsirt.com/english/advisories/2006/3291

[7] http://www.securityfocus.com/bid/19535

[8] http://www2.itrc.hp.com/service/cki/docDisplay.do?docId=c00746980

[9] http://marc.theaimsgroup.com/?l=bugtraq&m=11080510520047&w=2

[10] http://xforce.iss.net/xforce/xfdb/19276

[11] http://www.oracle.com/technetwork/topics/security/cpujan2013-1515902.html

[12] http://www.mandriva.com/security/advisories?name=MDVSA-2013:150

[13] http://secunia.com/advisories/55537

[14] http://www.sybase.com/detail?id=1099371

[15] http://osvdb.org/95311

[16] http://www.securityfocus.com/bid/61247

[17] http://xforce.iss.net/xforce/xfdb/85698

[18] http://www.securityfocus.com/bid/53134

[19] http://rhn.redhat.com/errata/RHSA-2013-1779. html

[20] http://lists.opensuse.org/opensuse-updates/2013-12/msg00118.html

[21] http://rhn.redhat.com/errata/RHSA-2013-1752.html

[22] http://rhn.redhat.com/errata/RHSA-2013-1753.html

[23] http://www.cvedetails.com/product/16924/IBM-Z-os.html?vendor_id=14

[24] http://www.cvedetails.com/vulnerability-ist/vendor_id-14/product_id-17/cvssscoremin-6/cvssscoremax-6.99/IBM-AIX.html