Risk Assessment & Mitigation for Interactive Voice Response System

Author

[1]Sanjay Kumar, [2]Ramavati Savitri, [3]Dr. Vinayak Ayatye

[1,2](Researcher/Department of Computer Science/Malla Reddy Engineering College, Hyderabad, India)
[3](Professor/ Department of Computer Science/Malla Reddy Engineering College, Hyderabad, India)

Abstract

In the present era of information technology, information nowadays is just a telephone call away. However, applications such as telephone banking etc. need extra security for making it a reliable service for the people. In this paper we have identified vulnerabilities and risks related to IVR (Interactive Voice Response) their likelihood and impact on the given organization. We also tried to suggest few control methods in order to reduce vulnerabilities and risks.

Introduction

Interactive voice response (IVR) systems allow people to interact with computers in an automated fashion, through voice or touch-tone phones. Often, these systems process confidential data such as credit card numbers, social security numbers, user PIN information, and other personally identifiable information (PII). IVR assessment helps organizations to secure their IVR systems and identify security holes before attackers can gain access.IVR systems are typically used for telephone banking, credit card services, hospitals, call centers and into automobile systems for hands-free operation. Most of the time, IVR systems are conveniently left out of regular security testing and internal audits.

Risk and Vulnerabilities Assessment for Interactive Voice Response system In order to do the risk and vulnerability assessment, the most vital task is to identify critical assets, risk, vulnerabilities and threats related to IVR system mainly voice recognition.

Risk is probability of losing valuable asset. Vulnerability is system's weakness which allows an attacker to reduce a system's information assurance.

Some Vulnerabilities for Interactive Voice Response based on our findings are:

1. Improper System Configuration – This vulnerability appears when there is mismatch between actual system configuration which is needed and which is being used, for e.g.- there is requirement of Windows + MySQL and the configuration which is being used is Windows + SQLServer.

2. Improper results due to different Platforms – The Given IVR product should function exactly same irrespective of platforms used, e.g. whether deployed on Linux or Windows, it should give same result.

3. Loss of pre-existing functionality – In case if any new functionality is added, there should not be loss of pre-existing functionality.

4. Use of Improper Voice Recognition Engine – Proper Voice Recognition Engines should be used. Faulty Voice Recognition Engine can cause system crash.

5. Version mismatch between Voice Recognition Engine and Voice packs – There should be proper compatibility between voice recognition engine and voice packs.

6. Generation of Personal Information in log file – Appearance of personal information such as credit card information in generated log file. Based on above vulnerabilities, following risk assessment has been done.

Table 1: Vulnerability, Threat & Risk Summary for Interactive Voice Response (IVR) system

No.	Vulnerability	Threat	Risk Summary
1	Improper system configuration	Denial of Service.	Loss of Availability
2	. Platform dependency	. variation in output	. Improper result
3	Loss of pre-existing functionality due to enhancement	Functionality Manipulation	Loss of Availability & Improper result
4	Improper Voice Recognition Engine	system crash	Loss of Availability
5	Mismatch between Voice Recognition Engine &Voice Packs versions	System cannot recognize particular voice packs	Improper or no result
6	Generation of personal information in log files	information theft	Confidentiality Loss

Table 2: Some other Vulnerability based on findings through various sources:

No.	Vulnerability	Threat	Risk Summary
1	Improper use of Telephone system (Hossein Bidgoli, 2006)	Malicious use by unauthorized person.	customers data loss
2	Poorly written apps (Hossein Bidgoli, 2006)	Unauthorized access of Confidential data	data loss
3	Spy ware (Thorsten Holz, Herbert Bos,2011)	Unauthorized access.	Data loss
4	Vendor back doors (Hossein Bidgoli, 2006)	Un authorized access	Data loss
5	Systems not monitored (Hossein Bidgoli, 2006)	Unauthorized access	Data Loss
6	Stolen credentials (Thorsten Holz, Herbert Bos,2011)	Unauthorized access	Compromises confidentiality
7	Poor disaster recovery (Hossein Bidgoli, 2006)	Effect on IT infrastructure/data.	Data loss
8	Poor password protection (Thorsten Holz, Herbert Bos,2011)	Poor authorization.	Compromises confidentiality
9	Software bugs (Thorsten Holz, Herbert Bos,2011)	Unauthorized access	Data loss
10	Ineffective controls (Thorsten Holz, Herbert Bos,2011)	Unauthorized access	Integrity loss
11	Calling cards (Hossein Bidgoli, 2006)	Prepaid/preregistered account. Effect on User credentials	Hackers can easily break password
12	Voice mail system (Thorsten Holz, HerbertBos,2011)	Mail Server access. Poor User credentials	hackers might enter into a system
13	Spoofing Attack (Hossein Bidgoli, 2006)	unauthorized access	Financial loss
14	Unnecessary protocols (Thorsten Holz, Herbert Bos,2011)	Unauthorized access	Unauthorized use of systems

Based on Vulnerabilities, risk summary we are suggesting some mitigation controls in table 3.
Table 3: Risk Summary, Risk Impact Rating and Mitigation Controls

Vulnerability	Risk Summary	Impact Rating	Mitigation Techniques
Improper system Configuration	Loss of Availability and Integrity	High	Proper Checks & validation points at the time of development
Platform Dependency	Loss of Confidentiality	High	Telephone system to be provided to authorized person only
Loss of pre-existing functionality due to	Loss of important customers data	Moderate	Daily Backup system is required
Improper Voice Recognition Engine	Damage important data	High	Proper User access control is required
Mismatch between Voice Recognition Engine &Voice Packs versions	Unauthorized access	Moderate	Proper User access control is required
Generation of personal information in log files	Compromises confidentiality	Moderate	User id, Account Number and password should be confidential
Calling cards	Hackers can easily break password		Strong password
Voice mail system	Due to poor credentials, hackers might be easily enter into a system	High	Proper User access control is require
Loss of pre-existing functionality in case of enhancement	Financial loss and loss of important customers data	High	Particular software policy should be implemented

Conclusion:

In the present era of digitization and such a large scale use of Technology, it is possible that there may be human and system interaction at each and every step using Voice Recognition Methodology. As far as security is concerned, no such systems can be entirely free from the risk of unauthorized use. However, diligent attention to system management and to security can reduce that risk considerably. In this paper we identified vulnerabilities and did risk assessment. Here we also tried to mitigate those risks by providing some control techniques.

References

[1]. Avaya Inc™ (2003): Avaya Interactive Voice Response Security.

[2]. Dr. Ida Androwich, Dr. Margaret Ross Kraft: Use of Interactive voice response technology in Health Care from Loyola University Chicago.

[3]. Hossein Bidgoli: Handbook of Information Security, Threats, Vulnerabilities, Prevention.

[4]. Pillai's Institute of Information Technology: Interactive Voice Response system for Educational Institution, E-ISSN 0976-3945.School of computer engineering: Vulnerability evaluation of speaker verification under voice conversion spoofing: the effect of text constraints, Temasek Laboratories@NTU from Singapore.

[5]. Thorsten Holz, Herbert Bos: Detection of Intrusions and Malware, and Vulnerability Assessment- 8th edition.