ISSN NO. 2320-5407

Journal homepage:http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Risk Assessment & Mitigation for Interactive Voice Response System

Kumari Ankita, Mohini Mehta, Dr. Priti Puri
Symbiosis Centre for Information Technology, Hinjewadi, Phase-1Pune – 411057, Maharashtra, India

Manuscript Info

Manuscript History:

Received: 22 May 2015
Final Accepted: 25 July 2015
Published Online: August 2015

Key words:

Risk, Vulnerability, IVR, Threat, Security, Confidentiality

Corresponding Author
Kumari Ankita

Abstract

In the today's computer world, information is just a telephone call away. In this paper, we have tried to identify vulnerabilities, risks, their corresponding likelihood related to Interactive Voice Response (IVR) and their impact on the given organization. We also tried to suggest few control methods in order to mitigate those risks.

INTRODUCTION

Interactive voice response (IVR) systems are the systems by which people may link with computer databases in an robotic manner, via voice or touch-tone phones. These IVR systems handles confidential data such as credit card numbers, user PIN information, and other personally identifiable information (PII). In order to do the risk and vulnerability assessment, the most important task is to identify critical assets, risk, vulnerabilities and threats related to IVR system especially for voice recognition.Vulnerability of any system is the weakness/flaw in that particular system,and threat is exploitation of that vulnerability by threat source. At the same time,risk is the probability of occurring that threat and impact is the loss happened by that incident to the organization.

Risks &Vulnerabilities Assessment for Interactive Voice Response system

We have considered the Risk assessment Matrix given by NIST 800-30. Some initial Vulnerabilities for IVR based on our findings and some others are from literature, also mentioned in the table. We have also tried to provide some mitigation controls for all the vulnerabilities mentioned. Impact rating is given-High-h, Moderate-M and Low-L

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

Vulnerability	Threat	Risk Summary	Impact Rating	Mitigation Techniques
Improper system configuration e.g.- if the requirement of Windows+MySQL & configurationused is Windows+SQLServer.	Denial of Service.	Loss of Availability	H	Proper Checks & validation points at the time of development, senior technical team also check the system requirements
Platform dependency,	variation in	Loss of	H	IVR system should be platform independent

e.g. whether deployed on Linux or Windows, they are not giving same result.	output	Confidentiality		Proper Checking and matching the platforms then start operating
Loss of pre-existing functionality due to enhancement	Functionality Manipulation	Loss of important customers data	M	Agile approach should be considered for future additional functions
Improper Voice Recognition Engine	system crash	Damage important data	H	Proper audits, inspections and periodic checking for engines
Mismatch between Voice Recognition Engine &Voice Packs versions	System cannot recognize particular voice packs	Improper functioning	M	Proper employee training, compatibility check for voice recognition engine & voice pack versions
Generation of personal information in log files(credit cards,PII)	information theft	Compromises integrity & confidentiality	M	User id, Account Number and password should be confidential, use encryption mechanism to encrypt data in logs. Proper log monitoring and backup is required

Telephone related vulnerability (Hossein Bidgoli, 2006)	Malicious use by unauthorized user	customers data loss	M	Proper employee training should be given
Session Initiation Protocol (SIP) system is vulnerable to general IP and VoIP attack(Mark Collier ,2005)	Unauthorized access	Confidentiality loss/data theft	H	24/7 monitoring should be done and logs should be maintained . Use SIP optimized firewalls, which help to use the standards-based security and provide the best possible protection. (Mark Collier ,2005)
Stolen credentials (Thorsten Holz, Herbert Bos,2011)	Unauthorized access	Compromises confidentiality	M	Proper information should be send to corresponding department to stop that credentials used, allow new credentials, proper training to employees
Poor disaster recovery (Avaya Inc™,2003)	Unavailability of IT infrastructure/data.	Data loss/business loss	H	Proper Disaster recovery planning and Business continuity planning should be there
Weak password protection (Thorsten Holz, Herbert Bos,2011)1	Poor authorization	Compromises confidentiality	H	Proper training to employees, strong password policies ,alphanumeric ,special characters should be mandatory ,password renewal after regular time interval should be done
Ineffective access controls (Thorsten Holz, Herbert Bos,2011)5	Unauthorized access	Integrity loss , loss of confidentiality	M	Role based access control, biometric should be for employees
Improper handling of Calling cards(Hossein Bidgoli, 2006)	Hackers can easily break password	loss of confidentiality	H	Strong password, proper employee training, audits
Improper Voice mail system Thorsten Holz, Herbert Bos(2011)	hackers might enter into a system	Due to poor credentials, hackers might be easily enter into a system, confidentiality loss	H	Proper User access control, role based access control

man-in-the-middle telephone attacks, "Voice phishing or vishing (Ruishan Zhang , Xinyuan Wang , Ryan Farley , Xiaohui Yang , Xuxian Jiang ,2009)	unauthorized access	Financial loss and loss of important customers data	H	Customer database should be maintained and Sound verification of authentic customer should be done. Data should be stored encrypted wherever possible to avoid Man in the middle attack
Sensitive Information Disclosure issues such as Internal IP Revealed (Foundstone,2014-2015)	Internal unaware or frustated employees	Confidentiality loss, availability loss	M	Internal IP should be used by role based approach, only authentic and authorized people should allow to use and monitoring is required, audits & validations, employee trainings
Source code disclosure (Foundstone,2014-2015)	Unauthorized access	Integrity loss	H	Encrypted and secure source code implementation is required
Application Logic Bypass vulnerabilities (Foundstone,2014-2015)	accidentally done by unaware employee	Improper results	M	Checkpoints at various position in application, proper validation and employee awareness
Input Validation vulnerabilities (Foundstone,2014-2015)	Misused by hacker Unauthorized access	unavailability	M	Proper input validations,24/7 monitoring of logs
Brute Force attacks (Foundstone,2014-2015)	Misused by hacker Unauthorized access	unavailability	M	Network monitoring 24/7,latest firewalls in place ,logs maintenance
DOS attack s (Foundstone,2014-2015)	Done by hacker	unavailability	M	Backup pocilies,24/7 monitoring of logs and proper logs maintenance

Conclusion:

In the present era of information technology, it can be possible that 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, it is possible that by diligent attention to system management and to security can reduce that risk considerably. In this paper we have tried to find out some vulnerabilities and provide risk assessment. Here we have also tried to mitigate those risks by providing some control techniques.

References:

Avaya Inc™ (2003): Avaya Interactive Voice Response Security.
Hossein Bidgoli(2006): Handbook of Information Security, Threats, Vulnerabilities, Prevention.
Ruishan Zhang , Xinyuan Wang , Ryan Farley , Xiaohui Yang , Xuxian Jiang (2009):On the Feasibility of Launching the Man-In-The-Middle Attacks on VoIP from Remote Attackers
David Persky (2007): SANS Institute InfoSec Reading Room- VoIP Security Vulnerabilities
Mark Collier (2005): Basic Vulnerability Issues for SIP Security
Foundstone, A Division of McAf ee (2014-2015)Interactive Voice Response (IVR) Assessment