SecureAgent: Security Evaluation Expert System

Contents

Palak Sharma (ps2671@g.rit.edu)
Rochester Institute of Technology, NY, USA

1. Executive Summary

Importance of having a high quality security framework for Information systems is already given top most priority. However, assessing security standards for these crucial information resources is a demanding task, which becomes even more cumbersome at higher organizational levels. In order to make the task of security assessment accessible at stakeholder's end, this project proposes "SecureAgent – A rule based expert system for security evaluation." This application makes use of a rule based expert system which is exposed to the users through a web based and android based graphical user interface. The knowledge base for the security assessment is acquired from "Performance Measurement Guide for Information Security", by National Institute of Standards and Technology [1].

SecureAgent has a console based, a web based and an android based interface. Hence, exposing it to a large user base. The console based and web based applications are equipped with JESS [2] rule engine for knowledge base processing. The web application is responsive, i.e. the web application can be viewed on a tablet or a mobile. Along with this, the project offers two android based expert system application which differ in their rule base implementation. (a) First android application utilities rule implemented in java, whereas (b) Second android application utilizes e2gDroid lite [3] as expert system shell for the rule base implementation. The android application has the advantage of working in remote locations with no internet access as the application allows the rule base to be stored in a file in phone memory.

In a broad sense, Impact, Efficiency and Implementation are the three measures taken into account for this application. Based on the user response for the security assessment questions, SecureAgent provides the security evaluation result in terms of percentage along with the recommendations to improve the current security level.

2. Requirements Specification

Currently the SecureAgent application supports security evaluation in terms of Impact, Efficiency and Implementation. However, the hierarchical design of the application, makes its scalable to support other security measures in future. The security measures are acquired from "Performance Measurement Guide for Information Security", by National Institute of Standards and Technology [1]. The purpose of this guide is to provide measures for assessment of security policies and procedures at organizational level. This document consists of 19 metrics but the scope of SecureAgent is limited to 5 metrics (41 rules) for web based and console based application and 3 metrics (14 rules) for android based application.

2.1.1 Requirements for Console and Web-based Application

The following metrics are taken from [1] and the description for these metrics are rephrased.

Measure Type - Impact

- Metric 1: Security Budget – The output of this metric is expressed in terms of the percentage of the budget allocated to security resources to the total amount dedicated to information system resources.

Measure Type - Efficiency

- Metric 2: Vulnerability Management – Expressed in terms of the total information system vulnerabilities alienated to the total reported vulnerabilities during that time frame.
- Metric 3: Access Control (AC) – Based on the user inputs, whether the organization makes use of automated tools for intrusion detection, remote access illegal access and recording audit logs, this metric calculates the ratio of the illegal access points details to the total number of access points in the system.

Measure Type - Implementation

- Metric 4: Personnel Security (PS) – To ensure security of information resources, this metric is calculated by identifying the verified users to the total number of users.
- Metric 5: System and Services Acquisition (SA) – In order to verify that all the security requirements are fulfilled in case of accessing third party services, this metric is called as a percentage to the number of fulfilled cases to the total number of cases.

2.1.2 Requirements for Android Applications

The two android based applications use the following metrics from [1]:

Measure Type - Impact

- Metric 1: Security Budget – The output of this metric is expressed in terms of the percentage of the budget allocated to security resources to the total amount dedicated to information system resources.

Measure Type - Efficiency

- Metric 3: Access Control (AC) – This metric calculates the ratio of the illegal access points details to the total number of access points in the system.

Measure Type - Implementation

- Metric 4: Personnel Security (PS) – Based on user inputs for the password protection and software update policies, this metric calculates the total systems equipped with security policies to the total number of system in the organization.

3. Methodology

SecureAgent expert system is developed in 5 phases which are described in the following sub sections.

3.1.1 Phase 1: Problem Description and Analysis

The problem addressed in SecureAgent is security evaluation at organizational level from stakeholder point of view. The Graphical User interface of the system asks the end user for responses by asking simple questions. Such system is particularly useful for high level stakeholders who are responsible for security of information resources for multiple projects under same organization.

3.1.2 Phase II: Knowledge Base acquisition

Based on [1], the problem scope of this project is security evaluation at organizational level and the project infrastructure is designed by the knowledge gained from literature survey on [4,5,6,7,8]. On thorough analysis of 19 security metrics specified in [1], the problem set for SecureAgent is obtained, which consist of 5 metrics. The design of the system is hierarchical allowing features scalability [4,5,8] and the development framework is inspired from [7]. The knowledge base acquired from [1], is then converted into JESS rules (for console and web application), JAVA rules (for first android application) and e2gDroid rules (for second android application).

3.1.3 Phase III: Rules Design & Implementation

As per the description and formula's provided in [1], the rules for different security metrics are formulated.

- **For Console and Web Based Application**

The rules depicted in Table 1 are taken into account and converted to JESS rules [2] to be executed in JESS expert system shell. Refer to Appendix 1.0 for JESS Rules.

SNo.	Security Metrics	Rules	Evaluation Result
1	Security Budget Impact	If the user enters security budget greater than total information technology budget.	Cannot generate evaluation result. (Security Budget cannot be greater than total information technology budget.)
2	Security Budget Impact	Security Impact Budget Percentage > 90	Good
3	Security Budget Impact	Security Impact Budget Percentage <= 90 and Security Impact Budget Percentage > 75	Medium
4	Security Budget Impact	Security Impact Budget Percentage <=75	Bad
5	Vulnerability Efficiency	If the user enters mitigated vulnerabilities are greater than identified vulnerabilities.	Cannot generate evaluation result. (Mitigated vulnerabilities cannot be greater than identified vulnerabilities.
6	Vulnerability Efficiency	Vulnerability Efficiency Percentage >90	Good
7	Vulnerability Efficiency	Vulnerability Efficiency Percentage <= 90 and Vulnerability Efficiency Percentage > 75	Medium
8	Vulnerability Efficiency	Vulnerability Efficiency Percentage <= 75	Bad
9	Access Control Efficiency*	It the user enters unauthorized access points greater than total access points.	Cannot generate evaluation results. (Unauthorized access points cannot be greater than remote access points.)

10	Access Control Efficiency*	Access Control Efficiency Percentage < 5	Good
11	Access Control Efficiency*	Access Control Efficiency Percentage < 10 and Access Control Efficiency Percentage >= 5	Medium
12	Access Control Efficiency*	Access Control Efficiency Percentage >=10	Bad
13	Personnel Security Implementation	If the user enters the screened personnel details greater than the total personnel detail.	Cannot generate evaluation result. (Number of authorized personnel cannot be less than screened personnel.)
14	Personnel Security Implementation	Personnel Security Implementation Percentage > 90	Good
15	Personnel Security Implementation	Personnel Security Implementation Percentage <= 90 and Personnel Security Implementation Percentage > 75	Medium
16	Personnel Security Implementation	Personnel Security Implementation Percentage <= 75	Bad
17	System and Services Acquisition Implementation	If the user enters the total service acquisition contracts with security specification greater than total service contracts.	Cannot generate evaluation result. (Total number of service acquisition contracts cannot be less than acquisition contracts with security specification.)
18	System and Services Acquisition Implementation	System and Services Acquisition Implementation Percentage > 90	Good
19	System and Services Acquisition Implementation	System and Services Acquisition Implementation Percentage <= 90 and System and Services Acquisition Implementation Percentage > 75	Medium
20	System and Services Acquisition Implementation	System and Services Acquisition Implementation Percentage <= 75	Bad
21	Overall Security	Overall Security Percentage > 90	Very Good
22	Overall Security	Overall Security Percentage <= 90 and Overall Security Percentage >75	Good
23	Overall Security	Overall Security Percentage <= 75 and Overall Security Percentage > 50	Medium
24	Overall Security	Overall Security Percentage <= 50	Bad

Table 1: Rules for Security Evaluation

Access Control Efficiency - The metric involves inferencing other rule based on user selection of automated rules. Please refer to the JESS rules in appendix 1 for further details.*

- **For Android Applications**

The rules depicted in Table 2 are taken into account and converted to JAVA rules for first android application and e2gDroid Rules [3] to be executed in e2gDroid expert system shell. Refer to Appendix 2.1 and 2.2 for the rules.

SNo.	Security Metrics	Rules	Evaluation Result
1	Security Budget Impact	If the user enters security budget greater than total information technology budget.	Cannot generate evaluation result. (Security Budget cannot be greater than total information technology budget.)
2	Security Budget Impact	Security Impact Budget Percentage > 90	Good
3	Security Budget Impact	Security Impact Budget Percentage <= 90 and Security Impact Budget Percentage > 75	Medium
4	Security Budget Impact	Security Impact Budget Percentage <=75	Bad
5	Vulnerability Efficiency**	If the user enters mitigated vulnerabilities are greater than identified vulnerabilities.	Cannot generate evaluation result. (Mitigated vulnerabilities cannot be greater than identified vulnerabilities.
6	Vulnerability Efficiency**	Vulnerability Efficiency Percentage >90	Good
7	Vulnerability Efficiency**	Vulnerability Efficiency Percentage <= 90 and Vulnerability Efficiency Percentage > 75	Medium
8	Vulnerability Efficiency**	Vulnerability Efficiency Percentage <= 75	Bad
9	Access Control Efficiency***	It the user enters unauthorized access points greater than total access points.	Cannot generate evaluation results. (Unauthorized access points cannot be greater than remote access points.)
10	Access Control Efficiency***	Access Control Efficiency Percentage < 5	Good
11	Access Control Efficiency***	Access Control Efficiency Percentage < 10 and Access Control Efficiency Percentage >= 5	Medium
12	Access Control Efficiency***	Access Control Efficiency Percentage >=10	Bad
13	Personnel Security Implementation*	If the user enters the number of systems with equipped policies greater than the total systems.	Cannot Determine. Please enter valid values in the above form.
14	Personnel Security Implementation*	Personnel Security Implementation Percentage > 90	Good

15	Personnel Security Implementation*	Personnel Security Implementation Percentage <= 90 and Personnel Security Implementation Percentage > 75	Medium
16	Personnel Security Implementation*	Personnel Security Implementation Percentage <= 75	Bad

Table 2: Rules for Security Evaluation for Android

Personnel Security Implementation - The metric involves inferencing other rule based on user selection of user use of security practices. Please refer to the rules in appendix 2.1 and 2.2 for further details.*

*Vulnerability Efficiency** - Only applicable for first android application with Java Rules.*

*Access Control Efficiency*** - Only applicable for second android application with e2gDroid Rules.*

3.1.4 Phase IV: Expert System Development & Implementation Phase

In all, 4 projects are created. Java based projects are based on JESS rule base whereas the two android applications use Java and e2gDroid based rules respectively. A brief description of JESS and e2gDroid shell is given below.

1) Project 1: SecureAgent - Console Based Expert System
2) Project 2: SecureAgent - Web Based Expert System
3) Project 3: SecureAgent - Android Expert System with Java Rule base.
4) Project 4: SecureAgent - Android Based Expert System with e2gDroid Rule base.

JESS (Java Expert System Shell)

JESS was developed by Ernest Friedman-Hill of Sandia National Labs [1]. It utilizes RETE algorithm for rule processing. The rule base is converted to JESS rules by the developer and the JESS inference engine uses RETE algorithm [9] to process the rules. The inference engine matches the facts with the rules available in the rule base and accordingly produces output. Jess Developer's Environment (JessDE) is available as a plugin for Eclipse Juno IDE. The latest JESS version is 7, which is used in this project. However, a current limitation of JESS 7.0 is that it is not supported in android application. This feature is implemented in JESS 8.0 which is available only for license users.

E2GDroid Lite expert system shell

It is a knowledge base compatible expert system shell that runs on Android devices [3]. Knowledge base is converted to e2gDroid compatible rules by developer using e2gRuleEngine applet. Knowledge bases can either be downloaded from internet or can be stored as text file on phone memory. The rules are processed in sequential order by using backward chaining mechanism. The e2gDroid Lite application provides features such as “Why” and “Explain” which equips the application with reasoning capabilities. Another useful feature of e2gDroid Lite is that the user interface creation for android is simple and thus the developer only has to concentrate on the rule implementation part.

Tools and Technologies

SNo.	Application Type	Rule Base Implementation	Development Environment	Development Editor	User Interface Technologies	Backend Code Technologies
1	Console Based Expert System	JESS Rules (JESS 7.0)	JDK 1.8	Eclipse Juno	N/A	Core JAVA
2	Web Based Expert System	JESS Rules (JESS 7.0)	JDK 1.8 TOMCAT 7.0	Eclipse Juno	Responsive web application based on Angular js and Bootstrap	JAVA EE - Servlet
3	First Android Application	JAVA/JavaScript	Android SDK 23	Android Studio 2.1.2	Android application using web view component.	N/A
4	Second Android Application	E2gDroid Rules	e2gDroid Lite 1.9	Notepad ++	User interface as provided by e2gDroid application.	N/A

External Libraries Used

1) Project 1 and Project 2: SecureAgent – Console & Web Based Expert System

SNo.	Library Name	Download Link
1	gson-2.2.2.jar	https://mvnrepository.com/artifact/com.google.code.gson/gson/2.2.2
2	java-json-schema.jar	https://mvnrepository.com/artifact/com.github.fge/json-schema-validator/2.1.7
3	jess.jar	http://www.jessrules.com/jess/download.shtml
4	servlet-api.jar	https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api/3.1.0

3.1.5 Phase V: Testing

All the below mentioned test cases are executed on windows machine with following specification:

SNo.	Device Name	Operating System	Processor	RAM
1	ASUS X555LAB	Windows 10 (64 bit)	Intel Core i7	8 GB

1. **Project 1 and Project 2: SecureAgent – Console & Web Based Expert System**

Testing Environment Specification:

SNo.	Browser Name	Version	Observations
1	Google Chrome	51.0	Application works as desired.
2	Mozilla Firefox	42.0	Functionality works as desired. one angular js error display validation is not supported.
3	Internet Explorer	11.4	Functionality works as desired. one angular js error display validation is not supported.

Manual testing with different set of inputs for the questions on the user interface. The system response was the evaluation result in percentage, graded as good/medium/bad along with the recommendations. Refer to section 4 for user interface details.

2. **Project 3: SecureAgent - Android Expert System with Java Rule base.**

Testing Environment Specification:

SNo.	Type	Name	API	Target
1	Emulator	Nexus 5X	19	Android 4.4
2	Device	Samsung A3	21	Android 5.0.2

Manual tested the android application on the emulator and the Samsung A3 device. The application works perfectly with all the validations.

3. **Project 4: SecureAgent - Android Based Expert System with e2gDroid Rule base.**

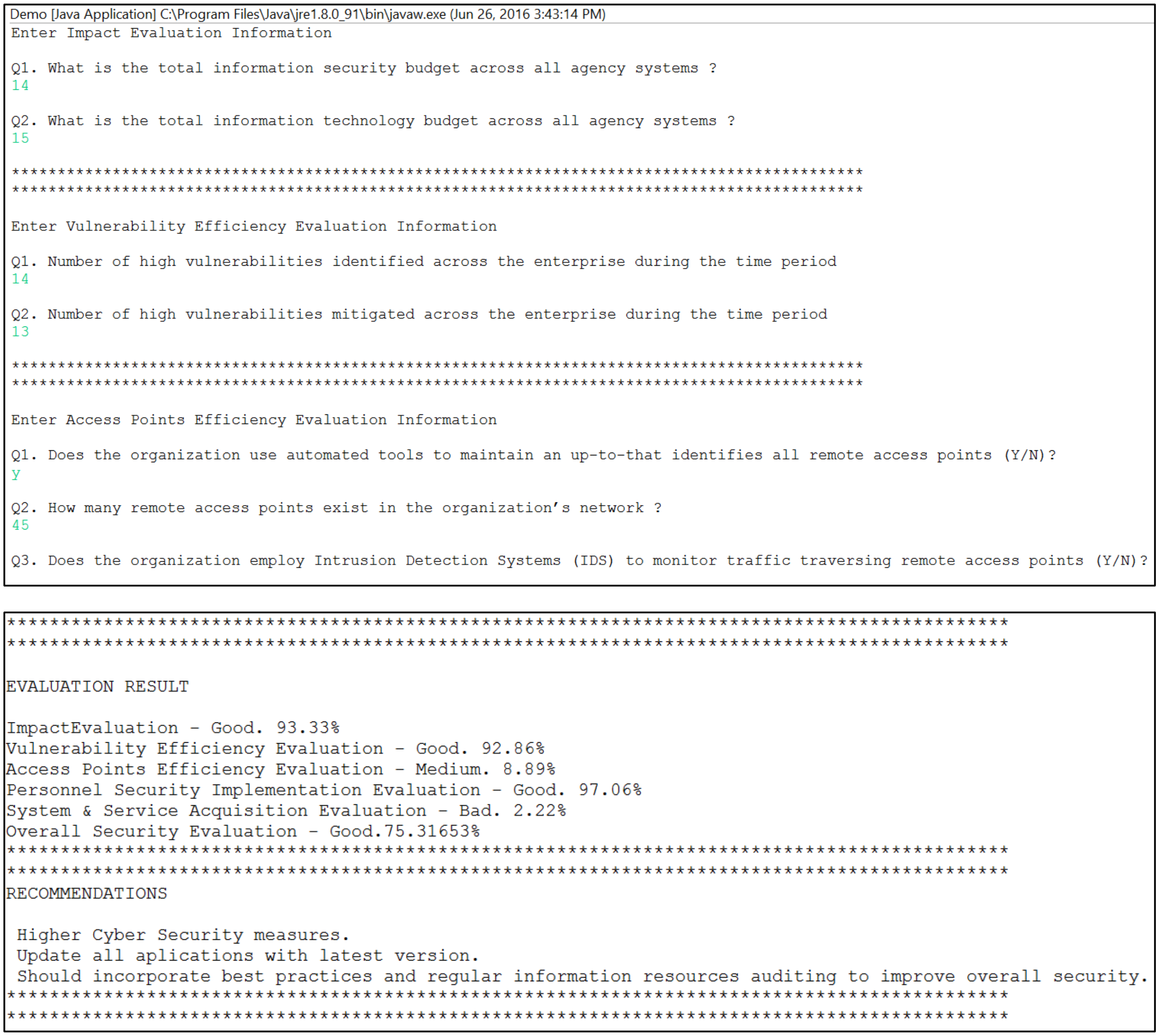
Testing Environment Specification:

SNo.	Type	Name	API	Target
1	Device	Samsung A3	21	Android 5.0.2

Downloaded the e2gDroid Lite Application from google store and loaded the knowledge base file in the sdk card of the phone. Then ran the application on the device, the response is evaluation result in percentage, graded (good/medium/bad) as well as the recommendation. The description for validation error codes for e2gDroid Lite is available at the company website.

4 User Interface

1) Project 1: SecureAgent - Console Based Expert System

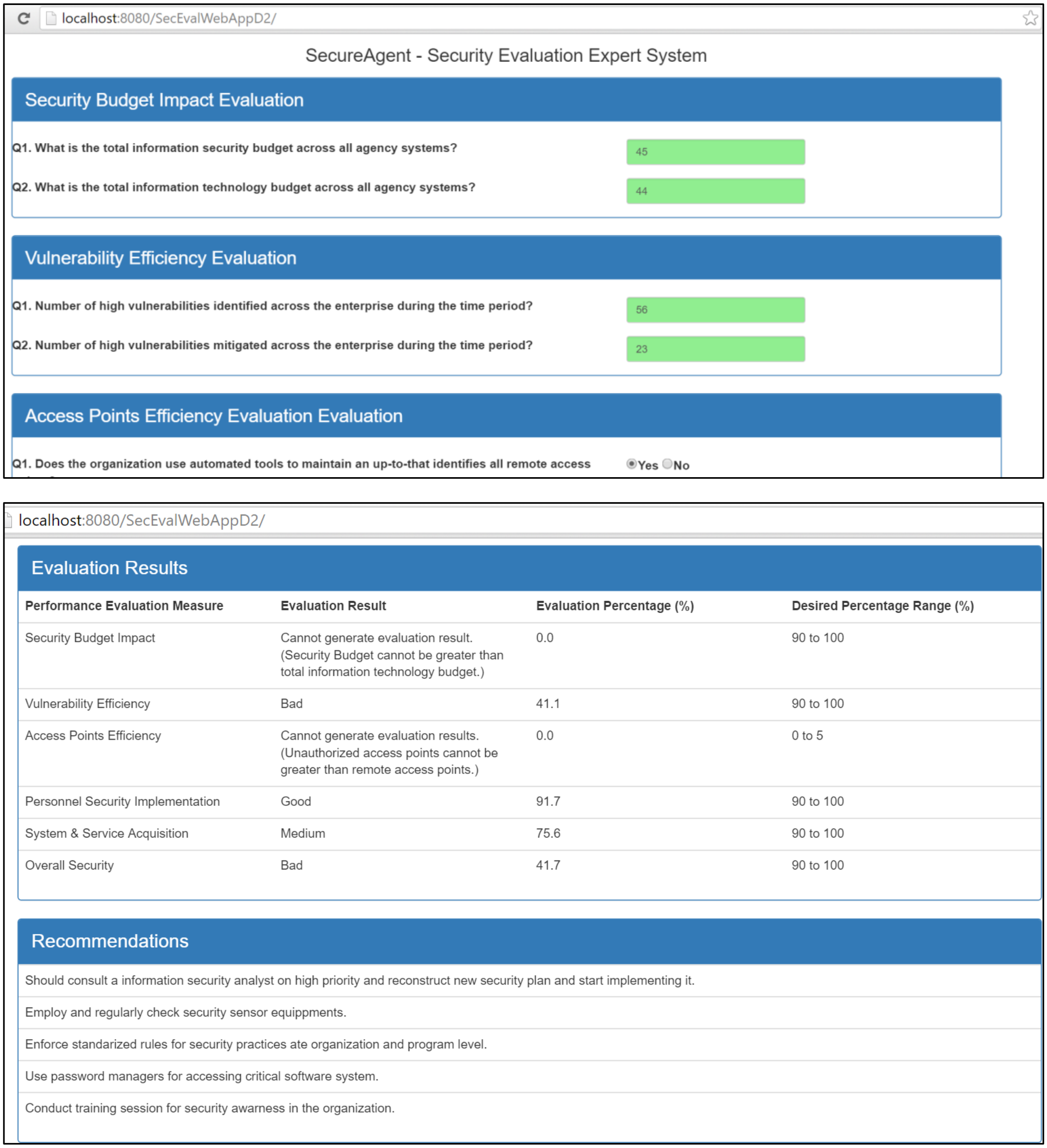


```
Demo [Java Application] C:\Program Files\Java\jre1.8.0_91\bin\javaw.exe (Jun 26, 2016 3:43:14 PM)
Enter Impact Evaluation Information

Q1. What is the total information security budget across all agency systems ?
14

Q2. What is the total information technology budget across all agency systems ?
15

*********************************************************************************************
*********************************************************************************************

Enter Vulnerability Efficiency Evaluation Information

Q1. Number of high vulnerabilities identified across the enterprise during the time period
14

Q2. Number of high vulnerabilities mitigated across the enterprise during the time period
13

*********************************************************************************************
*********************************************************************************************

Enter Access Points Efficiency Evaluation Information

Q1. Does the organization use automated tools to maintain an up-to-that identifies all remote access points (Y/N)?
y

Q2. How many remote access points exist in the organization's network ?
45

Q3. Does the organization employ Intrusion Detection Systems (IDS) to monitor traffic traversing remote access points (Y/N)?
```

```
*********************************************************************************************
*********************************************************************************************

EVALUATION RESULT

ImpactEvaluation - Good. 93.33%
Vulnerability Efficiency Evaluation - Good. 92.86%
Access Points Efficiency Evaluation - Medium. 8.89%
Personnel Security Implementation Evaluation - Good. 97.06%
System & Service Acquisition Evaluation - Bad. 2.22%
Overall Security Evaluation - Good.75.31653%
*********************************************************************************************
*********************************************************************************************
RECOMMENDATIONS

 Higher Cyber Security measures.
 Update all aplications with latest version.
 Should incorporate best practices and regular information resources auditing to improve overall security.
*********************************************************************************************
*********************************************************************************************
```

Figure 1: Console Application GUI

2) Project 2: SecureAgent - Web Based Expert System



SecureAgent - Security Evaluation Expert System

Security Budget Impact Evaluation

Q1. What is the total information security budget across all agency systems? 45

Q2. What is the total information technology budget across all agency systems? 44

Vulnerability Efficiency Evaluation

Q1. Number of high vulnerabilities identified across the enterprise during the time period? 56

Q2. Number of high vulnerabilities mitigated across the enterprise during the time period? 23

Access Points Efficiency Evaluation Evaluation

Q1. Does the organization use automated tools to maintain an up-to-that identifies all remote access ● Yes ○ No

Evaluation Results

Performance Evaluation Measure	Evaluation Result	Evaluation Percentage (%)	Desired Percentage Range (%)
Security Budget Impact	Cannot generate evaluation result. (Security Budget cannot be greater than total information technology budget.)	0.0	90 to 100
Vulnerability Efficiency	Bad	41.1	90 to 100
Access Points Efficiency	Cannot generate evaluation results. (Unauthorized access points cannot be greater than remote access points.)	0.0	0 to 5
Personnel Security Implementation	Good	91.7	90 to 100
System & Service Acquisition	Medium	75.6	90 to 100
Overall Security	Bad	41.7	90 to 100

Recommendations

Should consult a information security analyst on high priority and reconstruct new security plan and start implementing it.

Employ and regularly check security sensor equippments.

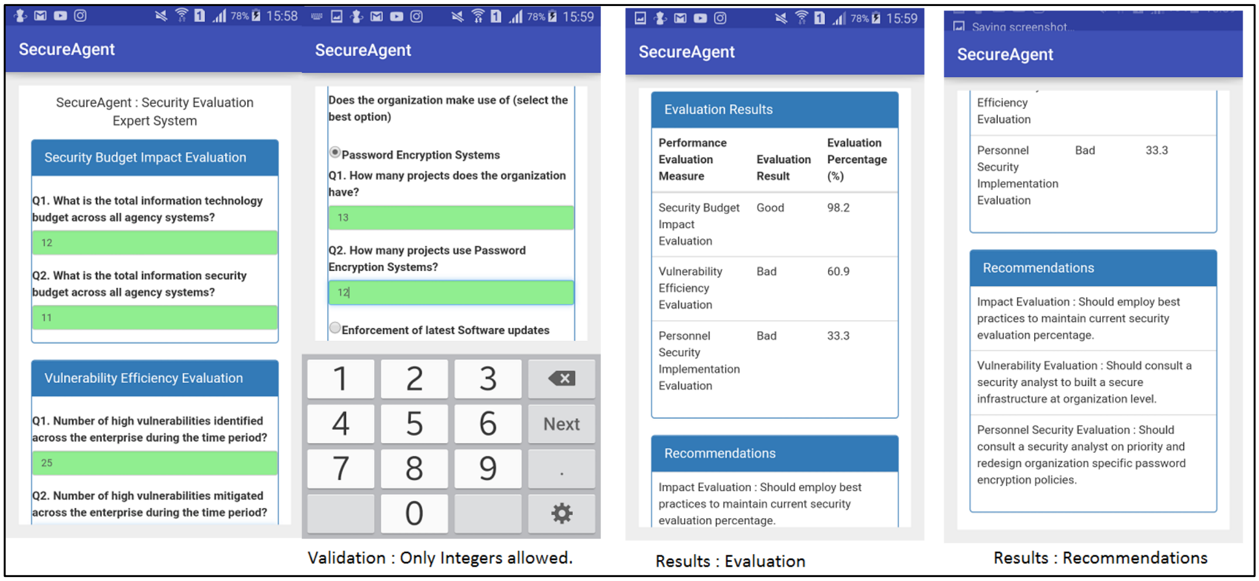
Enforce standarized rules for security practices ate organization and program level.

Use password managers for accessing critical software system.

Conduct training session for security awarness in the organization.

Figure 2: Web Application GUI

3) Project 3: SecureAgent - Android Expert System with Java Rule base.



SecureAgent : Security Evaluation Expert System

Security Budget Impact Evaluation

Q1. What is the total information technology budget across all agency systems?

12

Q2. What is the total information security budget across all agency systems?

11

Vulnerability Efficiency Evaluation

Q1. Number of high vulnerabilities identified across the enterprise during the time period?

25

Q2. Number of high vulnerabilities mitigated across the enterprise during the time period?

Does the organization make use of (select the best option)

● **Password Encryption Systems**

Q1. How many projects does the organization have?

13

Q2. How many projects use Password Encryption Systems?

12

○ **Enforcement of latest Software updates**

Validation : Only Integers allowed.

Evaluation Results

Performance Evaluation Measure	Evaluation Result	Evaluation Percentage (%)
Security Budget Impact Evaluation	Good	98.2
Vulnerability Efficiency Evaluation	Bad	60.9
Personnel Security Implementation Evaluation	Bad	33.3

Recommendations

Impact Evaluation : Should employ best practices to maintain current security evaluation percentage.

Results : Evaluation

Efficiency Evaluation		
Personnel Security Implementation Evaluation	Bad	33.3

Recommendations

Impact Evaluation : Should employ best practices to maintain current security evaluation percentage.

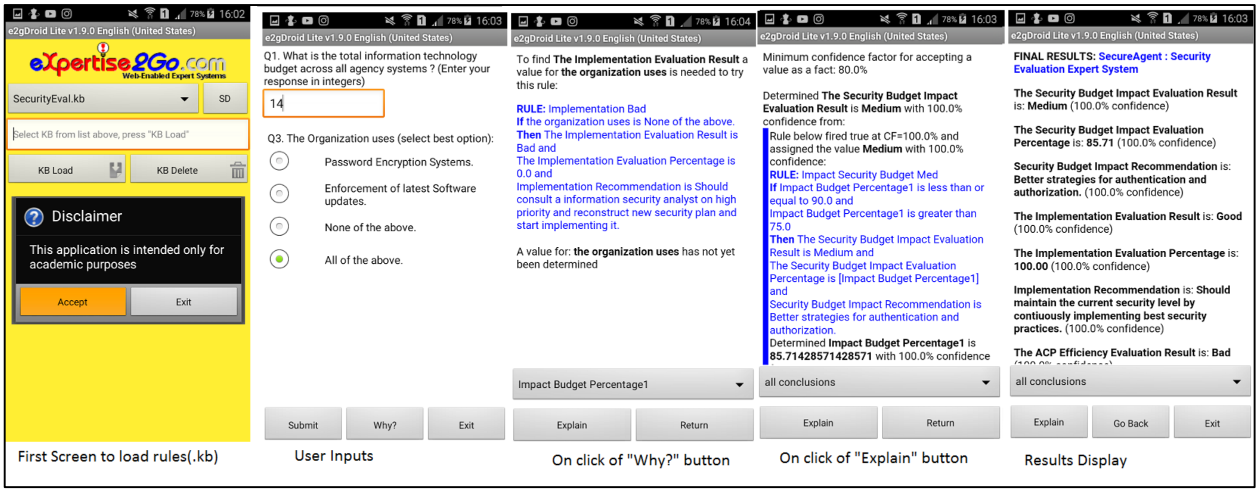
Vulnerability Evaluation : Should consult a security analyst to built a secure infrastructure at organization level.

Personnel Security Evaluation : Should consult a security analyst on priority and redesign organization specific password encryption policies.

Results : Recommendations

Figure 3: Android Application GUI (Samsung A3)

4) Project 4: SecureAgent - Android Based Expert System with e2gDroid Rule base.



SecurityEval.kb

Select KB from list above, press "KB Load"

Disclaimer

This application is intended only for academic purposes

First Screen to load rules(.kb)

Q1. What is the total information technology budget across all agency systems ? (Enter your response in integers)

14

Q3. The Organization uses (select best option):

○ Password Encryption Systems.

○ Enforcement of latest Software updates.

○ None of the above.

● All of the above.

User Inputs

To find **The Implementation Evaluation Result** a value for **the organization uses** is needed to try this rule:

RULE: Implementation Bad
If the organization uses is None of the above.
Then The Implementation Evaluation Result is Bad and
The Implementation Evaluation Percentage is 0.0 and
Implementation Recommendation is Should consult a information security analyst on high priority and reconstruct new security plan and start implementing it.

A value for: **the organization uses** has not yet been determined

Impact Budget Percentage1

On click of "Why?" button

Minimum confidence factor for accepting a value as a fact: 80.0%

Determined **The Security Budget Impact Evaluation Result** is **Medium** with 100.0% confidence from:

> Rule below fired true at CF=100.0% and assigned the value **Medium** with 100.0% confidence:
> **RULE:** Impact Security Budget Med
> **If** Impact Budget Percentage1 is less than or equal to 90.0 and
> Impact Budget Percentage1 is greater than 75.0
> **Then** The Security Budget Impact Evaluation Result is Medium and
> The Security Budget Impact Evaluation Percentage is [Impact Budget Percentage1] and
> Security Budget Impact Recommendation is Better strategies for authentication and authorization.
> Determined **Impact Budget Percentage1** is **85.71428571428571** with 100.0% confidence

all conclusions

On click of "Explain" button

FINAL RESULTS: **SecureAgent : Security Evaluation Expert System**

The Security Budget Impact Evaluation Result is: **Medium** (100.0% confidence)

The Security Budget Impact Evaluation Percentage is: **85.71** (100.0% confidence)

Security Budget Impact Recommendation is: **Better strategies for authentication and authorization.** (100.0% confidence)

The Implementation Evaluation Result is: **Good** (100.0% confidence)

The Implementation Evaluation Percentage is: **100.00** (100.0% confidence)

Implementation Recommendation is: **Should maintain the current security level by contiuously implementing best security practices.** (100.0% confidence)

The ACP Efficiency Evaluation Result is: **Bad**

all conclusions

Results Display

Figure 4: Android Application GUI (Samsung A3)

5 Hardware & Software Requirements

1) Project 1 & Project 2: SecureAgent – Console/Web Based Expert System

SNo.	Type	Specifications
1	Operating System	Windows, Linux, Unix
2	Integrated development environment (IDE)	Eclipse IDE Juno
3	Server	TOMCAT 7.0
4	JAVA	JDK 1.8
5	JESS	JESS 7.0 jar

2) Project 3 & Project 4: SecureAgent - Android Expert System with Java/e2gDroid Rule base.

SNo.	Type	Specifications
1	Operating System	Windows, Linux, Unix
2	Integrated development environment (IDE)	Android Studio, Notepad ++
3	Mobile/Mobile Phone Emulator	Andriod mobile phone API level 19 & above (Ex- Google Nexus).
4	JAVA	JDK 1.8
5	Mobile Application (only for project 4)	e2gDroid Lite application downloaded from google store on android mobile phone (search for e2gDroid on play store and download the app).

6 Applications & Limitations

Applications

1) "SecureAgent" can be used for fabricating organization specific security rules and for regular security assessment at project and at organization level. A key feature of SecureAgent is use of JESS, which separated the data from the logic. For example, if a new measure is to be added or a previous measure is to be edited, the developer need not write any extra logic, he just has to add/edit rules to the rule base.
2) The advantage of using a responsive framework for website development, makes "SecureAgent" (project 2) portable even on mobile and tablets. Also the dynamic binding element of the web page allows the user to make change to the questions and see the output synchronously.
3) "SecureAgent" android application makes it accessible in remote location where internet connection is not present. Specially project 4, which makes use of e2gDroid shell, requires a file as rule base input, which can be saved in the phone memory. Thus making the SecureAgent application more accessible.
4) For the benefit of the stakeholder, project 4 interface provides reasoning options such as "**Why** – to answer why this particular question is asked" and "**Explain** – to inquire how this result was calculated". Thus providing more information to the stakeholders.

Limitations

1) Currently SecureAgent application supports 5 security measures for project 1 & 2 and 3 security measures for android applications. However, if required more measures can be added to the rule base of SecureAgent to provide more robust security evaluation.
2) SecureAgent app is developed only for android mobiles, as a future work it can be developed for ios and windows platform.
3) The backend code for JESS rule implementation is exposed through servlet. As s future work, it could be made reusable by exposing it as REST Service. Thus other applications can also use the security evaluation assessment by calling the rest service and hence increasing reusability.

7 User Manual

Ensure that the system has JDK 1.8 installed and below environment variables are set.

JAVA_HOME, JDK_HOME, JESS_HOME, JRE_HOME, TOMCAT_HOME

1) Project 1: SecureAgent - Console Based Expert System

Step 1 - Open Eclipse Juno IDE.

Step 2 - Unzip project 1 and import the project in Eclipse Juno.

Step 3 - Add all the jars in the *"lib"* folder to the java build path.

Step 4 - Run the *"demo.java"* file located in *"com.security.evaluation.demo"* package.

Step 5 - Answers the questions appearing in console and click enter.

2) Project 2: SecureAgent - Web Based Expert System

Step 1 - Open Eclipse Juno IDE.

Step 2 - Install Tomcat server by right click on server view -> Add new server.

Step 3 - Unzip project 2 and import the project in Eclipse Juno.

Step 4 - Add all the jars in the *"lib"* folder to the java build path.

Step 5 - Go to eclipse menu bar. Window -> Web Browser -> Select Google chrome browser. (For best user interface display.)

Step 6 - Run the application, by right click on the project -> run as -> "Run on Server".

Step 7 - The web application will open in google chrome browser. Answer the questions and click submit to see the evaluation results.

3) Project 3: SecureAgent - Android Expert System with Java Rule base.

Step 1 - Open Android Studio and import project 3.

Step 2 - Modify *"build.gradle"* file for module *"app"* and modify *buildToolsVersion* parameter to *"23.0.2"*.

Step 3 - Launch AVD manager and create emulator “Nexus 5 API 19”. Start the emulator. Or connect your android mobile phone with help of USB to the computer.

Step 4 - Run the application by choosing either the emulator or the device option.

4) Project 4: SecureAgent - Android Based Expert System with e2gDroid Rule base.

Step 1 – Download “e2gDroid Lite” app from google play store in your android mobile phone.

Step 2 – Unzip project 4 and place the *“SecurityEval.kb”* file in the *“e2gkb”* folder in device storage.

Step 3 – Open the “e2gDroid Lite” app on your mobile and select the *“SecurityEval.kb”* file from the dropdown options in the SD slot.

Step 4 – Click on “KB Load” button and then on “Start” button.

Step 5 – Answers the questions. Please consider that all the questions either accepts integers as input or are radio button options.

8 Appendix 1.0

JESS Rules for Project 1 & 2 SecureAgent: Console and Web based Expert System

Refer to file *“security_rule.clp”* located under “*src”* folder in project 1 and 2.

9 Appendix 2.0

Java Rules for Project 3 SecureAgent: Android based Expert System using Java Rule base.

Refer to file *“security_controller.js”* located under “*assets”* folder inside “*app”* folder in project 3.

9 Appendix 2.1

E2gDroid Rules for Project 4 SecureAgent: Android based Expert System using e2gDroid Rule base.

RULE 1

RULE [Calculate Impact Budget Percentage1]

If [iq one] ? and

[iq two] ?

Then [Impact Budget Percentage1] = {([iq two] / [iq one]) * 100}

RULE 2

RULE [Calculate Access Point Efficiency Percentage1]

If [iq three] ? and

[iq four] ?

Then [Access Point Efficiency Percentage1] = {([iq four] / [iq three]) * 100}

RULE 3

RULE [Impact Security Budget Bad]

If [Impact Budget Percentage1] <= 75

Then [The Security Budget Impact Evaluation Result] = "Bad" and

[The Security Budget Impact Evaluation Percentage] = {[Impact Budget Percentage1]} and

[Security Budget Impact Recommendation is] = "Enforce standarized rules for security practices ate organization and program level."

RULE 4

RULE [Impact Security Budget Med]

If [Impact Budget Percentage1] <= 90 and

[Impact Budget Percentage1] > 75

Then [The Security Budget Impact Evaluation Result] = "Medium" and

[The Security Budget Impact Evaluation Percentage] = {[Impact Budget Percentage1]} and

[Security Budget Impact Recommendation] = "Better strategies for authentication and authorization."

RULE 5

RULE [Impact Security Budget Good]

If [Impact Budget Percentage1] > 90 and

[Impact Budget Percentage1] <= 100

Then [The Security Budget Impact Evaluation Result] = "Good" and

[The Security Budget Impact Evaluation Percentage] = {[Impact Budget Percentage1]} and

[Security Budget Impact Recommendation] = "Should maintain the current security level by contiuously implementing best security practices."

RULE 6

RULE [Impact Security Budget CannotDetermine]

If [Impact Budget Percentage1] > 100

Then [The Security Budget Impact Evaluation Result] = "Cannot Determine" and

[The Security Budget Impact Evaluation Percentage] = 0 and

[Security Budget Impact Recommendation] = "Invalid Input.Security budget cannot be greater than total budget."

RULE 7

RULE [Implementation Bad]

If [the organization uses] = "None of the above."

Then [The Implementation Evaluation Result] = "Bad" and

[The Implementation Evaluation Percentage] = 0 and

[Implementation Recommendation] = "Should consult a information security analyst on high priority and reconstruct new security plan and start implementing it."

RULE 8

RULE [Implementation Med]

If [the organization uses] = "Password Encryption Systems."

Then [The Implementation Evaluation Result] = "Medium" and

[The Implementation Evaluation Percentage] = 50 and

[Implementation Recommendation] = "Employ and regularly check security sensor equippments."

RULE 9

RULE [Implementation Med1]

If [the organization uses] = "Enforcement of latest Software updates."

Then [The Implementation Evaluation Result] = "Medium" and

[The Implementation Evaluation Percentage] = 50 and

[Implementation Recommendation] = "Employ and regularly check security sensor equippments."

RULE 10

RULE [Implementation Bad]

If [the organization uses] = "All of the above."

Then [The Implementation Evaluation Result] = "Good" and

[The Implementation Evaluation Percentage] = 100 and

[Implementation Recommendation] = "Should maintain the current security level by contiuously implementing best security practices."

RULE 11

RULE [Access Point Efficiency Good]

If [Access Point Efficiency Percentage1] < 5

Then [The ACP Efficiency Evaluation Result] = "Good" and

[The ACP Efficiency Evaluation Percentage] = {[Access Point Efficiency Percentage1]} and

[ACP Efficiency Recommendation] = "Should maintain the current security level by contiuously implementing best security practices."

RULE 12

RULE [Access Point Efficiency Med]

If [Access Point Efficiency Percentage1] >= 5 and

[Access Point Efficiency Percentage1] < 10

Then [The ACP Efficiency Evaluation Result] = "Medium" and

[The ACP Efficiency Evaluation Percentage] = {[Access Point Efficiency Percentage1]} and

[ACP Efficiency Recommendation] = "Should inforce privacy standards at organization and project level.Desired ACP percentage should be less than 5 %."

RULE 13

RULE [Access Point Efficiency Bad]

If [Access Point Efficiency Percentage1] >= 10 and

[Access Point Efficiency Percentage1] <= 100

Then [The ACP Efficiency Evaluation Result] = "Bad" and

[The ACP Efficiency Evaluation Percentage] = {[Access Point Efficiency Percentage1]} and

[ACP Efficiency Recommendation] = "Conduct training session for security awarness in the organization. Desired ACP percentage should be less than 5 %."

RULE 14

RULE [Access Point Efficiency CannotDetermine]

If [Access Point Efficiency Percentage1] > 100

Then [The ACP Efficiency Evaluation Result] = "Cannot Determine" and

[The ACP Efficiency Evaluation Percentage] = 0 and

[ACP Efficiency Recommendation] = "Invalid Input. unauthorized access points cannot be greater than total access points."

11 References

[1] Chew, Elizabeth, et al. Performance measurement guide for information security. US Department of Commerce, National Institute of Standards and Technology, 2008.

[2] Friedman-Hill, Ernest J. "Jess, the java expert system shell." Distributed Computing Systems, Sandia National Laboratories, USA (1997).

[3] http://www.expertise2go.com/e2g3g/e2g3gdoc/e2gmod7.htm#ANDROID. Retrieved June 26, 2016.

[4] Reznik, Leon. "Integral instrumentation data quality evaluation: The way to enhance safety, security, and environment impact." Instrumentation and Measurement Technology Conference (I2MTC), 2012 IEEE International. IEEE, 2012.

[5] Hoffman, A., Pollard, D., Reznik, L. Hierarchical Security Evaluation Framework and its Implementation on Android Smartphones.

[6] Mc Cune, Brian P., et al. "RUBRIC: A system for rule-based information retrieval." Software Engineering, IEEE Transactions on 9 (1985): 939-945.

[7] Cañadas, Joaquín, José Palma, and Samuel Túnez. InSCo-Gen: A MDD tool for Web rule-based applications. Springer Berlin Heidelberg, 2009.

[8] Zhang, Yajuan, et al. "Assessment of E-Commerce security using AHP and evidential reasoning." Expert Systems with Applications 39.3 (2012): 3611-3623.

[9] Hemmer, Markus C. (2008). Expert Systems in Chemistry Research. CRC Press. pp. 47–48. Retrieved March 30, 2012. ISBN 978-1-4200-5323-4