Reference


[04] Mohammad A. Rashid (Massey University, New Zealand), Liaquat Hossain (Syracuse University, USA) and Jon David Patrick (University of Sydney, Australia) (2002), The Evolution of ERP Systems: A Historical Perspective


[22] Rodi Heijblom (2015), Controlling risks when integrating Mobility and Enterprise Resource Planning (ERP), Master of Business Informatics, Utrecht University


[29] https://www.mysql.com/about/, Retrieved on 08th December 2015


[31] https://www.phpmyadmin.net/, Retrieved on 08th December 2015


Appendix A – NAV ERP system

Figure A-1 shows NAV ERP windows client architecture [34].

Figure A-1: Microsoft Dynamics NAV windows client architecture
Figure A - 2 shows NAV ERP three-tier architecture [35].

Figure A-2 : NAV ERP three-tier architecture

Figure A-3 shows NAV ERP server configuration interface, it was located on the ERP server computers program file -> NAV ERP administration tool path.
**Figure A-3: NAV ERP server configuration interface**
Appendix B – User Guide for the System

This is the user guide of our solution in order to running the application users must have hardware and software that we are mentioned in the Chapter 1.

B.1 How we can access the system?

Users can access the system by entering the system address on their web browser. After that they must have enter their login credentials. Below figure B-1 shows how users can access the system.

![System login screen](image)

*Figure B-1 : System login screen*

After successful login users can view there dashboard to perform various function that we have implemented within the system.
According to the user requirement they can perform actions within the system by clicking on the hyperlink, main system icons or navigating through the menu bar. Below sub sections we describe how to perform system main security scanning’s and audits.

### B.2 How do we scan NAV ERP server configuration?

To perform a NAV ERP server security scan user must have permission to read “CustomSettings.config” file that was located inside the NAV ERP server installation folder (Ex: Program Files\Microsoft Dynamics NAV\71\Service).

**Step 01:** Click on the “Dynamics NAV Configuration” link, it will open server configuration scan main page that consist of all scan data.
**Step 02:** Click on add new scan profile button.

![Image](image-url)

*Figure B-4: Uploading NAV ERP configuration file*

**Step 03:** After entering all form data click on save button.

*Figure B-5: Upload confirm dialog*

**Step 04:** Performing a security scan by clicking on the "1 (red color)" icon.

![Image](image-url)

*Figure B-6: Perform a security scan*
Step 05: After the clicking on scan icon system will display the Scan report

Dynamics NAV Configuration Scan

<table>
<thead>
<tr>
<th>Issue</th>
<th>Configuration Key</th>
<th>Current Value</th>
<th>Recommended Value</th>
<th>Security Tips</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>EnableSqlConnectionEncryption</td>
<td>false</td>
<td>true</td>
<td>By enabling the encryption on the SQL Connections used against the database. The Middle Attackers are unable or very hard to read or modify any requests that they may intercept.</td>
</tr>
<tr>
<td>02</td>
<td>ClientServicesMaxUploadSize</td>
<td>300</td>
<td>5</td>
<td>Limiting the size of files that can be uploaded will help to avoid out of memory errors. When those situation Attackers can create DOS based attacks.</td>
</tr>
<tr>
<td>03</td>
<td>ClientServicesProhibitedFileTypes</td>
<td>.bat,.xml,.pdf</td>
<td>-</td>
<td>It is recommended that file upload not used block all file types by putting &quot;*&quot; or block at least known executable/threat files.</td>
</tr>
<tr>
<td>04</td>
<td>SqlCommandTimeout</td>
<td>00:30:00</td>
<td>00:10:00</td>
<td>Setting less timeout for the SQL command will help to avoid out of memory errors. When those situation Attackers can create DOS based attacks.</td>
</tr>
<tr>
<td>05</td>
<td>ClientServicesOperationTimeout</td>
<td>MaxValue</td>
<td>00:10:00</td>
<td>Client services time out will help to prevent when unauthorized inside or Middle Attackers trying to run some large queries.</td>
</tr>
</tbody>
</table>

Figure B-7: Scan summary report

B.3 How do we scan NAV ERP User Permission Issues?

To perform a NAV ERP server permission issue scan, users must click on the “NAV User Permission Issues” link.

Step 01: After click on “NAV User Permission Issues” link you will see below interface;

Dynamics NAV Permission Sets Audit

Figure B-8: User permission set scan main
Step 02: To add new permission set you must need to click on “New Permission Set” link.

Add New Dynamics NAV Permission Sets Audit

<table>
<thead>
<tr>
<th>Permission Set Name</th>
<th>: Create Purchase Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module</td>
<td>: Purchase</td>
</tr>
<tr>
<td>Orginal Permission Set</td>
<td>: Browse... Create-PO.xlsx</td>
</tr>
</tbody>
</table>

*Figure B-9: Adding new permission set*

Step 03: After uploading main permission sets users can audit permission set by comparing the live NAV ERP server permission set.

Dynamics NAV Permission Sets Audit

*Figure B-10: Auditing permission sets*
Step 04: After the auditing phase if system found permission conflicts then users will see report that containing those conflict entries.

**NAV ERP Permission Audit Report**

<table>
<thead>
<tr>
<th>#</th>
<th>Object Type</th>
<th>Object Name</th>
<th>Read</th>
<th>Insert</th>
<th>Modify</th>
<th>Delete</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Table Data</td>
<td>User Setup</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Table Data</td>
<td>Vendors</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Table</td>
<td>Items</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Page</td>
<td>Purchase Order</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>5</td>
<td>Page</td>
<td>Vendors</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Figure B-11: Permission conflict entries report*

B.4 how do we audit NAV change log issues?

To perform a NAV ERP change log issue scan users must click on the "NAV Change Log Audit" link.

Step 01: After clicking the link users will see audit data filtering form by entering relevant data user required to click on Audit button (5)

**Dynamics NAV Change Log Analysis**

*Figure B-12: Change log audit form*
Step 02: If system found results based on user entered values system will display a list of changes as follows;

### NAV ERP Permission Audit Report

<table>
<thead>
<tr>
<th>#</th>
<th>Date and Time</th>
<th>Table name</th>
<th>Filed Name</th>
<th>Primary Key 1 Value</th>
<th>Type of Change</th>
<th>Old Value</th>
<th>New Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3/05/2016 8:23:02 AM</td>
<td>User Setup</td>
<td>Register Time</td>
<td>150</td>
<td>Deletion</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>3/11/2016 9:23:02 AM</td>
<td>Vendors</td>
<td>Pay-to-Vendor File</td>
<td>5000</td>
<td>Modification</td>
<td>5000</td>
<td>6000</td>
</tr>
<tr>
<td>3</td>
<td>3/11/2016 9:24:02 AM</td>
<td>Vendors</td>
<td>Prepayment %</td>
<td>6000</td>
<td>Insertion</td>
<td>0</td>
<td>100</td>
</tr>
</tbody>
</table>

**Figure B-13 : Change log audit report**

### B.5 How do we monitor NAV user sessions?

To view the NAV ERP user session report they users must need to click on the “NAV User Sessions Monitor” link. After clicking link figure B - 15 form will display by selecting relevant server using the drop down menu users can view user session report.

### Active Users Sessions Monitor

![Active Users Sessions Monitor](image)

**Figure B-14 : User session monitoring report**
B. 6 How do we audit NAV ERP user’s password strength?

Step 01: Users required obtain NTDIS database file from the AD server. After that clicking add new scan profile link on password strength master file user can create a new scan profile.

Password Strength Analysis

Step 02: Using the data upload form users can create new scan profile with relevant NTDIS database file.

Add New Dynamics NAV Configuration

Please fill all the required fields before submit this form!

AD Server Name : Primary Domain Server
AD Server NTDS.dit file : Browse... NTDS.dit

Figure B-15: Password strength audit profile create 1

Figure B-16: Password strength audit profile create 2
Step 03: By clicking relevant server profile scan button users can perform audits.

Password Strength Analysis

Choose an action... □ Add New Scan Profile

Scan Name: Primary Domain Server

Choose an action... □ Apply to selection

Figure B-17: Password strength audit scan

Step 04: View password strength report details.

Password Strength Analysis Report

<table>
<thead>
<tr>
<th>#</th>
<th>Audit Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>One to Six Characters</td>
<td>10 (33.33%)</td>
</tr>
<tr>
<td>02</td>
<td>Six to Eight Characters</td>
<td>12 (40%)</td>
</tr>
<tr>
<td>03</td>
<td>More than Eight Characters</td>
<td>8 (26.66%)</td>
</tr>
</tbody>
</table>

Password Content Analysis

<table>
<thead>
<tr>
<th>#</th>
<th>Audit Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Only lowercase alpha</td>
<td>15 (50%)</td>
</tr>
<tr>
<td>02</td>
<td>Only uppercase alpha</td>
<td>6 (20%)</td>
</tr>
<tr>
<td>03</td>
<td>Only alpha</td>
<td>9 (30%)</td>
</tr>
</tbody>
</table>

Password Length

<table>
<thead>
<tr>
<th>#</th>
<th>Length</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>5</td>
<td>10 (33%)</td>
</tr>
<tr>
<td>02</td>
<td>6</td>
<td>2 (6.66%)</td>
</tr>
<tr>
<td>03</td>
<td>7</td>
<td>4 (13.33%)</td>
</tr>
<tr>
<td>04</td>
<td>8</td>
<td>6 (20%)</td>
</tr>
<tr>
<td>05</td>
<td>9</td>
<td>5 (16.66%)</td>
</tr>
<tr>
<td>06</td>
<td>10</td>
<td>3 (3.33%)</td>
</tr>
</tbody>
</table>

Figure B-18: Password strength audit scan report
B.7 How do we scan NAV ERP server open ports?

**Step 01:** Click on the “Server Open Ports Scan” link and entering server name and IP address. After that click “Scan Server Port” button.

- Step 02: After click on scan port button system will scan server for open ports and display if it found vulnerable or risk based ports are open.

<table>
<thead>
<tr>
<th>#</th>
<th>Open Port No</th>
<th>Port Usage</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>3389</td>
<td>RDS</td>
<td>Attackers can access system through the remote desktop</td>
</tr>
<tr>
<td>02</td>
<td>21</td>
<td>FTP</td>
<td>File system can access using FTP:</td>
</tr>
<tr>
<td>03</td>
<td>23</td>
<td>Telnet</td>
<td>Telnet can be risk</td>
</tr>
<tr>
<td>04</td>
<td>139</td>
<td>NetBIOS</td>
<td>Using NetBIOS based sessions</td>
</tr>
</tbody>
</table>

**Figure B-19:** Server open ports scan

**Figure B-20:** Server open ports scan report
Appendix C – Test cases and test results

System has been tested using standard software testing process;

1. Unit testing – Test individual modules
2. Integration testing – When integrating the module this test performs.
3. System testing – After integrating the all module finally we test the entire system.
4. User interface testing – confirms the user interface have the industry standards.

In Table C-1 shows the detail description of the test cases and result.

<table>
<thead>
<tr>
<th>Case ID</th>
<th>Test Data</th>
<th>Expected Results</th>
<th>Pass/Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>Upload the NAV ERP server configuration file</td>
<td>Successfully uploaded</td>
<td>Pass</td>
</tr>
<tr>
<td>Case 2</td>
<td>Scan NAV ERP configuration data having security issues</td>
<td>found security issues are shown report with suggestions</td>
<td>Pass</td>
</tr>
<tr>
<td>Case 3</td>
<td>Scan NAV ERP configuration data after fixing the security issues</td>
<td>Show report indicating no issues found.</td>
<td>Pass</td>
</tr>
<tr>
<td>Case 4</td>
<td>Uploading NAV user permission set file</td>
<td>Successfully uploaded</td>
<td>Pass</td>
</tr>
<tr>
<td>Case 5</td>
<td>Changing uploaded permission set related data through NAV ERP and after that checking NAV user permission set for security issues</td>
<td>Show changed security permissions as report.</td>
<td>Pass</td>
</tr>
<tr>
<td>Case 6</td>
<td>Create new vendor and delete that vendor after that audit Vendor id and deleted user</td>
<td>Show deleted user related change log data</td>
<td>Pass</td>
</tr>
<tr>
<td>Case 7</td>
<td>Login to the system and change logged on computers name as “XYZ-PC” then restart computer and logon to the system. After that check NAV ERP user session audit report.</td>
<td>Show changed pc name and logon users name as conflict session.</td>
<td>Pass</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Case 8</td>
<td>In the windows domain controller create 10 users with same password and same character length, after that run the password strength scan</td>
<td>Show newly created user’s password strength data by updating existing contain user’s data as a report.</td>
<td>Pass</td>
</tr>
<tr>
<td>Case 9</td>
<td>ERP server computer create firewall rule to allow remote desktop, after that analysis server open port.</td>
<td>Report display port 3389 is open.</td>
<td>Pass</td>
</tr>
<tr>
<td>Case 10</td>
<td>Access the system by giving a wrong credential</td>
<td>Show error message saying user name or password incorrect</td>
<td>Pass</td>
</tr>
</tbody>
</table>

*Table C-1 : Test cases and test results*
Appendix D – Questionnaire used for requirement analysis

We have conducted an online survey using the “LimeSurvey” for the analysis of security issues founded during the literature review.

---

**Assessment of an ERP Implementation Information Security**

This survey has been designed as part of a MSc research project on Information Technology conducted at the University of Menzoa, Faculty of Information Technology. The purpose of the survey is to collect ERP Security related information.

### General Questions

- Does your organization have an ERP system?
  - Yes  
  - No

- Does your organization have an ERP security analysis tool?
  - Yes  
  - No

- Does your organization have an ERP security policy?
  - Yes  
  - No

- Do you think security analysis tool will protect and secure your organisation ERP system?
  - Yes  
  - No

- Does your think security policy will protect and secure your organisation ERP system?
  - Yes  
  - No

---

*Figure D-1: Requirements analysis survey - part 1*
### People Related Security Analyse

- **Does your organization maintain a password policy?**
  - [ ] Yes
  - [ ] No

- "Computer logon password strength may reason for ERP security issue" What is your opinion?
  - [ ] Not Critical
  - [ ] Medium Critical
  - [ ] Critical
  - [ ] High Critical
  - [ ] Extreme Critical

- If employees given system logon details to third party people or another employees, what is the level of security impact to the ERP system?
  - [ ] Not Critical
  - [ ] Medium Critical
  - [ ] Critical
  - [ ] High Critical
  - [ ] Extreme Critical

- How important is the security threats can be happen when users are forget to logoff or lock computers?
  - [ ] Not important
  - [ ] If it happens
  - [ ] Important
  - [ ] Very important
  - [ ] Extremely important

- How did you rank impact of Social Engineering Attacks to the ERP system?
  - [ ] Not Critical
  - [ ] Medium Critical
  - [ ] Critical
  - [ ] High Critical
  - [ ] Extreme Critical

- "Increases the risk of fraud and misappropriations by users who have excessive authority to the ERP system" What is your opinion?
  - [ ] Not Critical
  - [ ] Medium Critical
  - [ ] Critical
  - [ ] High Critical
  - [ ] Extreme Critical

- How did you rank the data loss when end users altered or deleted ERP system data by mistakenly or purposely?
  - [ ] Not Critical
  - [ ] Medium Critical
  - [ ] Critical
  - [ ] High Critical
  - [ ] Extreme Critical

*Figure D-2: Requirements analysis survey - part 2*
<table>
<thead>
<tr>
<th>Question</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>How you rank the impact to the organisation, when confidential data stolen or give to third parties by end user or others?</td>
<td>• Not Critical • Medium Critical • Critical • High Critical • Extreme Critical</td>
</tr>
<tr>
<td>Policy Related Security Analyse</td>
<td></td>
</tr>
<tr>
<td>What is the importance of an organisation ERP system policy?</td>
<td>• Not important • If it happens • Important • Very important • Extremely important</td>
</tr>
<tr>
<td>What is the importance of a defining users, systems and devices related password policy?</td>
<td>• Not important • If it happens • Important • Very important • Extremely important</td>
</tr>
<tr>
<td>What you think by having organisation policy related to the BYOD (bring your own devices) can be minimize the ERP security risk?</td>
<td>• Not Related • Can Be Related • Some Level Related • Highly Related • Extremely Related</td>
</tr>
<tr>
<td>How important is having an organisation ERP system security incident handling policy?</td>
<td>• Not important • If it happens • Important • Very important • Extremely important</td>
</tr>
<tr>
<td>What is the relevancy of ERP security by having a procedure of setting up authorization and access rights to the ERP system after Installation?</td>
<td>• Not Related • Can Be Related • Some Level Related • Highly Related • Extremely Related</td>
</tr>
</tbody>
</table>

Figure D-3: Requirements analysis survey - part 3
• How important is having a defined policy related to an emails, reports, backup file and system log files to the ERP security?
  - Not important
  - If it happens
  - Important
  - Very important
  - Extremely important

• “By having a policy related the Servers or Network devices physical/remote access can be minimize the threat level to the ERP system” What is you think?
  - Not Related
  - Can Be Related
  - Some Level Related
  - Highly Related
  - Extremely Related

• How is it important by having a policy for the third party people who access the ERP system?
  - Not important
  - If it happens
  - Important
  - Very important
  - Extremely important

Technology Related Security Analyse

• How are you rank of ERP security breaches using the outdated or vulnerable Application, Hardware or Firmware?
  - Not important
  - If it happens
  - Important
  - Very important
  - Extremely important

• How are you rank impact to the ERP based on security threats related to the Network or Application?
  - Not Critical
  - Medium Critical
  - Critical
  - High Critical
  - Extreme Critical

• How are you rank importance to the ERP implementation based on security issues of configuration on Firewall or VPN server?
  - Not important
  - If it happens
  - Important
  - Very important
  - Extremely important

Figure D-4 : Requirements analysis survey - part 4
How are you rank the impact of vulnerabilities having on third party application?

- Not important
- If it happens
- Important
- Very important
- Extremely important

"Secure data file storage, transmission and exchange related flaws, allowing hackers to obtain sensitive personal information." What is the level of security impact to the ERP system?

- Not Critical
- Medium Critical
- Critical
- High Critical
- Extreme Critical

**Figure D-5: Requirements analysis survey - part 5**
Appendix E – Questionnaire used for evaluating the system

We have conducted an online survey using LimeSurvey to evaluate our security analysis tool to check whether it was fulfilling the requirements.

**Evaluation of Microsoft Dynamics NAV ERP Security Analysis Tool**

This survey has been designed as part of a MSc research project on Information Technology conducted at the University of Moratuwa – Faculty of Information Technology. The purpose of the survey is to evaluate our Microsoft Dynamics NAV ERP Security Analysis Tool.

### Participant Information

- **Are you currently working on ERP industry?**
  - Yes
  - No

- **What is your designation?**
  - ERP Consultant
  - IT Security Auditor
  - Software Engineer
  - ERM Manager
  - IT Manager
  - IT professional
  - Other

### Quality Attributes

- **How are you rank the user interface of system?**
  - Poor
  - Below Average
  - Average
  - Good
  - Excellent

- **How are you rank the response time of application?**
  - Poor
  - Below Average
  - Average
  - Good
  - Excellent

- **How you rank the accuracy of result?**
  - Poor
  - Below Average
  - Average
  - Good
  - Excellent

- **What is your given quality grade for the exception handling?**
  - Poor
  - Below Average
  - Average
  - Good
  - Excellent

*Figure E-1: System evaluation survey - part 1*
<table>
<thead>
<tr>
<th>Question</th>
<th>Poor</th>
<th>Below Average</th>
<th>Average</th>
<th>Good</th>
<th>Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the level of user friendliness of the system?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How you rank the importance of security analysis modules?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security analysis tool results and suggestions are?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality of security analysis reports?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality of overall system?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Suggestions / Feedbacks**

Please give your suggestion to improve this solution

*Figure E-2: System evaluation survey - part 2*