Security Engineering Report

*Student 1: Name and Last Name, StudentID*

*Student 2: Name and Last Name, StudentID*

# TARGET OF EVALUATION (1/2 page)

This section should describe the part of the use case that you have analyzed and the assumptions you have made during the analysis.

# SUMMARY OF FINDINGS (1/2 page)

This section should describe the summary of all findings of the conducted work.

# DESCRIPTION OF METHOD APPLICATIONS TO ANALYSE %NAME OF THE TOPIC% (7 pages)

This section should report the assumptions, findings and application for each analyzed task.

## Identity and Access Management (3 pages)

### Summary of assumptions and finding (1/2 pages)

Present key assumptions and the key results of the security risk assessment of the task “Identity and Access Management”. Limit 1/2 page.

**The complete summary of results can be found in the document %Summary of results.xlsx% submitted as integral part of the current report.**

### Process used to analyze Authentication Requirements (1 pages)

Example of the description for the application of CORAS method:

We have used the CORAS method to analyze the Authentication Security. The main results of Step 1-3 is […]. We come up with these results based on the document %X% (cite the necessary document).

The results of Step 3 are the list of assets reported in diagram X and high-level risk analysis reported in Table Y (see diagram X and table Y at pages A-B in document %CORAS-exercise.pptx%). We defined this list of assets based on document/article/standard %X% (cite the necessary source).

The results of Step 4 are the asset table, likelihood and consequence scales for each asset, target definition and risk evaluation matrix, which reported at pages X-Y in document %CORAS-exercise.pptx%. We proposed the following list of assets for further risk assessment: [list assets selected for the risk assessment]. For example, we included in the risk assessment the asset A because this contains the sensitive information about users of the system.

At Step 5 and 6 we identified and estimate the main threats for the assets from Step 4. The corresponding threat diagrams reported at pages X-Y in document %CORAS-exercise.pptx%. We proposed these threats based on the document/article/standard Y (cite the necessary source). For example, we assume that threat A can lead to the unwanted incident B. This is possible due to existence of vulnerability C in the system under evaluation. This vulnerability can be used by threat D to initiate unwanted incident UI and attack asset A. We make this conclusion based on our experience in the Security.

At Step 7 we evaluate the risk based on the matrices proposed at Step 4 (see matrices A-B and risk diagrams C-D at pages E-F in document %CORAS-exercise.pptx%). Based on the results of this step we can conclude that the main risks need to be treated are [list risks that needs to be treated].

At Step 8 to mitigate the major risks we proposed the security controls that reported in diagrams A-B and table C in document %CORAS-exercise.pptx%. We selected these security controls based on the document/article/standard Y (cite the necessary source) or our own experience. For example, to mitigate the risk R1 we proposed to implement security controls SC1 because it can reduce the risk down to an acceptable level according to the document/article/standard Y (cite the necessary source). Or, for example, to mitigate the risk R2 we proposed to implement security controls SC2 based on our experience in Security.

### Process used to find Access Control Requirements (1 pages)

Example of the description for the application of SecRAM method:

At Step 1 we identified the primary assets and assess their impact on the Operational Focus Areas (OFAs) (see table 1.1 and 1.2 in the document %SecRAM-exercise.xlsx%). The main primary assets that we identified are the following [list 3-5 primary assets with the highest overall impact].

At Step 2 we identified supporting assets for the list of primary assets from Step 1 (see table 2 in the document %SecRAM-exercise.xlsx%). For example, for primary asset PA we identified the following supporting assets [list corresponding supporting assets] because we find this information in the document/article/standard X (cite the necessary source).

At Step 3 we identified threats to our supporting assets from Step 2 (see table 3 in the document %SecRAM-exercise.xlsx%). For example, the main threats for supporting asset SA are the following threats [list threats] because we assumed that supporting asset SA has weak protection against X that makes these threats possible to happened. This conclusion we made based on the information from the document/article/standard X (cite the necessary source).

At Step 4 we evaluated the impact and risk level of the threats identified at Step 3 (see table 4.1 and 4.2 in the document %SecRAM-exercise.xlsx%). The main threats that should be mitigated are the following threats [list 5 threats with highest risk level].

At Step 5 we proposed a set of security controls to mitigate major threats identified at Steps 3-4 (see table 5 in the document %SecRAM-exercise.xlsx%). We selected these security controls based on the document/article/standard X (cite the necessary source) or our own experience. For example, to mitigate the threat T1 we proposed to implement security controls SC1 because it can reduce the risk down to an acceptable level according to the document/article/standard Y (cite the necessary source). Or, for example, to mitigate the threat T2 we proposed to implement security controls SC2 based on our experience in Security.

## Web Application and Database Security (2 pages)

### Summary of assumptions and finding (1/2 pages)

Present key assumptions and the key results of the security risk assessment of the task “Web Application and Database Security”. Limit 1/2 page.

### Process used to analyze Web Application and Database Security Requirements (1+1/2 pages)

Example of the description for the application of CORAS method in section 3.1.2. or SecRAM method in section 3.1.3

## Example of the description for the application of SecRAM method Network and Infrastructural Security (2 pages)

### Summary of assumptions and finding (1/2 pages)

Present key assumptions and the key results of the security risk assessment of the task “Network and Infrastructural Security”. Limit 1/2 page.

### Process used to analyze Network and Infrastructural Security Requirements (1+1/2 pages)

Example of the description for the application of CORAS method in section 3.1.2. or SecRAM method in section 3.1.3

# ANNEX

An integral part of the report we attach the following documents:

1. Summary of Results (see file %Summary of results.xlsx%).
2. [for CORAS] Power Point slides (or PDF file) reporting the application of CORAS method (see file %CORAS-exercise.pptx% (or %CORAS-exercise.pdf%)).
3. [for SecRAM] Excel document reporting the application of SecRAM method (see file %SecRAM-exercise.xlsx%).

# REFERENCES

1. Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (The Hague, The Netherlands, April 01 - 06, 2000). CHI '00. ACM, New York, NY, 526-531. DOI= <http://doi.acm.org/10.1145/332040.332491>.
2. Tavel, P. 2007. *Modeling and Simulation Design*. AK Peters Ltd., Natick, MA.
3. Sannella, M. J. 1994. *Constraint Satisfaction and Debugging for Interactive User Interfaces*. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.
4. Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. *J. Mach. Learn. Res.* 3 (Mar. 2003), 1289-1305.
5. Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE. In *Proceedings of the 16th Annual ACM Symposium on User Interface Software and Technology* (Vancouver, Canada, November 02 - 05, 2003). UIST '03. ACM, New York, NY, 1-10. DOI= <http://doi.acm.org/10.1145/964696.964697>.

*This work has been done by the undersigned students and has not been copied or otherwise derived from the work of others not explicitly cited and quoted.*

*Signature of NAME SURNAME Signature of NAME SURNAME*