

Information Security

Risk analysis and related topics

Thesis and Project Proposals

NISlab
Gjøvik University College

Last updated: July 9, 2009

Contents

1	Analysing Security Decisions using Simulations	2
2	Cost and effectiveness of information security controls	2
3	A Comparison of Information Security Games	2
4	A New Information Security Game	2
5	Attack Defense Scenarios for Improving Information Security Understanding	2
6	Information Security Risk Management and Attacker/ Defender Mutual Knowledge	3
7	Low cost information security training and certification	3
8	Information Security Pragmatics	3
9	ISM simulation platform evaluation	3
10	Risk analysis for Privacy and Identity Management	4

1 Analysing Security Decisions using Simulations

The objective of information security management is to provide value to top management (and shareholders/governors). Thus, the information security manager needs to understand the goals of the organization and how his information security management decisions may influence these goals. The objective of this project is to investigate if the construction and evaluation of a simulation model can be a useful tool in improving this understanding.

2 Cost and effectiveness of information security controls

Information security management is about making sure that the appropriate countermeasures are implemented. In order to do this, the information security manager needs to know the effectiveness and the costs associated with these controls. The objective of this MSc project is to collect these cost and effectiveness data for a small number of controls. The project may obtain this data both through literature surveys, interviews and case studies.

3 A Comparison of Information Security Games

In the information security community, there is a growing interest in the use of computer game and edutainment technology. Recently, there has been developed several information security games (e.g. CyberCIEGE). The objective of this project is to evaluate a subset of these games with respect to their awareness and educational effect and their gameflow properties. Gameflow refers to the experience so gratifying that people are willing to play for the game for its own sake.

4 A New Information Security Game

Many consider information security to be boring. On the other hand - many people are addicted to computer games. The objective of this MSc project is to develop and evaluate an information security training or awareness game. The game can address social engineering, password creation and management or any other information security issue. The evaluation of the game should include qualitative or quantitative use experiments.

5 Attack Defense Scenarios for Improving Information Security Understanding

The notion of an 'attacker' is a key element in information security. Information security controls are often motivated by a concern for the possibility of something 'bad' happening.

The objective of this MSc project is to develop a library of attack-defense scenarios. The attack-defense scenarios should be made interactive and educational. The interactive scenarios should be evaluated with respect to their suitability for inclusion in an information security awareness and training programme.

6 Information Security Risk Management and Attacker/Defender Mutual Knowledge

In many cases, information security depends on actions performed by an intelligent adversary. Typically, adversary and defender may have some knowledge about the knowledge of the other party. Assuming that the parties are rational (in the usual economic sense), the state of knowledge will influence the actions made. The objective of this MSc project is to improve our understanding of how the state of mutual knowledge of attacker/defender influence the risk management process of a rational decision maker for important classes of attack/defence scenarios.

7 Low cost information security training and certification

There are several information security knowledge and skill certification schemes, e.g. CISM, SSCP, CAP, CSSLP, CISSP. In most cases, these certification schemes target the information security professional rather than the 'normal' computer user. Thus, there is a need for a 'lightweight' certification scheme, where the training and certification requires less than 8 hours of effort and both training and certification can be performed online. The objective of this MSc project is to develop such a training and certification package and evaluate its suitability for the identified target group.

8 Information Security Pragmatics

Most organizations carry out some form of Information Security Management (ISM). However, it is unclear what ISM activities are in fact carried out and how responsibilities are distributed. The objective of this MSc project proposal is to investigate how ISM is carried out in practice and what challenges management perceive in the area of ISM.

9 ISM simulation platform evaluation

There are several standard simulation platforms and languages. Many of these have a strong focus on physical/kinetic models. Cyber defence scenarios usually have a stronger focus on organizational, humans and IT components. The objective of the project is to

evaluate if standard simulation platforms and languages can be used to speed up the development of ISM training systems.

10 Risk analysis for Privacy and Identity Management

According to Westin, privacy can be interpreted as

the claim of individuals...to determine for themselves when, how and to what extent information about them is communicated to others.

The objective of this research is to better understand risks to privacy both from attacker and target perspectives. In particular, the intention is to investigate the dynamic nature of privacy risks through the application of game theory.

This MSc project will investigate aspects of risks relating to privacy and identity management. In particular, the MSc project should investigate how alternative identity management approaches will influence the risks to privacy. This MSc project is part of a larger project (PETWeb II) funded by the Research Council of Norway (NFR).