Security Evaluation Supported by Information Security Mechanisms

Jakub Breier

Physical Analysis and Cryptographic Engineering
Temasek Laboratories@NTU
Nanyang Technological University
Singapore

25 June 2014

'Security is a business issue, not a technical issue.'[1]

[1] Glaessner, T., Kellerman, T., and V. McNevin: Electronic Safety and Soundness: Securing Finance in a New Age. 2004.

Goals of security evaluation:

- Determine which security mechanisms are implemented correctly.
- Periodically check the quality of the mechanisms.
- Find the most appropriate mechanisms with respect to price and effect - evaluate the efficiency of security investments.

Security Evaluation

There are several security frameworks, which can be used to quantify the effectiveness of security controls in an organization:

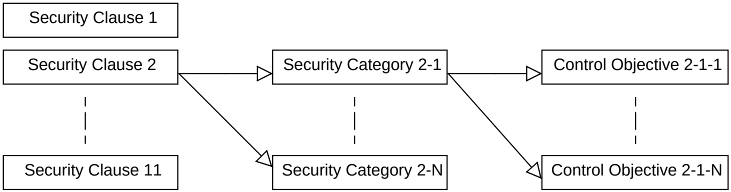
- Control Objectives for Information Technology (COBIT).
- ISO/IEC 27002 (ISO/IEC 17799) Code of practice for information security management.
- Information Technology Infrastructure Library (ITIL).
- US NIST SP 800 Series.

ISO/IEC 27002:2005

It provides best practice recommendations on information security management in order to initiation, implementation and maintaining Information Security Management Systems (ISMS).
The main security clauses are:

- Security Policy
- Organizing Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

ISO/IEC 27002 Structure



ISO/IEC 27002:2005 Standard structure:

- 11 Security clauses
- 39 Security categories
- 133 Control objectives

Security Evaluation and ISO/IEC 27002

The process of security evaluation in accordance to the standard is following:

- Security analyst picks the right control objectives from the ISO/IEC 27002.
- He goes through all of them and checks whether they are implemented or not.
- If the implementation quality is insufficient or the security mechanisms required to fulfill the objective is not implemented at all, he constitutes recommendations based on his experience.

Problems with this Approach

- Qualitative measurement scale
  - Inexplicit values: low-medium-high risk.
- Subjectivity
  - Result is influenced by analyst's knowledge and experience.

Main Goals

Main motivation of our work was to:

- Examine the compliance with the ISO/IEC 27002 standard.
- Minimize the subjective influences - usage of quantitative methods to determine the importance of particular security mechanisms.
- Ease of use - the implementation quality can be easily assessed and the score should be viewable in different levels of detail.

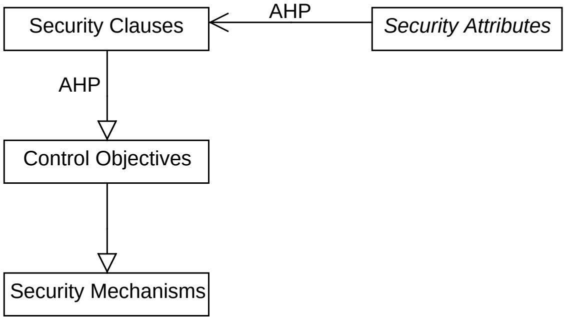
The final result - security evaluation system based on the score of security mechanisms.

Contributions

To reach the goals we have made following:

- Mapping of security mechanisms to control objectives - there are 357 mechanisms, representing the lowest level of hierarchy.
- Usage of methods that can determine importance of elements in the model.
- Usage of security statistics so that the evaluation model can reflect the current security issues in a real world.

Methods in Hierachy 1/3



Analytic Hierarchy Process

Analytic Hierarchy Process (AHP) is a technique of organizing and analyzing complex decisions. Decision factors are arranged in a hierachic structure, splitted into overall goal, criteria, subcriteria and alternatives in successive levels.

- We make the judgements upon the lowest level elements of the hierarchy in the form of paired comparisons.
- Following the hierarchical structure, we compare them on a single property, without concern about other properties.
- The comparison is based on verbal judgements (equal, moderately more, strongly more, very strongly more, extremely more), expressed in discrete values from 1 to 9.

Availability Matrix

$$
\begin{array}{l}
\text{Availability} \\
SP \\ OIS \\ AM \\ HRS \\ PES \\ COM \\ AC \\ ISADM \\ ISIM \\ BCM \\ CMP
\end{array}
\begin{array}{c}
\begin{array}{ccccccccccc}
SP & OIS & AM & HRS & PES & COM & AC & ISADM & ISIM & BCM & CMP
\end{array} \\
\begin{pmatrix}
1/1 & 2/1 & 1/5 & 9/1 & 1/5 & 1/3 & 5/1 & 5/1 & 7/1 & 1/7 & 3/1 \\
1/2 & 1/1 & 1/7 & 9/1 & 1/7 & 1/6 & 2/1 & 3/1 & 7/1 & 1/7 & 2/1 \\
5/1 & 7/1 & 1/1 & 9/1 & 3/1 & 2/1 & 7/1 & 7/1 & 9/1 & 2/1 & 5/1 \\
1/9 & 1/9 & 1/9 & 1/1 & 1/9 & 1/7 & 1/3 & 1/2 & 1/2 & 1/9 & 1/7 \\
5/1 & 7/1 & 1/3 & 9/1 & 1/1 & 2/1 & 5/1 & 5/1 & 9/1 & 2/1 & 5/1 \\
3/1 & 6/1 & 1/2 & 7/1 & 1/2 & 1/1 & 5/1 & 5/1 & 7/1 & 1/2 & 5/1 \\
1/5 & 1/2 & 1/7 & 3/1 & 1/5 & 1/5 & 1/1 & 1/3 & 2/1 & 1/8 & 2/1 \\
1/5 & 1/3 & 1/7 & 2/1 & 1/5 & 1/5 & 3/1 & 1/1 & 7/1 & 1/6 & 4/1 \\
1/7 & 1/7 & 1/9 & 2/1 & 1/9 & 1/7 & 1/2 & 1/7 & 1/1 & 1/8 & 1/3 \\
7/1 & 7/1 & 1/2 & 9/1 & 1/2 & 2/1 & 8/1 & 6/1 & 8/1 & 1/1 & 8/1 \\
1/3 & 1/2 & 1/5 & 7/1 & 1/5 & 1/5 & 1/2 & 1/4 & 3/1 & 1/8 & 1/1
\end{pmatrix}
\end{array}
$$

$$
\begin{array}{c}
\begin{array}{ccccccccccc}
SP & OIS & AM & HRS & PES & COM & AC & ISADM & ISIM & BCM & CMP
\end{array} \\
W_{ava}^{T} = \begin{pmatrix} 0.077 & 0.052 & 0.236 & 0.012 & 0.195 & 0.129 & 0.026 & 0.043 & 0.020 & 0.192 & 0.029 \end{pmatrix}
\end{array}
$$

Asset Management

Control objective	Security mechanism	ID
Inventory of assets (IA)	Identification of all assets with their level of importance and information about the asset	M1
	Identification of ownership and information classification for each asset - with the level of protection	M2
	Ensuring the integrity of information - hashing	M3
	Ensuring the availability of information - backuping, physical and environmental security, redundancy	M4
Ownership of assets (OA)	Implementation of access control policies (DAC, MAC, RBAC)	M5
	Implementation of non-repudiability mechanisms - operating system level, digital signatures	M6
	Implementation of accounting mechanisms - operating system level, authentication servers (TACACS, RADIUS), network logs	M7
	Implementation of authentication mechanisms - authentication servers (TACACS, RADIUS), tokens, biometrics, passwords	M8
Acceptable use of assets (AUA)	Identification of rules for usage of electronic devices and computer networks	M9
Classification guidelines (CG)	Determination of classification levels and implementation of confidentiality mechanisms - cryptography (securing data storages and data transmissions), steganography	M10
Information labeling and handling (ILH)	Definition of policies for labeling classified information - physical and electronic labels	M11

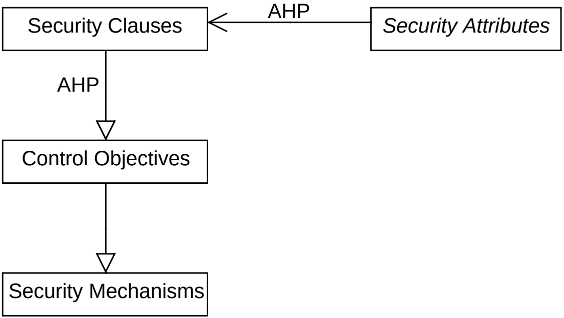
Asset Management Matrix

Below is the Asset management weight matrix with the corresponding weight vector:

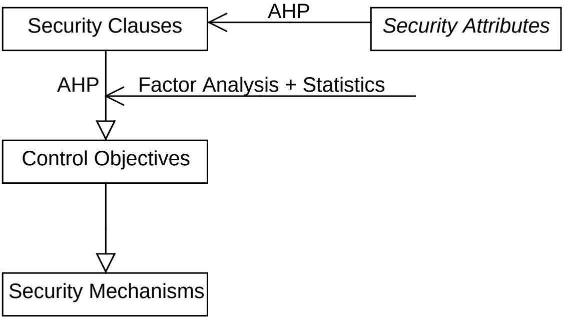
$$
\begin{array}{ll}
\text{Asset management} & \begin{array}{ccccc} \quad IA & \quad OA & \quad AUA & \quad CG & \quad ILH \end{array} \\
\begin{array}{l} IA \\ OA \\ AUA \\ CG \\ ILH \end{array} & \begin{pmatrix} 1/1 & 9/1 & 7/1 & 9/1 & 9/1 \\ 1/9 & 1/1 & 1/3 & 1/1 & 1/1 \\ 1/7 & 3/1 & 1/1 & 3/1 & 3/1 \\ 1/9 & 1/1 & 1/3 & 1/1 & 1/1 \\ 1/9 & 1/1 & 1/3 & 1/1 & 1/1 \end{pmatrix}
\end{array}
$$

$$
\begin{array}{ll}
 & \begin{array}{ccccc} IA & OA & AUA & CG & ILH \end{array} \\
W_{AM}^{T} = & \begin{pmatrix} 0.664 & 0.060 & 0.156 & 0.060 & 0.060 \end{pmatrix}
\end{array}
$$

Methods in Hierachy 2/3



Methods in Hierachy 2/3



Factor Analysis

Factor analysis (FA) is a statistical method used to describe variability among observed, correlated variables in terms of a potentially lower number of unobserved variables called factors.

- The observed variables are modeled as linear combinations of the potential factors.
- FA can be used to reduce the redundant information contained in several correlated variables.
- We will use it to reveal the correlations among control objectives and to insert dependencies in our measurement model.

Control Objectives for Factor Analysis

Table: One control objective from each security clause.

Information security policy document	CO_1
Confidentiality agreements	CO_2
Inventory of assets	CO_3
Information security awareness, education, and training	CO_4
Physical entry controls	CO_5
Disposal of media	CO_6
User password management	CO_7
Input data validation	CO_8
Reporting information security events	CO_9
Business continuity and risk assessment	CO_{10}
Protection of organizational records	CO_{11}

Control Objectives and Security Threats

Table: Control objectives' protection against Top 10 security threats [2].

	CO_1	CO_2	CO_3	CO_4	CO_5	CO_6	CO_7	CO_8	CO_9	CO_{11}
Keylogger/Form-grabber/Spyware	7	1	1	7	3	1	5	5	5	3
Exploitation of default or guessable credentials	7	3	1	8	3	1	9	1	4	3
Use of stolen login credentials	3	1	1	5	7	3	7	1	5	5
Send data to external site/entity	5	1	1	7	3	3	5	1	3	5
Brute force and dictionary attacks	7	1	3	9	5	3	9	1	5	5
Backdoor	5	3	1	7	5	1	5	5	5	3
Exploitation of backdoor or command and control channel	5	1	1	5	3	1	5	3	5	7
Disable or interfere with security controls	7	3	1	7	8	1	5	2	5	5
Tampering	8	3	1	8	3	1	1	1	5	3
Exploitation of insufficient authentication	7	3	1	8	7	1	5	1	3	5

[2] W. Baker, A. Hutton, D. Hylender, J. Pamula, Ch. Porter, and M. Spitler. Data Breach Investigations Report 2012. Technical report, Verizon, 2012.

Factor Analysis

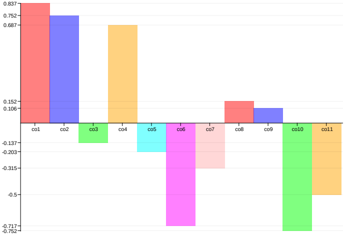
$$
\begin{array}{cc}
 & \begin{matrix} CO_1 & CO_2 & CO_3 & CO_4 & CO_5 & CO_6 & CO_7 & CO_8 & CO_9 & CO_{10} & CO_{11} \end{matrix} \\
\begin{matrix} CO_1 \\ CO_2 \\ CO_3 \\ CO_4 \\ CO_5 \\ CO_6 \\ CO_7 \\ CO_8 \\ CO_9 \\ CO_{10} \\ CO_{11} \end{matrix} &
\begin{pmatrix}
1 & 0.484 & 0.208 & 0.788 & -0.171 & -0.498 & -0.208 & -0.092 & -0.043 & -0.715 & -0.400 \\
0.484 & 1 & -0.333 & 0.410 & 0.263 & -0.655 & -0.273 & -0.063 & -0.124 & -0.333 & -0.469 \\
0.208 & -0.333 & 1 & 0.519 & 0.053 & 0.509 & 0.515 & -0.232 & 0.207 & -0.111 & 0.156 \\
0.788 & 0.410 & 0.519 & 1 & -0.073 & -0.054 & 0.127 & -0.265 & -0.254 & -0.573 & -0.473 \\
-0.171 & 0.263 & 0.053 & -0.073 & 1 & 0.103 & 0.139 & -0.190 & 0.033 & 0.404 & 0.255 \\
-0.498 & -0.655 & 0.509 & -0.054 & 0.103 & 1 & 0.417 & -0.456 & -0.135 & 0.509 & 0.307 \\
-0.208 & -0.273 & 0.515 & 0.127 & 0.139 & 0.417 & 1 & -0.190 & -0.056 & 0.212 & 0.128 \\
-0.092 & -0.063 & -0.232 & -0.265 & -0.190 & -0.456 & -0.190 & 1 & 0.432 & -0.232 & -0.267 \\
-0.043 & -0.124 & 0.207 & -0.254 & 0.033 & -0.135 & -0.056 & 0.432 & 1 & 0.207 & -0.097 \\
-0.715 & -0.333 & -0.111 & -0.573 & 0.404 & 0.509 & 0.212 & -0.232 & 0.207 & 1 & 0.156 \\
-0.400 & -0.469 & 0.156 & -0.473 & 0.255 & 0.307 & 0.128 & -0.267 & -0.097 & 0.156 & 1
\end{pmatrix}
\end{array}
$$

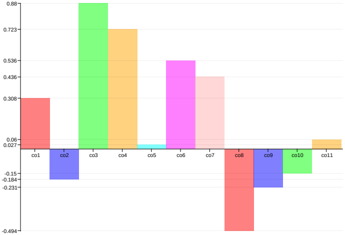
Factors 1/2

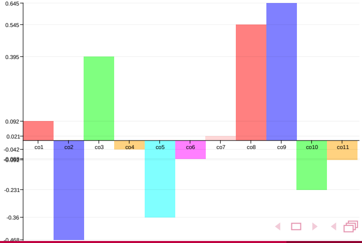
Table: Factors.

	F_1	F_2	F_3
CO_1	0.858	0.313	0.048
CO_2	0.690	-0.145	-0.434
CO_3	-0.128	0.851	0.436
CO_4	0.693	0.720	-0.023
CO_5	-0.195	0.040	-0.303
CO_6	-0.727	0.540	-0.027
CO_7	-0.317	0.432	0.082
CO_8	0.176	-0.573	0.671
CO_9	-0.081	-0.188	0.413
CO_{10}	-0.720	-0.121	-0.218
CO_{11}	-0.506	0.059	-0.073

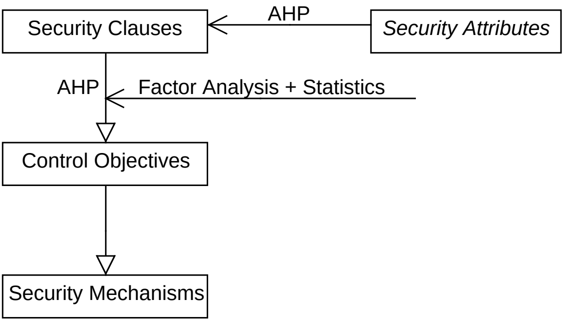
Factors 2/2


0.837
0.752
0.687
0.152
0.106
-0.137
-0.203
-0.315
-0.5
-0.717
-0.752
co1
co2
co3
co4
co5
co6
co7
co8
co9
co10
co11

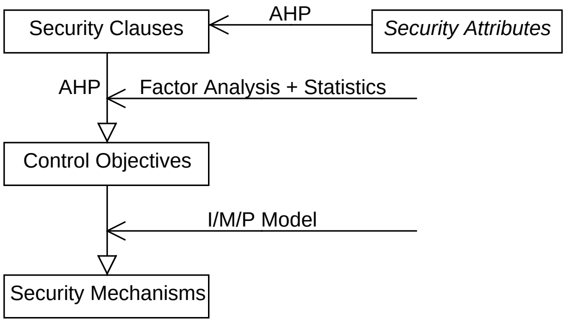

0.88
0.723
0.536
0.436
0.308
0.06
0.027
-0.15
-0.184
-0.231
-0.494
co1
co2
co3
co4
co5
co6
co7
co8
co9
co10
co11


0.645
0.545
0.395
0.092
0.021
-0.042
-0.231
-0.36
co1
co2
co3
co4
co5
co6
co7
co8
co9
co10
co11

Methods in Hierachy 3/3



Methods in Hierachy 3/3



I/M/P Model 1/3

- Llanso[3] introduces an approach for selecting and prioritizing security controls from NIST 800-30.
- He computes weights of the controls, using three component weights - prevention, detection and response (P/D/R) against an attack.
- We will use implementation, maintenance and policy (I/M/P) components.

[3] T. Llanso. Ciam: A data-driven approach for selecting and prioritizing security controls. In Systems Conference (SysCon), 2012 IEEE International

I/M/P Model 2/3

Raw weighting:

$$RawWeighting_i = wI_i.owI_i + wM_i.owM_i + wP_i.owP_i \qquad (1)$$

where overall weightings have values
$owI_i = 0.6, owM_i = 0.20, owP_i = 0.20.$

Relative weighting:

$$RelativeWeighting_i = \frac{RawWeighting_i}{\sum_{j=1}^{n} RawWeighting_j} \qquad (2)$$

I/M/P Model 3/3

Table: Control objective: Controls against malicious code.

Security Mechanism	I	M	P	RW
Implementing operating system policies prohibiting the use of unauthorized software, downloading unsigned executable files and working with other than data files on workstations without privileges.	9	5	7	**0.244**
Implementing strong account policies with separated privileges and clear accountability and non-repudiability.	7	3	9	**0.206**
Deployment of antivirus software on each system with the real-time check of unwanted code and periodical update of this software.	9	9	2	**0.238**
Ensuring that installed programs are up to date.	3	9	7	**0.156**
Providing business continuity plan - backuping and version management.	3	7	9	**0.156**

Security Mechanisms' Score

Level	Score	Description
0	0.0	Not implemented
1	0.2	Implemented with serious limitations
2	0.4	Implemented with minor unknown limitations
3	0.6	Implemented with known limitations
4	0.8	Implemented well, not tested in a real environment
5	1.0	Implemented well, tested and verified in a real environment

Control Objective Evaluation 1/2

$$S_{CO_i} = \sum_{j=1}^{n} S_{M_j} \times RW_{M_j}$$

Where:

- S_{M_j} is the security mechanism's score.
- RW_{M_j} is the security mechanism's weight.

Control Objective Evaluation 2/2

$$FinalScore = RW_{CO_i} * \prod_{j=1}^{n} \left(S_{CO_i} + \frac{S_{CO_j} * COR_{ij}}{1 + COR_{ij}} \right) \tag{3}$$

- RW_{CO_i} is the weight of control objective i, obtained by using AHP.
- S_{CO_i} is the score of control objective i.
- S_{CO_j} is the score of control objective j, correlated with i.
- COR_{ij} is the correlation between i and j.

Conclusions

- The proposed model evaluates the security state in accordance to ISO/IEC 27002 standard with respect to the score of security mechanisms.
- The model implementation is easy to use and flexible.
- To test the methodology we conducted a study on a medium-sized IT company, using a prototype application implementing our methods.

Thank you for your interest!

Any questions?