An approach to standardizing security analysis methods for virtual systems

ANN FRISINGER, LOUISE YNGSTROM
The Royal Institute of Technology
Department of Teleinformatics
Email: afri@it.kth.se
Phone: +46-8-7931321
Mobile: +46-70-7931321

The Royal Institute of Technology/Stockholm University
Department of Computer and Systems Sciences
Email: louise@dsv.su.se
Phone: +46-8-161610
Fax: +46-8-7039025

Key words: Information security, security analysis, risk analysis, method, virtual system, standard, networked education, NED-ify, X-ify.

Abstract: As the use of global networking grows and information systems change characteristics, becoming open, distributed, and integrating communication, computing, and media technology, there is a need for security analysis methods that can handle the new environment with new actors, new rules, short system development and life times, and also new ways of using the systems. In addition, there is a need for methods that can be applied already at an early system development stage. We will in this paper present an approach to standardize the security analysis method and show how this method can be used to evaluate the security in a virtual target system.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35575-7_19

J. H. P. Eloff et al. (eds.), *Information Security Management & Small Systems Security*

1. INTRODUCTION

Risk analysis, RA, is basic to all security, yet it continues to be rated as not precise, give a false sense of precision, not updated [PFL97], tedious, subjective, inconsistent, and useless [JAC96]. There are many reasons to the negative outlooks on RA; quantifying risks and costs for incidents is problematic since the forecast should be based on prior experiences and statistics [HAM96] and it is well-known there is an under-reporting of incidents in the security arena. There are no reliable industry wide statistics on which to base the risk analysis [SAR87, SAR91, BAS93] but most recent studies, for instance [AUD94, AUD98, BJO97, BJO98, GLO97, HIN98, POW98, RPS94, RRV97, ÖCB94] show a general increase in for instance hacking, fraud, and virus incidents. Few studies, if any, apply their statistics to specific environments or types of applications, and the systematic handling of multidimensional data (e.g., actors, purposes for attacks, vulnerabilities, threats, assets, user requirements, and costs) is problematic. Howard [HOW97] tried to handle this problem through a taxonomy, with meager result. It was suggested by [SOL97] to exchange RA by a security baseline approach similar to the baseline approach defined by BS7799 [BS7799]. However, instead of letting RA be the basic for choice of baseline and security controls, business requirements will determine security requirements, security policy and ultimately the security controls from BS 7799.

Our view is slightly different: we approach the environment of global networks with open distributed systems, where organizations offer services which are some specific integration of communications, computing and media; in our case a Networked Education System, and we need to have an opinionon how to safeguard this "system", called NED. NED operates in a global space, parts of NED areowned by - thus can be controlled by - the education system, but most parts are shared globally. Moreover, NED is only a virtual system. Our NED will operate in a general distributed environment through its "business processes" described in a NED conceptual model.

Our aim is to provide a generic systematic learning method for performing (successive) security evaluations of a virtual system in an open distributed environment. We will test our method on NED, but the method should be general enough to be able to handle other types of virtual systems, forinstance X. In the test of the NED, the general evaluation method is adjusted by "NED-ifying" our criteria: These "-ifys" will serve as a base for analyzing general "ify" parameters useful also for other, virtual or real, application types in open distributed environments.

This paper is a summary of the first part of the research [FRI98] and is describing:

1. An approach to standardize the security analysis method for virtual as well as real systems. How to adjust, "X-ify", the quantification of asset attractiveness, vulnerabilities, and costs for incidents in the risk analysis.
2. How this method was used to evaluate the security in the virtual target system NED, i.e. how to adjust, "NED-ify", the quantification of asset attractiveness, vulnerabilities, and costs for incidents in the risk analysis for the target system NED.

2. AN APPROACH TO STANDARDIZE THE SECURITY ANALYSIS METHOD

The following description gives an overview of the standard method for how to perform an adjusted, or "X-ified", security analysis in a virtual or real system, see figure 1.

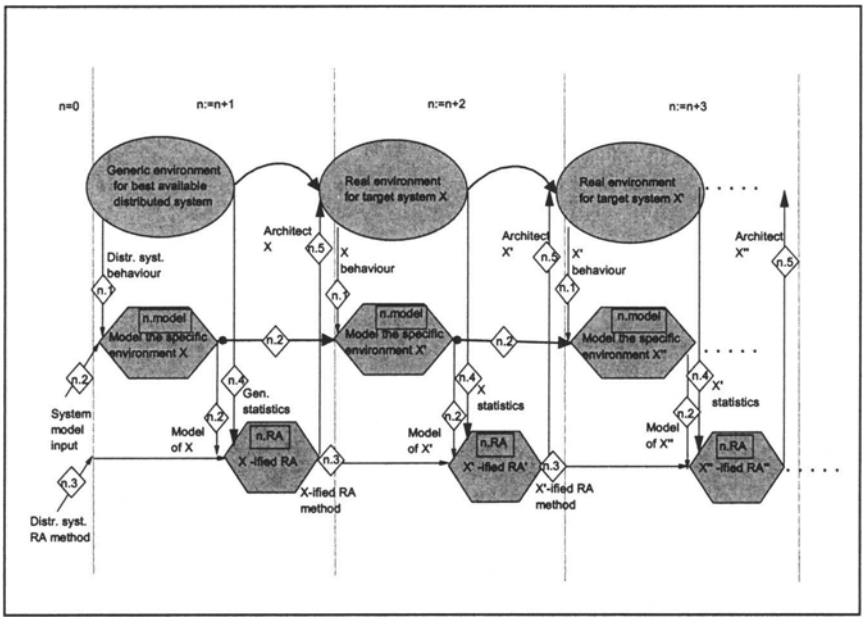

Figure 1. Generic method for performing an adjusted security analysis

2.1 Process n.model -- Model the specific environment X

- Process input:
  - (n-1).2: ***The best available input to be used to model the specific environment X.*** If system X exists and system X has been modeled

before, this is then the prior model, otherwise this may be information based on interviews with users and designers of components of the target system X, and studies of X related work
    - n.1: ***The best available input on X system behavior.*** If system X exists, this is then the X behavior in its environment, otherwise this may be input from another similar system.
- Process description: Model the specific environment X
    - When evaluating what should be done in order to provide security in a distributed information system, a starting point is to understand the system, i.e. what it consists of, its purpose, how it works, how it works in its environment, and how it works without any extra security controls.
    - A model of the specific environment provides an understanding of the target system. The system can be modeled by specifying the business process for the target system together with a conceptual model which describes all the objects involved in the process.
- Process output:
    - n.2: A model of the specific environment X

2.2 Process n.RA -- X-ified RA (risk analysis)

- Process input:
    - n.2: A model of specific environment X
    - (n-1).3: A risk analysis, RA, method. If system X has been evaluated before, this is the RA method (and taxonomy if applicable) that was used at that time, otherwise use the best available method.
    - n.4: Best available statistics to be used in the risk analysis. If system X already exists, use statistics from system X, otherwise use the best available statistics from a similar system.
- Process description: X-ified RA (risk analysis)
    - **Develop/redevelop risk analysis method.** If system X has been analyzed before, evaluate the risk analysis method (and taxonomy if applicable) that was used for step n-1. If needed, update the method and the taxonomy for step n. Document any changes in the method so that system and method evolution can be followed up.
    - **Understand the system environment and identify target system assets.** Let IT assets together with other assets related to goodwill, customer satisfaction, and trust (immaterial assets) be the base when making the security analysis.
    - Define the system **security assumptions** so that the way the system should be comprehended is well defined and the same for all viewers.

- Examine who are the **actors**, authorized and non-authorized, in the system.
- Look at possible **purposes for attacks**.
- Describe what are the **vulnerabilities** to which the system is prone.
- Look at **users' security requirements**.
- Thereafter, the risks should be identified and valued. This will be achieved in the **risk analysis**. The risk analysis should be based on statistics that may or may not come from the X system. If it comes from the X-system, it may not perfectly match the current X environment and situation. Therefore, the values for attractiveness of assets, system vulnerabilities, and costs for incidents are "X-ified" so that they suit the current environment. See more about the "X-ification" below where we describe the security analysis of NED.

- Process output:
  - n.3: ***The RA, risk analysis, method*** that was used in step n
  - n.5: ***Requirements for building/updating the security architecture of X.*** A prioritized set of security requirements will be found after completing the risk analysis. For each asset in storage, transfer, process, a security requirement expressed for confidentiality, integrity, and availability will be provided. From the list, it is possible to pick the assets (in storage, transfer, or process) with a "high security value" in the columns of confidentiality, integrity, availability. Those are the assets that we will focus on first when building a security architecture and when specifying a security policy for X (in n+1).

3. SECURITY ANALYSIS ON TARGET SYSTEM NED

The following is a description of how the method was used to perform an initial security analysis, step n=1, for the virtual target system NED, and how the "best available statistics" was adjusted, or "NED-ified". See figure 2 below.

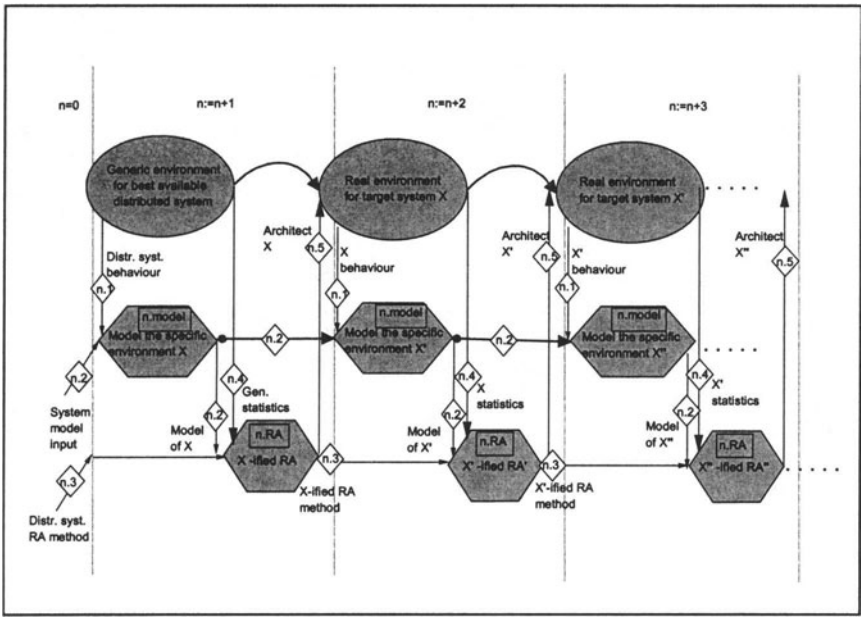

Figure 2. Method for performing an adjusted security analysis on target system NED

3.1 Process 1.model-- Model the specific environment NED

- Process input:
  - 0.2: ***The best available input to model the specific environment NED:*** The best available input for modeling the specific environment NED was based on interviews with users and designers of components of the target system NED, and on studies of NED related work
  - 1.1: ***The best available input on NED system behavior:*** NED did not exist in its whole. Although NED could be built from a variety of components for which the technology already existed, but had never been integrated into one complete cooperating system. The best available input on system behavior was therefore based on studies of other distributed systems.
- Process description: Model the specific environment NED
  - The NED process was specified together with a conceptual model which described all the objects involved in the process. The process and the conceptual model could be described after interviewing users and designers of components of the NED target system and by studying NED related work.
- Process output:

- 1.2: ***A model of the specific environment NED:*** The NED specific model, consisting of a process and a conceptual model.

3.2 Process n.RA -- X -ified RA (risk analysis)

- Process input
  - 1.2: ***The NED model,*** i.e. the process and conceptual model, of the specific environment NED
  - 0.3: ***Studies of risk analysis related work.*** 1.4: ***Best available statistics to be used in the risk analysis.*** Statistics and taxonomy published by R. Baskerville comprising figures calculated from 147 distinct reported incidents that damaged organizations and appeared to arise from the use of computer-based systems during a two-year period (1992-1993) [BAS96].
- Process description
  - **Develop/redevelop risk analysis method.** The risk analysis method presented in this paper was defined as a result of studies of related work.
  - **Understand the system environment and identify target system assets.** A set of assets was found by studying the model of NED, i.e. the process and conceptual model.
  - Define the system **security assumptions** with basic system protections for the virtual system NED and look at vulnerability aspects. The initial system resistance was described.
  - Examine who are the **actors**, authorized and non-authorized, in the system.
  - Look at possible **purposes for attacks**. The attacks can be *accidental* or *deliberate*. The motives for deliberate attacks can be classified into three main categories; *vandalism*, *espionage*, and *fraud*.
  - Describe what are the **vulnerabilities** to which the system is prone. Consider how these vulnerabilities could be exploited, what are the **threats**, and what different kinds of **attacks** and **hazards** are possible. We are classifying the hazards into **deliberate** respective **accidental** hazards. Furthermore we divide the deliberate hazards into *physical*, *falsification*, *malicious software*, and *cracking*. The accidental hazards are divided into *catastrophe* and *error*.
  - Look at **users' security requirements**. Understanding users' needs is important when deciding what threats are really worth to consider from the users' point of view.
  - Thereafter, identify and value the risks. This is achieved in the **risk analysis**, see a description of the risk analysis method below. The risk analysis identifies and value risks by use of linguistic variables, fuzzy

set theory, compatibility functions, and is using best available statistics that is adjusted to be used for the system in focus. The NED-ified cost-values for incidents can be set after performing a business value assessment.

- Process output:
  - 1.3: ***A risk analysis method.*** The risk analysis method described in this paper, together with a taxonomy for categorizing incidents.
  - 1.5: ***Requirements for building the initial NED security architecture.*** A prioritized set of **security requirements** was found after completing the risk analysis. For each asset in storage, transfer, and process, a security requirement expressed for confidentiality, integrity, and availability was provided, see example in table 1.

Table 1. Sample from security requirements table

Security requirements for:	**Confidentiality**	**Integrity**	**Availability**
CourseDescr.in storage	Open	Normal	Normal
CourseDescr.in transfer	Open	Normal	Normal
CourseDescr.in process	Open	Normal	Normal
Course Syllabus in storage	Internal Use Only	Normal	Low
Course Syllabus in storage	Internal Use Only	Normal	Low
etc. . .	. . .	. . .	. . .

From this list, it is possible to pick the assets, in storage, in transfer, or in process with a "high security value" in the columns of confidentiality, integrity, availability. Those are the assets that we will focus on first when building a security architecture and when specifying a security policy for NED. This table function as a guideline during that work.

4. NED-IFIED RISK ANALYSIS

In the initial risk analysis of NED, the forecast was based on statistics published by R. Baskerville. The figures were calculated from 147 distinct reported incidents that damaged organizations and appeared to arise from the use of computer-based systems during a two-year period (1992-1993) [BAS96]. This information was coming from different organizations within the different sectors. We could not be sure the statistical figures could be correctly applied to NED with a successful result. We therefore "NED-ified" it.

The risk analysis was performed according to the method described below. For each asset, the level-of-injury, expressed by a linguistic value from the set {no harm, harm, serious harm, very serious harm}, was calculated according to formula 1.

(1) Level-of-Injury(attack on asset) = P(attack on asset) $\otimes^1$ Cost(attack on asset)

Where:

- P(attack on asset) is the probability for an incident to occur.
- The probability is expressed by a linguistic value from the set {none, low, medium, high}.
- Cost(attack on asset) is the cost when the incident occurred.
- The cost is expressed by a linguistic value from the set {none, low, medium, high}.
- The $\otimes^1$ operation gives the product of P(attack on asset) and Cost(attack on asset), see Table 2.

Table 2. The Cost() $\otimes^1$ P() operation

Cost()→ P() ↓	**none**	**low**	**medium**	**high**
none	no harm	no harm	no harm	no harm
low	no harm	harm	serious harm	serious harm
medium	no harm	harm	serious harm	very serious harm
high	no harm	serious harm	serious harm	very serious harm

The adjusted, or NED-ified, probability for attack on an asset was calculated by use of formula 2:

(2) P(attack on asset) = {Attractiveness(asset) $\otimes^2$ Vulnerability(storage/transfer/process)} $\otimes^3$ P(hazard)

Where:

- Attractiveness(asset) is an adjusted (NEDified), measure of how attractive the asset is to an attacker.
- The attractiveness is expressed by a linguistic value for the set {none, low, medium, high}.
- Vulnerability(storage/transfer/process) is a "NEDified" measure of how vulnerable the asset is in different media; that is storage, transfer, process; and in the aspect of confidentiality, integrity, and availability; as seen from the system owning organization's perspective. The vulnerability is expressed by a linguistic value for the set {none, low, medium, high}

- P(hazard) is the probability for a hazard using best available incident statistics for thesystem. For NED, statistics presented by R.Baskerville was found as best available [BAS96].
- The $\otimes^2$ calculates the product of attractiveness and vulnerability. See table 3.

Table 3. The attractiveness vulnerabilty operation

Vulnerability() → Attractiveness() ↓	none	low	medium	high
none	none	none	none	none
low	none	low	low	medium
medium	none	medium	medium	high
high	none	medium	high	high

The $\otimes^3$ operation calculates the product of attractiveness and vulnerability and p(hazard). The figures used were calculated with help of fuzzy set theory, and compatibility functions, see table 4 for the NEDified operation.

Table 4. Example of the$\otimes^3$ NEDified operation

Attractiveness() ⊗3 Vulnerability()	**P(attack on asset); numerical value**
none	P(*hazard)* x *0*
low	P(*hazard)* x *(π+4)/48*
medium	P(*hazard)* x *0.5*
high	P(*hazard)* x 1- (π+4 /48)

The outcome of the operation is now a numerical probability value per asset in storage/transfer/process and for the requirements confidentiality/integrity/availability. Numerical values are summarized and the converted back to a linguistic value by use of the conversion table 5.

Table 5. NED conversion to linguistic value

P(attack on asset); range 0..100	P(attack on asset); range none..high
0	none
1-33	low
34-66	medium
67-100	high

5. CONCLUSIONS AND FURTHER WORK

In this paper we presented an approach to standardize the security analysis method for virtual as well as real systems. This method was used to evaluate the security in the virtual target system NED. In the risk analysis

the quantification of assets attractiveness, vulnerabilities, and costs for incidents were adjusted, "NED-ified" or "X-ified", to fit the system in focus.

After the first round of study we can create the initial generation of security protection system. This should be seen as a start value, as good as any. When we in the next step will show how the method can be performed in steps with n>1 for security analysis in the real target system NED, we have a method to start with. The standardized method will facilitate reevaluations. Although the input values of the method parameters, e.g. the adjusted statistics, will vary, the first analysis provides values to compare with and learn from. This enables systems to adjust to current reality over time where protecting system measures that are hit by many incidents could be replaced by new generations of protecting measures (this is excluding the event of system hit by a very severe incident with a high-level of injury, which will have impact on most of the protecting measures). The protecting measures that are best suited to solve the problem will be used in the next version of the system.

Future generations of security evaluations and risk analysis must find new ways of dealing with masses of complicated data in the quest for patterns. Neural networks, artificial intelligence, and genetic algorithms may allow us to do this [MIL95].

Many other fields, e.g. economy, physics, biology, geology, and metrology, has started to develop methods based on these new techniques and drawing a parallel from the security risk analysis field to those other sectors is attempting.

References

[AUD94] Audit Commission: Opportunity Makes a Thief. An Analysis of Computer Abuse, Audit Commission national report 1994

[AUD98] Audit Commission: Gost in the Machine, An analysis of IT Fraud and Abuse (Update), 1998 ISBN 186240 056 3

[BAS93] Richard Baskerville, 'Information Systems Security Design Methods: Implications for Information Systems Development', 1993, ACM Computing Surveys, Vol.25, No.4, pp.375-414.

[BAS96] Richard Baskerville, 'A taxonomy for Analysing Hazards to Information Systems' published on pp.167-176 in 'Information Systems Security, facing the information society of the 21st century' by Sokratis K.Katsikas and Dimitris Gritzalis, Chapman & Hall, ISBN 0-412-78120-4.

[BJO97] Ernest&Young: Björck Fredrik, 1997 Information Security Survey - Sweden 1997, Stockholm, Ernest&Young

[BJO98] Ernest&Young: Björck Fredrik, 1998 Information Security Survey - Sweden 1998, Stockholm, Ernest&Young

[GLO97] Global Information Security Survey 1997, Ernest&Young, Cleveland 1997

[BS7799] BS7799: Code of Practice for Information Security Management, British Standards Institute 1995

[FRI98] Ann Frisinger, 'Security in the Networked Education Process', 15 June 1988, TRITA-IT AVH 98:02, ISSN 1103-534X, ISRN KTH/AVH--98/02--SE.

[HIN98] Stephen Hinde, 'Recent Security Surveys, Computers & Security', 17(1998)207-210

[HOW97] John D. Howard, 'An Analysis Of Security Incidents On The Internet', Ph.D. Dissertation, Carnegie Mellon University, April 7, 1997, URL: http://www.cert.org/research/JHThesis.

[HAM96] Gustaf Hamilton, 'Risk Management 2000', Studentlitteratur 1996, ISBN 91-44-00082-0.

[JAC96] Jacobsson 1996 Jacobson R.V. CORA Cost-of-Risk Analysis, IFIP'96 WG11.2 Samos Greece

[MIL95] Gregory J. Millman, 'Around the World on a Trillion Dollars a Day', Transworld publishers ltd., British Library 0593039653, 1995

[PFL97] Charles P Pfleeger, 'Security in Computing', Prentice Hall, 2nd ed, 1997

[POW98] Richard Power,1998 CSI/FBI Computer Crime and Security Survey. Computer Security Journal XIV, no 3:31-42

[RPS94] RPS: Datorrelaterad brottslighet. Uppföljning av en enkätundersökning hos polismyndigheterna, RPS rapport 1994:13

[RRV97] Datorrelaterade missbruk och brott - en kartläggning gjord av Effektivitetsrevisionen, RRV 1997:33

[SAR87] Saari, J., 'Computer Crime: Numbers lie. Comput.Sec. 6, 2, 111-117', 1987.

[SAR91] Saari, J., 'Top management challenge: From quantitative guesses to prudent baseline of security.' In Proceedings of the 1991 IFIP Computer Security Conference (Brighton, England, May). IFIP, Geneva, Switzerland, 295-300.

[SOL97] von Solms 97 R. Von Solms, 'Can security Baselines replace Risk Analysis' in Proceedings of the IFIP TC1113th International conference on Information Security (SEC'97): 14-16 May 1997, Copenhagen, Denmark, Chapman&Hall 1997, pp 91-98

[ÖCB94] Säkerhetshöjande åtgärder för samhällsviktiga datasystem inom den civila delen av totalförsvaret, ÖCB Dnr 6-1185-94