RC24529 (W0804-015) April 2, 2008
Computer Science

IBM Research Report

IT Security as Risk Management: A Research Perspective

Pau-Chen Cheng, Pankaj Rohatgi
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598

Research Division
Almaden - Austin - Beijing - Cambridge - Haifa - India - T. J. Watson - Tokyo - Zurich

IT Security as Risk Management: A Research Perspective*

Pau–Chen Cheng pau@us.ibm.com
Pankaj Rohatgi rohatgi@us.ibm.com

IBM Thomas J. Watson Research Center

April 11, 2008

Abstract

This article is a brief white paper explaining our view for conducting research on "IT Security as Risk Management". While we do not have an end–to–end validation of our view, it is the thought underlying our research on risk management.

1 What is IT Security ? Where is the Risk ?

We believe that the very majority of IT security research has been focused on one theme: *to distinguish the good from the bad*, and there are ample examples such as :

- virus scanner: what is a virus and what is not.
- intrusion detection : what is an intrusion and what is not.
- access control policy : what accesses should be allowed and what should not be. Appendix A presents our view on traditional access control models.
- firewall policy : what traffic should be allowed and what should not be.

While tremendous progress has been made, there does not seem to be any IT security technology that can tell the good from the bad with perfect accuracy. Most instances of IT security systems still seem to have higher than desirable false rates. We submit that this imperfection is due to the *lack of sufficient information* when making the good–or–bad decisions; for example,

- A firewall usually cannot fully understand the contents and intents of messages passing among applications. It is a difficult tradeoff between blocking bad/malicious messages and allowing good/legitimate messages.
- Anti–virus scanners work on limited computing resources and incomplete or even out–of–date virus signatures. It is a difficult tradeoff between blocking malicious contents and allowing legitimate contents [1]. The same can be said for anti–spam, IDS, etc.

The situation is made even worse by the ever increasing number of new applications, new protocols, new programming and mark–up languages, new . . . and the accompanying new vulnerabilities and new attacks. Conversely, research such as those done by Chen et.al. [2, 3] has shown that near 100% accuracy could be achieved in telling the good from the bad if enough state information and knowledge is available, albeit in a postmortem manner. Without enough information, we could only see *different shades of grey* instead of a clear–cut boundary between white and black, good and bad. This is especially so in making a real–time decision, when the one event that can accurately tell the good from the bad has not happened yet. The fundamental constraint is our *inability to accurately predict the future*. We usually do not know enough about the past either. Therefore there is inherent uncertainty in making security decisions and

[*] This Research is conducted through participation in the International Technology Alliance sponsored by the U.S. Army Research Laboratory and U.K. Ministry of Defense and was accomplished under Agreement Number W911NF-06-3-0001. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the US Army Research Laboratory, the U.S. Government, the UK Ministry of Defense, or the UK Government. The US and UK Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

in specifying security policies. We could not be sure if a decision made according to a security policy will not lead to bad consequences; the Robert Hanssen espionage case [4, 5] would be a good example. We dare to submit that what has been done and what will be done in IT security is basically ***guessing***, albeit in an educated manner. This guessing nature implies that each IT security decision could lead to bad consequences with non–zero probability; and we define *risk* as the *expected value of damage* incurred through the bad consequences.

The *goal of research on IT security* should *not* be finding the perfect distinction between the good and the bad, but *managing risk to keep it below an acceptable level within one's resource constraints*. To achieve this goal, we believe that it is necessary to move away from the binary, good–or–bad mode of thinking, and accept and address the different shades of grey, or the uncertainty explicitly. This belief leads to the research areas discussed in section 2.

2 Wide–Open Research Areas in Risk Management

We believe that there are five wide–open research areas on IT security as risk management listed below. The references in the list point to the relevant work that we and our colleagues have done and are not meant to be exclusive.

1. *Quantified Risk Estimate*
   - estimating IT security risk quantitatively. The first requirement in doing risk management is to have a sense of how much risk is associated with a decision. While a high–precision estimate is usually hard to get due to the unpredictable future, it is possible to obtain a rough estimate, at least in certain context [6].

     Our experiences show that two steps should be taken first:
     - *identifying the context within which risk is to be managed.* It is very hard to reason about risk without a context. The context would determine what kinds of bad consequences are possible, what damages may be incurred under what conditions, etc.
     - *determining what kinds of consequences are bad within the context and how bad they are.* "One's poison is another's meat". Risk implies that some events may happen to damage tangible or intangible assets of value. The notion of value is context–dependent and could be both objective and subjective; and this notion directly impacts the risk estimate.
   - identifying factors contributing to or modulating risk [7].
2. *Risk–Based Decision Making* : determining *who, where and how much* risk to take using quantified risk estimates. We believe that quantified risk can be viewed as a countable and limited[1] resources and risk–based decision making can be viewed as a *resource allocation problem*, where economics principles and approaches such as a market can be applied [8]. The goal here would be to achieve optimum risk–vs–benefit tradeoff over many decisions and actions yet still stay within one's risk tolerance.
3. *Risk Mitigation* : mitigating risk so as to perform useful actions that would otherwise be denied due to high risk associated with them. Most existing IT security technologies can be used for risk mitigation. The research questions are :
   - What risk mitigation measures to apply in a particular context ?
   - How much is the residual risk after application of the chosen measures ?
4. *Continuous Adaption and Improvement* : one's perception of risk and risk tolerance would change as the environment and needs change with time. So the models and parameters of risk estimation, risk–based decision making and risk mitigation need to adapt to changes, which could be observed by sampling the results of applying risk–based decisions and risk mitigation measures. Also, given the guessing nature, there is always a need to improve these models and parameters.

   We further argue that continuous adaption and improvement largely satisfies the need of validating these models and parameter. Since even if the current models and parameters are valid, they may not be so in the future due to the changes that will happen inevitably.

   Our work shows that machine learning seems to be a very promising way to do continuous adaption and improvement [9]. This is logical since adaption requires the ability to learn.
5. *Integration* of the results of research in the above four areas into an adaptive risk–based security system shown in Figure 1.

[1] One should not take unlimited risk.

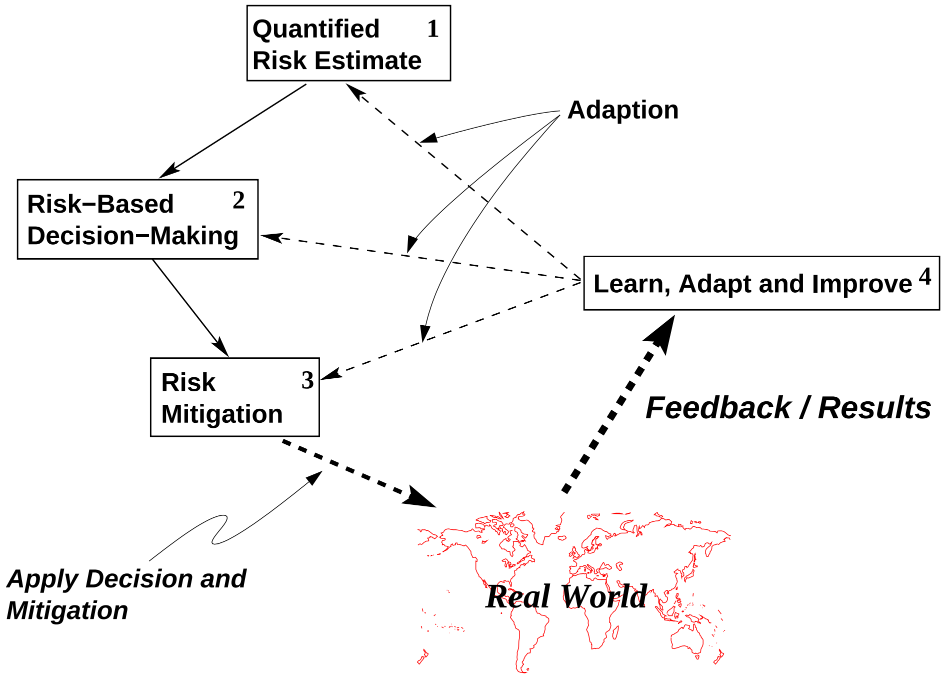
Quantified Risk Estimate 1
Adaption
Risk−Based Decision−Making 2
Learn, Adapt and Improve 4
Risk Mitigation 3
Feedback / Results
Apply Decision and Mitigation
Real World

Figure 1: Integrated Adaptive Risk–Based Security System

Although much more progress is needed in each and every of the five areas to make IT security as risk management a reality, researches in these areas can and should be done in parallel to benefit one another.

3 Acknowledgment

We would like to thank David Safford, Wietse Venema and Michael Steiner for the thoughtful comments and useful information they provided.

References

[1] Antivirus protection worse than a year ago. heise Security UK, December 2007. http://www.heise-online.co.uk/security/Antivirus-protection-worse-than-a-year-ago--/news/100900. (Cited on page 1)

[2] Samuel T. King and Peter M. Chen. Backtracking Intrusions. *ACM Transactions on Computer Systems*, 23(1):51–76, February 2005. http://www.eecs.umich.edu/∼pmchen/papers/king05_2.pdf. (Cited on page 1)

[3] George W. Dunlap, Samuel T. King, Sukru Cinar, Murtaza A. Basrai, and Peter M. Chen. Revirt: Enabling Intrusion Analysis through Virtual Logging and Replay. In *Symposium on Operating System Design and Implementation (OSDI)*, December 2002. http://www.eecs.umich.edu/∼pmchen/papers/dunlap02.pdf. (Cited on page 1)

[4] Robert Philip Hanssen Espionage Case. FBI National Press Office, February 2001. http://www.fbi.gov/libref/historic/famcases/hanssen/hanssen.htm. (Cited on page 2)

[5] David A. Vise. *The bureau and the mole: the unmasking of Robert Philip Hanssen, the most dangerous double agent in FBI history*. Atlantic Monthly Press, 2002. (Cited on page 2)

[6] Pau-Chen Cheng, Pankaj Rohatgi, Claudia Keser, Paul A. Karger, Grant M. Wagner, and Angela Schuett Reninger. Fuzzy Multi–Level Security: An Experiment on Quantified Risk–Adaptive Access Control. In *IEEE Symposium on Security and Privacy*, May 2007. (See also [10]). (Cited on page 2)

[7] Pau-Chen Cheng and Paul A. Karger. *Risk Modulating Factors in Risk–Based Access Control for Information in a MANET*, 2008. IBM Research Report RC24494, http://domino.watson.ibm.com/library/CyberDig.nsf/Home (use search key ”RC24494”). (Cited on page 2)

[8] Ian Molloy, Pau-Chen Cheng, and Pankaj Rohatgi. *Trading in Risk: Using Markets to Improve Access Control*, 2008. IBM Research Report RC24439, http://domino.watson.ibm.com/library/CyberDig.nsf/Home (use search key ”RC24439”). (Cited on page 2)

[9] Yow Tzu Lim, Pau-Chen Cheng, John Andrew Clark, and Pankaj Rohatgi. Policy Evolution using Genetic Programming: A Comparison of Three Approaches. In *IEEE World Congress on Computational Intelligence (WCCI)*, June 2008. (Cited on page 2)

[10] Pau-Chen Cheng, Pankaj Rohatgi, Claudia Keser, Paul A. Karger, Grant M. Wagner, and Angela Schuett Reninger. *Fuzzy Multi–Level Security: An Experiment on Quantified Risk–Adaptive Access Control*, 2007. IBM Research Report RC24190, http://domino.watson.ibm.com/library/CyberDig.nsf/Home (use search key ”RC24190”). (Cited on page 3)

[11] David F. Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli. *Role–Based Access Control*. Artech House Publishers, April 2003. ISBN 1580533701. (Cited on page 4)

[12] David E. Bell and Leonard J. LaPadula. Computer Security Model: Unified Exposition and Multics Interpretation. Technical Report ESD–TR–75–306, The MITRE Corporation, Bedford, MA. HQ Electronic Systems Division, Hanscom AFB, MA, March 1976. http://csrc.nist.gov/publications/history/bell76.pdf. (Cited on page 4)

A Abstract View on Traditional Access Control Models

We think all traditional access control models assign an user/subject to groups, and each group is assigned a particular set of rights. An access request made by an user/subject is granted if and only if the user/subject belongs to a group that has the right to make such an access. For example, the groups are :

- roles in the RBAC model [11],
- security clearances in the Bell–Lapadula MLS model [12],
- entries in an access control list in the traditional discretionary access control model.

Different models differ in how the group memberships are defined, encoded and maintained/updated. But they have one feature in common: a group is treated as a classic set and an access control decision boils down to a *binary* set membership testing of the subject. An access control policy based on such a model is encoded in group memberships and group rights that are determined before the implementation and enforcement of the policy. The policy represents a pre–determined, *fixed trade–off* between the need to provide access and the risk of providing the access.

Our experiences show that such a policy is usually too rigid and the group memberships and rights can not be kept up–to–date in a dynamic world. Legitimate business needs and changes in environments, tools etc. would demand exceptions and the policy is usually augmented in an ad–hoc manner to satisfy the demands. The additional risk associated with the exceptions is not accounted for and the trade–off represented by the original policy, and even the policy itself becomes meaningless.