A Layered Decision Model for Cost-Effective Network Defense

Huaqiang Wei
Computer Science Dept.
University of Idaho
Wei3004@uidaho.edu

Deborah Frincke
Pacific Northwest Nat'l Lab.
University of Idaho
frincke@cs.uidaho.edu

Jim Alves-Foss
Computer Science Dept.
University of Idaho
jimaf@cs.uidaho.edu

Terry Soule
Computer Science Dept
University of Idaho
tsoule@cs.uidaho.edu

Hugh Pforsich
Accounting Dept.
CSU, Sacramento
pforsich@csus.edu

Abstract[1]

Network safeguarding practices involve decisions in at least three areas: identification of well-defined security policies, selection of cost-effective defense strategies and implementation of real-time defense tactics. Although choices made in each of these three affect the others, many existing decision models handle these three decision areas in isolation. There is no comprehensive tool that can integrate them to provide a single efficient model for safeguarding a network. In addition, there is no clear way to determine which particular combinations of defense decisions result in cost-effective solutions. To address these problems, this paper introduces a layered decision model (LDM) for use in deciding how to address defense decisions based on cost-effectiveness. To illustrate the technique, the LDM model is applied to the design of network defense for a sample e-commercial business.

1. Introduction

There are many decisions involved in managing network system protection. Ideally, a security decision system would support a cohesive security process [10], which supports well-defined security policies, defense strategies and real-time defense tactics.

"Security policy is a set of rules and practices that specify or regulate how a system or organization provides security service to protect sensitive and critical system resources [4]." A defense strategy is the combinations of different defense techniques and operations. A defense tactic is the instantaneous defensive reaction when a network is under attack. Currently, these decisions are carried out by a variety of different tools. These decision tools include IT security governance plan [1,5], and the methodologies of the risk assessment [2,7,14,17,22] and business impact analysis [3,8-10] for high-level security goals; business cost modeling [23] and security investment analysis [12,13,16] for defense strategies; cost modeling for intrusion detection systems [19-21], and the game theory modeling [12,15] to support the network defense tactics.

[1] This research was funded in part by DARPA (project number: F30602-02-1-0165)

While there is a proliferation of tools for decision support, the connectivity between decisions about security policies, defense strategies and defense tactics is weak and there is no guarantee that these decisions will be consistent. It is also hard to tell how a cost decision of one kind (e.g., about goals) will affect cost outcomes at another level (e.g., regarding tactics). We present a layered decision model to support consistent, connected decisions at three layers: security policies, defense strategies, and defense tactics, and to balance costs at all layers.

The layered decision model (LDM) integrates decisions about security policies, defense strategies and defense tactics in a uniform framework. In addition, this model provides an analytical framework that allows traceability of costs between layers. This framework combines risk assessment, business cost modeling, and cost-benefit analysis which uses return on investment (ROI) analysis. The work in this paper is preliminary, but should provide a good foundation for future work in this area.

2. Description of the Layered Decision Model

The layered decision model (LDM) includes three decision layers: security policies, defense strategies and defense tactics. The layers are used to define the decision parameters, establish relationships between decision types, and both support and record decisions made. Security policies are defined at decision Layer Zero; defense strategies at Layer One; and defense tactics at Layer Two.

Other model components, used variously as inputs or as "internal state" needed to make a decision, include the risk assessment for identifying threat profiles, the business cost modeling for estimating the business cost associated with each threat and related security mean(s), and the cost-benefit analysis based on the return on investment (ROI) analysis for comparing and selecting the cost-effective defense mean(s).

Security policies, defense strategies and defense tactics vary with business types and times. To formally describe the LDM, we consider a particular business type *b* at a particular time *t*, and make the following definitions:

$T_{t,b,0} = \{ t_1 \ldots t_m \}_{t,b,0}$ is a set of threats that represent the threat environment before ranking.

$T_{t,b,1} = \{ t_1 \ldots t_n \}_{t,b,1}$ is a set of threats after ranking.

$P_{t,b} = \{ p_1 \ldots p_n \}_{t,b}$ is a set of security policies.

$G_{t,b} = \{ g_1 \ldots g_n \}_{t,b}$ is a set of business goals.

$S_{t,b} = \{ S_{t,b,1} \ldots S_{t,b,k} \}_{t,b}$ is a set of strategy sets.

$S_{t,b,k} = \{ s_{k,1} \ldots s_{k,n} \}_{t,b,k}$ is the kth set of defense strategies. k is the set number.

$R_{t,b} = \{ r_1 \ldots r_n \}_{t,b}$ is a set of defense tactics.

The flow through the model's architecture is shown in Figure 1. Specific security policies, defense strategies and defense tactics are determined as the model is used – they are not embedded in the structure of the model itself. So, for instance, a security manager may combine both business goals, and personal experience and knowledge when determining the specific policies to be set within Layer Zero.

By connecting decisions in this way, we achieve several advantages. First, we provide a way to organize the *making* of decisions. Second, we establish explicit connectivity between decisions of different types, so that the consequences of decisions at any layer become clearer (if a tactic set is changed so it no longer fulfills the strategy that shows up as a gap, for instance). Third, we set the basis for performing an integrated cost assessment at multiple levels of decision making. Finally, we allow for iteration between levels, so that not only can decisions about tactics and strategy be made within the context of business goals, but also decisions about which business goals are reasonable to establish may be made with a better understanding of the associated costs.

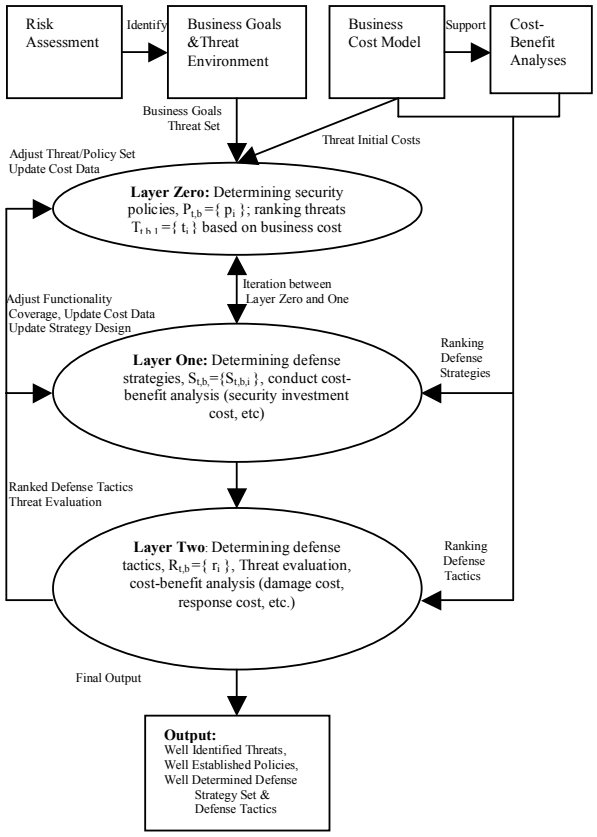

Figure 1 Layered decision model

As shown in Figure 1, the inputs to Layer Zero are the business goals and threat environment. The outputs are policies (which embody the goals) and ranked threats (based on the priorities of the business). Layer Zero may be considered the set of all decisions about *what a business ought to be doing*.

Layer One addresses defense strategies as selected within the context of predetermined business goals. The purpose of making decisions in Layer One is to determine a set of defense strategies that will achieve the needs of the security policy with respect to the ranked threats. There will be many possible strategies that would be sufficient – but which ones are best for a particular organization? In our model, defense strategies are selected both on the basis of Layer Zero decisions about goals as well as the specific defensive techniques that are available, budget, and any additional external values (ex: moral imperatives to use/not use certain defense strategies like active defense) which are of importance. By identifying multiple strategy sets, they can be compared based on implementation cost of Layer Two.

To complete the creation of Layer One in the case of multiple strategy sets, business cost modeling and cost-benefit analysis should be applied to assess each strategy's cost and benefit, and then each strategy set would be ranked based on cost-effectiveness (i.e. return on investment (ROI)). Other methods of ranking are also possible. Layer One may be considered the set of all decisions about *the approach a business ought to use to achieve its goals*.

Layer Two decisions involve choosing specific defense tactics. The input of Layer Two is a particular defense strategy set provided by Layer One (as well as the associated ranked threats). Thus, there will be "multiple" instances of Layer Two. When making Layer Two decisions in our model, we propose organizations use cost-benefit analysis. This will allow for feedback to Layer One (i.e., the most cost effective strategy could be selected). Layer Two may be considered the set of all decisions about *the technique a business ought to use to fulfill its strategies*.

As we have indicated, business cost modeling is explicitly required in our layered decision model. This is because we wish to assess the cost each threat might incur, and the cost effectiveness of different defense plans or decision sets, so as to be able to choose between them. The question of how best to define the costs of security is an open one, but we provide some suggestions for methods that work well with our model in this section. The cost-benefit analysis we propose is largely drawn from Lee's[19] and Wei's study [11] regarding the cost modeling for network intrusion detection system, in which they divided the cost into damage cost, response cost and operational cost, conducted cost-benefit analysis and decided if the attack worth mitigating or not.

At Layer Zero business cost modeling is applied to assess business cost (single loss expectancy (SLE) and annual loss expectancy (ALE)) of each threat type, based on which all threats can be ranked accordingly. ALE can be used as a threat index to rank and indicate how critical each threat is. The higher the ALE, the more critical the threat is. The ranked threats are used to define security policy set at Layer Zero, defense strategies at Layer One and defense tactics at Layer

Two. The cost parameters of Layer Zero are estimates based on experience, which can be refined at lower layers.

The business cost of security or other aspects of a business can be measured in such a way as to include the decline of corporation revenue and disruption of business operation [8]. These measurements are often provided either as a dollar amount or as a percentage in an annual report post-mortem. From the perceived risk assessment, the cost associated with each threat or attack incident includes the following cost items:

The first cost item is the labor cost, **LaborCost**, which includes working cost in inspection, repairing, backing up, shutting down the system, and reinstallation to restore the system. The second cost item is the material cost, **MaterialCost**, which includes replacement cost for hardware, software and facilities. The third cost item is the confidential data and trade secret loss, **DataLoss**. The fourth cost item is employee's salary, **IdlePay**, when network is down and employees are idle. The last cost item is the cost of business disruption, **BusinessDistruption**, which is incurred by the problem in processing orders and lack of response to customer inquires.

These cost items are post-occurrence and exclude the cost of taking precautions to prevent other security attacks, which should be part of the costs associated with system defenses that are already established (in other words, part of the cost of the selected strategy/tactics of Layers One and Two. The post-occurrence cost represents the worst scenario that the attack is 100% complete and the damage cost is 100% progressed. Defining Cost_ps[i] is the post-occurrence cost of threat i, then,

$$\text{Cost\_ps}[i] = \text{BusinessDisruption} + \text{IdlePay} + \text{DataLoss} + \text{LaborCost} + \text{MaterialCost} \quad (2.1)$$

Reducing the cost of attacks requires investment in defense, which is called pre-occurrence cost. The cost modeling and the business cost results (SLE and ALE) can be applied at Layer One to evaluate the cost-effectiveness of defense plans and defense investments. These defense investments might include such things as purchasing hardware or software **(MaterialCost**), one time labor costs (**LaborCost)**, ongoing maintenance costs to maintain patches (**MaintenanceCost**) and training costs for personnel, for instance to reduce vulnerability to social engineering or careless handling of security systems, or even improvements in software design to reduce flaws in new software (**TrainingCost**). The sum of these cost items is considered as pre-occurrence investment cost. There are other possible costs – such as the cost of borrowing funding to pay for these elements or the cost of what isn't being supported because the funding was allocated for security, but we do not explicitly include that in this equation, which could easily be modified to include those factors also. We define Cost_pr[j] to be the pre-occurring cost of security investment of defense strategy j, stated here as:

$$\text{Cost\_pr}[j] = \text{MaterialCost} + \text{LaborCost} + \text{MaintenanceCost} + \text{TrainingCost} \quad (2.2)$$

There might be many defense strategy sets. To determine which one is the most cost-effective, Layer One conducts the cost-benefit analysis (based on return on investment analysis) to compare all defense strategy sets and select the best one.

We define effect[i,j] to be the effectiveness of a specific defense set j when countering a threat i, P[i] is the annual probability or likelihood of threat i. The return on investment (ROI) is the ratio of cost saving and investment cost, so ROI of investing defense set j to counter threat i is:

$$\text{ROI}[i,j] = (\text{Cost\_ps}[i] \times \text{P}[i] \times \text{effect}[i,j]) / (\text{Cost\_pr}[j] + \text{Cost\_ps}[i] \times \text{P}[i] \times (1 - \text{effect}[i,j])) \quad (2.3)$$

(Cost_ps[i] × P[i] × effect[i,j]) is the cost saving or benefit (Benefit(i,j)) of using defense set j to counter threat i.

At Layer Two SLE is needed to describe the damage cost of each threat, and to evaluate and compare the effectiveness of multiple defense tactics. In addition, response cost and operational cost are also needed to evaluate whether or not a threat is worth mitigating through cost-benefit analysis. Layer Two gives feedback to Layer One about the effectiveness of each defense tactic when mitigating specific threats, which helps Layer One refine the design of defense strategy set to cost-effectively mitigate all threats to fulfill business goals. The refinery might include reducing or adding certain functionality to mitigate specific threats. Layer Two also gives feedback to Layer Zero about the updated information regarding if specific threats are worth mitigating or not, which helps Layer Zero refine the threat set and security policy set, which might include re-ranking the threats.

The integrated cost should include the above three cost categories: the damage cost (SLE or ALE) used at three layers; the security investment cost used at Layer One; the response cost and operational cost used at Layer Two. LDM provides such framework to consistently estimate these costs associated with all decision paths, which are traceable.

The decision making process is not a one-time effort. It requires multiple iterations to refine the decision parameters in order to find the cost-effective solutions at three decision layers. This iterative decision process requires not only the upper layers providing input to lower layers, but also the lower layers giving feedback to upper layers. Figure 2 shows an example of hierarchical relationships among three decision layers.

3. Using the Model

In this section we illustrate the model by applying LDM to the construction of a layered decision set for a simplified model of an e-commercial business case. In this scenario, the fictitious company is a Web based on-line trading company that sells products to customers all over the country. The current year's enterprise strategy of this company is to increase the revenue by 20% based on previous year's revenue of $100,000,000. The objective of the network security is to protect the business goals listed in table 3.1.

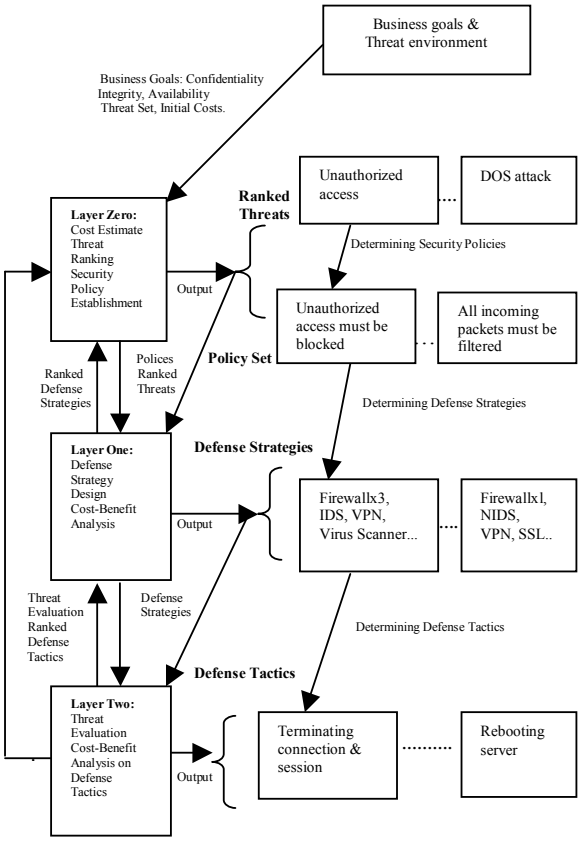

Figure 2 Hierarchical relationships among three decision layers

Table 3.1 Business goals and security requirements

Business Goal	Category	Security requirements
g_1	Confidentiality	The critical customer records should be available only to authorized people
g_2	Integrity	The system files should not be modified by unauthorized people
g_3	Availability	To ensure the e-commercial service availability (24x7), the (D)DOS attack must be prevented. Once it happens, it must be mitigated promptly and effectively
g_4	Non-repudiation	To prevent an agent from sending spoofed email with malicious intent, a sending agent can't deny sending information; a receiving agent can't deny receiving information.

Therefore, based on the above business goals the management needs to identify threats and determine proper security policies, defense strategies and defense tactics. The following section discusses the decision procedure and decision results based on the LDM concept.

3.1 Security Policies

Having defined the business goals, $G = \{g_1, g_2, g_3, g_4\}$, the company would need to identify threats and rank them (T):

1) **Unauthorized access** (t_1)--- attacker can obtain unauthorized access by guessing user names and passwords. The attacker may obtain the root access and change system files, or modify trading data.
2) **Application level attack** (t_2)--- attacker may exploit well-known weakness in software and OS that are commonly found on servers to obtain root access.
3) **Denial of service attack** (t_3)--- attack by flooding target host with packets.
4) **IP spoofing attac**k (t_4)--- attacker can modify the source IP address of the packet he sends, which makes people assume that the packet comes from somewhere else.
5) **Virus and Worm attack** (t_5)--- Virus and worm can spread through email and network space.

Therefore, $T_{t,b,0} = \{ t_1, t_2, t_3, t_4, t_5\}$

The annual frequencies (times/year) of these are 5, 2, 5, 10, and 5 respectively. Based on estimate, the successful events of these threats cause the revenue decrease by 0.5%, 0.03%, 0.01%, 0.05%, and 0.03% respectively. Table 3.2 lists the ranked threats and their ranks according to their initial estimated business costs.

Table 3.2 Ranked threats

Threat	Frequency	Business Cost	Rank
t_1	5	$3,000k	1
t_2	2	$72k	4
t_3	5	$60k	5
t_4	10	$600k	2
t_5	5	$180k	3

Therefore, $T_{t,b,1} = \{ t_1, t_4, t_5, t_2, t_3\}$ in which the threats are ordered from the highest business cost to the lowest business cost. Based on the business goals and the ranked threats the model defines the following security policies:

p_1: Ingress and egress filtering must be always conducted.
p_2: The system must be virus free.
p_3: If network traffic exceeds its normal threshold by 25%, traffic rate limitation must be activated.
p_4: If Web server is substantially slower than normal the system administrator may need to restart the Web server, or switch the service to a back up server.
p_5: Remote access must be authenticated with passwords, and passwords must be no less than 8 characters and must be changed every 60 days.
p_6: Improper communication between servers must be recognized and blocked.
p_7: All incoming packets must be filtered.
p_8: Unauthorized access must be blocked.
p_9: Communication with servers must be encrypted.
P_{10}: No unapproved software be installed on any workstation without authorization from the system administration.
P_{11}: No-email or Internet access is allowed on critical corporate financial servers and database servers.
P_{12}: All account security events must be logged.
P_{13}: All server data will be backed up daily using incremental back-ups. Fully backup will be done on the weekly basis.

Therefore, $P_{t,b} = \{ p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10}, p_{11}, p_{12}, p_{13} \}$

3.2 Defense Strategies

Based on the security policies of Layer Zero, the Layer One decision is where the organization proposes and evaluates three potential defense strategy sets described below based on the budget and the availability of defense techniques, and

select one with the highest overall ROI. The business cost modeling is applied to assess the investment cost. The cost-benefit analysis is conducted to select the best strategy set.

Strategy set one ($S_{t,b,1}$) is a comprehensive package and assumes that the company has sufficient budget to purchase or implement these defense strategies. Table 3.3 lists $S_{t,b,1}$'s elements and major threats each defense strategy might counter.

Table 3.3 $S_{t,b,1}$'s features

Defense Strategy	Location	Explanation
Three Firewalls ($s_{1,1}$)	Between gateway and Internet; between Web server and application server; between application server and database server	To conduct access control. (major threats: t_1- t_5)
Three HIDS (host-based IDS) ($s_{1,2}$)	Each server has one	To monitor entire network. (major threats: t_1- t_5)
VPN device ($s_{1,3}$)	At remote access points	To secure remote control. (major threats: t_1,t_2, t_3)
REC 2827 and 1918 protocols ($s_{1,4}$)	Whole network	To enforce ingress filtering and egress filtering. (major threats: t_3)
Content filtering server ($s_{1,5}$)	Whole network	To scan URL request. (major threats: t_4)
Virus/worm scanner ($s_{1,6}$)	Whole network	To detect and disinfect virus. (major threats: t_5)
Level 2 switch ($s_{1,7}$)	Among the servers	To maintain proper communication. (major threats: t_1- t_4)
Level 3 switch with IDS features. ($s_{1,8}$)	Among the servers	(major threats: t_1- t_5)
Level 4-7 application switch ($s_{1,9}$)	Among the servers	To regulate network traffic. (major threats: t_1,t_3, t_5)
SSL ($s_{1,10}$)	Whole network	To secure Internet based transactions. (major threats: t_1, t_4)
IPSec encryption ($s_{1,11}$)	Whole network	To enforce authentication. (major threats: t_1- t_5)

Strategy set two ($S_{t,b,2}$) assumes limited implementation of security defense strategies. This situation may occur when budget are limited. Table 3.4 lists all the features of $S_{t,b,2}$, and major threats each defense strategy might counter.

Table 3.4 $S_{t,b,2}$'s features

Defense Strategies	Location	Explanation
One Firewall ($s_{2,1}$)	Outside Web server	To conduct access control (major threats: t_1- t_5)
NIDS(network based IDS) ($s_{2,2}$)	Whole network	To monitor entire local network. (major threats: t_1- t_5)
RFC 2827 and 1918 protocols ($s_{2,3}$)	Whole network	To do ingress and egress Filtering. (major threats: t_3)
VPN device ($s_{2,4}$)	At remote access points	To ensure secure remote access. (major threats: t_1, t_2, t_3)
NAT(network address translator) ($s_{2,5}$)	Whole network	To conceal real IP addresses. (major threats: t_1, t_2, t_3)
SSL ($s_{2,6}$)	Whole network	To secure Internet based transaction. (major threats: t_1, t_4)
Virus/worm scanner ($s_{2,7}$)	Whole network	To detect and disinfect virus. (major threats: t_5)

Strategy set three ($S_{t,b,3}$) has similar features as strategy set one ($S_{t,b,1}$), but uses components from another vendor. The prices are higher, but the effectiveness is lower relative to $S_{t,b,1}$ when handling some attacks. Table 3.5 lists these defense strategy sets and their corresponding overall effectiveness for different threats.

Table 3.5 Defense strategy sets and attacks

Threat / Strategy	Unauthorized access (UA)	(D) DOS (DOS)	Apps. Attack (AA)	IP Spoofing (IPS)	Virus/ Worm (VW)
$S_{t,b,1}$	0.85	0.75	0.85	0.70	0.75
$S_{t,b,2}$	0.60	0.70	0.70	0.60	0.70
$S_{t,b,3}$	0.65	0.60	0.80	0.60	0.75
Revenue Drop (% of revenue)	0.5%	0.03%	0.01%	0.05%	0.03%
Frequency (times/yr)	5	2	5	10	5

Each strategy set can handle the above threats through each individual defense strategy, but with different effectiveness. Under each defense strategy set, each defense strategy may handle one or more attacks. Attack frequency is a controversial subject beyond the scope of this research – as a guideline, one might rely on agency forecasts for these, but the difficulty of getting such data does indicate why it is so difficult to get accurate cost/benefit outcomes! However, even relative ranking of expected frequency is useful.

The business cost, as a percentage of revenue drops after a successful attack can be estimated based on the past experience and outside publications too. The percentage of the revenue drop of each attack type is the actually average business cost divided by the projected revenue.

Table 3.6 displays how effective each defense strategy set is when handling different attacks. Based on the business cost model developed in section two, the expected investment cost, expected cost saving (benefit) and ROI are estimated.

Table 3.6 Cost-Benefit analyses for defense strategy sets

Strategy / Attack	$S_{t,b,1}$	$S_{t,b,2}$	$S_{t,b,3}$
UA	Benefit(1,UA)= $2,550k	Benefit(2,UA) = $1,785k	Benefit(3,UA) = $1,836k
AA	Benefit(1,AA)= $1,275k	Benefit(2,AA) = $700k	Benefit(3,AA) = $800k
DOS	Benefit(1,DOS) = $54k	Benefit(2,DOS) = $50k	Benefit(3, DOS) = $58k
IPS	Benefit(1, IPS) = $84k	Benefit(2, IPS) = $71k	Benefit(3, IPS) = $71k
VW	Benefit(1,VW) =$14k	Benefit(2, VW) =$12k	Benefit(3, VW) = $13k
Investment Cost	$220k	$160k	$300k
Expected Benefit (cost saving)	$4,025k	$2,645k	$2,821k
ROI	18.3	16	9

From the result table we can see that $S_{t,b,1}$ has the highest overall ROI when handling different types of attacks. Therefore, we select $S_{t,b,1}$ as the best strategy set. Please notice that it might be able to estimate the return on investment (ROI) of each individual defense strategy (i.e. IDSs ($s_{1,2}$)) when handling each individual attack (i.e. unauthorized access attack (t_1)), but the purpose of this example is to estimate the overall cost-effectiveness of a package (set) of defense strategy when handling a list of identified threats. Therefore, the ROI represents the overall cost-effectiveness of each defense strategy set, instead of the individual cost-effectiveness of each defense strategy.

3.3 Defense Tactics

Based on the Layer One decision of the defense strategy, Layer Two is where we identify and then evaluate defense tactics: a. Blocking access; b. Terminating session/connection; c. Recording /logging and notify administrator; d. Switching to redundant network; e. Backup and restoration; f. Turn off the host and reboot server; g. Automatic scanning and cleaning; h. Cooperating with other ISP for rate limiting.

The following is an example of the decision process of defense tactics for countering an "Unauthorized Access Attack." The hacker broke into the Web server and tried to modify the system files. The IDS detected the incident and the

LDM estimated the cost and assessed the following three potential defense tactics based on defense strategy set one:

1) Tactic one (r_1): Terminating the connection and session.

2) Tactic two (r_2): Recording, logging and notifying administrator.

3) Tactic three (r_3): Turning off the host and rebooting the server.

The potential damage cost (SLE) of the successful attack could be \$600k. r_1 has 85% effectiveness and its cost (includes response cost and operational cost) is \$100k. r_2 is only 50% effective, even though its cost is only \$50k. r_3 is 90% effective, but its cost could be as high as \$200k.

The ROI of r_1 is: (\$600k×0.85) / (\$100k + \$600k × 0.15) = 2.68

The ROI of r_2 is: (\$600k×0.5) / (\$50k + \$600k × 0.50) = 0.86

The ROI of r_3 is: (\$600k×0.9) / (\$200k + \$600k × 0.1) = 2.08

Therefore, the LDM decided to select r_1, "Terminating the connection and session" to mitigate the unauthorized access attack. If r_1 failed, r_3 could be the best alternate.

Another issue is to evaluate whether or not a threat is worth mitigating. We assume there is an "Application Level Attack" in the network. Its estimated damage cost (SLE) is \$36k. But the response cost to this attack would be as high as \$50k, which includes labor cost to investigate the incident, reboot the server and terminate the connection, and the cost incurred by the delay of services during the restoration process. Therefore, this threat is considered not worth mitigating.

The threat analysis result is given to both Layer Zero and One as feedback. Layer Zero decides to remove this threat from the ranked significant threat set. Instead of installing three expensive HIDS, Layer One decides to reduce one HIDS and install patch file, which is very inexpensive and very effective to such kind of "Application Level Attack." The patch file's cost is only \$2k, which saves about \$50k after removing one HIDS.

4. Conclusion

To cost-effectively safeguard network, this research develops a uniform layered decision model that supports consistently connected decisions at three decision layers: security policies, defense strategies and real-time defense tactics. In addition, this model provides an analytical framework that allows traceability of costs between all decision layers, and performs iterative traversing decision process between decision layers.

Future efforts include model refinement, additional simulation, sensitivity analysis and the model implementations in the real-world network defense system.

References

[1] IT Governance Institute (ITGI), *Board briefing on IT governance*, 2nd Edition, 2003, ISBN 1-893209-64-4,http://itgi.org.

[2] R.Campbell and G. Sands, "A modular approach to computer security risk management," *The American Federation of Information Processing Societies (AFIPS) Conference Proceedings*, AFIPS Press, V.48, pp.293-303, 1979.

[3] P. Fites and M. Kratz, *Information systems security*, Van Nostrand Reinhold, New York, 1993.

[4] L. Wheeler, "Taxonomies and glossaries," 2004, www.garlic.com/~lynn/secgloss.html.

[5] Y. Jung, I. Kim, S. Kim, "The design and implementation for the practical risk analysis tools," *Proceedings of the* (IFIP) *International Federation for Information Process* August, 2003. Karlstad University, Sweden. http://www.cs.kau.se/IFIP-summerschool/preceedings /Jung.pdf.

[6] C. Keeling and S. O'Reilly, *Business continuity in the e-commerceenvironment*,2002, http://www.insight.co.uk/whitepapers.htm

[7] I. Gilbert, "Guide for selecting automated risk analysis tools," *NIST Special Publication 500-174*, October, 1989.

[8] M. Erbschloe, *Information warfare: How to survive cyber attacks*, Osborne/McGraw-Hill, CA, USA, 2001.

[9] M. Krause and H. Tipton, *Handbook of information security management*, Auerbach Pub, 5th edition, December 2003.

[10] R. Henning, Harris Corporation, *Strategic security investment*, 2004,http://www.statonline.com/technologies/whitepapers/paper_ssi.pdf.

[11] H. Wei and D. Frincke, "Cost-benefit analysis for network intrusion detection systems," *CSI 28th Annual Computer Security Conference*, Oct. 29-31, 2001, Washington, D.C.

[12] H. Cavusoglu, S. Raghunathan and B. Mishra, "A model for evaluating IT security investments," *Communications of the ACM*, Vol. 47, No 7, pp. 87-92, July 2004.

[13] L.Gordon and M. Loeb, "The economics of information security investment," *ACM Trans. IS Security*, Vol.5, No.4, pp. 438-457, Nov. 2002.

[14] K. Badenhorst,J. Eloff and L. Labuschagne, "A comparative framework for risk analysis methods," *Computer & Security*, Vol. 12, No. 6, pp.597-603, Dec. 1993.

[15] K. Lye and J. Wing, "Game strategies in network security," in the *Proceedings of the Foundations of Computer Security Workshop 2002*, July 26, 2002, Copenhagen, Denmark.

[16] K. Soo Hoo, "How much is enough? A risk-management approach to computer security," *Consortium for Research on Information Security and Policy*, Stanford University, June 2000.

[17] CISCO white paper, *Cisco SAFE: a security blueprint for enterprise networks*, 2004, http://www.cisco.com.

[18] C. Paquet and W. Saxe, *The business case for network security*, Cisco Press, Indianapolis, USA, 2005.

[19] W. Lee, W. Fan, M. Miller, S. Stolfo and E. Zadok, "Toward cost-sensitive modeling for intrusion detection and response," *Computer Security*, Vol.10, No.1-2, pp. 5-22, 2002.

[20] D. Kinn and K. Timm, "*Justifying the expense of IDS*, Part One: An overview of ROIs for IDS," 2004, http://www.securityfocus.com/infocus/1608.

[21] D. Kinn and K. Timm, "*Justifying the expense of IDS*, Part Two: Calculating ROI for IDS," 2004, http://www.securityfocus.com/infocus/1621.

[22] S. Butler, "Security attribute evaluation method: A cost-benefit approach," *Proceedings of the 24th International Conference on Software Engineering*, pp. 232-241, May 19 - 25, 2002, Orlando, Florida, USA.

[23] H. Wei and D. Frincke, "Risk assessment and cost-effective business modeling for network *security," The 7th World Multi-Conference on Systemics, Cybernetics and Informatics SCI 2003*, July 29-August 1, 2003, Orlando, Florida USA.