The UMAP Journal

Vol. 25, No. 2

Publisher
COMAP, Inc.

Executive Publisher
Solomon A. Garfunkel

ILAP Editor
Chris Arney
Interim Vice-President
for Academic Affairs
The College of Saint Rose
432 Western Avenue
Albany, NY 12203
`arneyc@mail.strose.edu`

On Jargon Editor
Yves Nievergelt
Department of Mathematics
Eastern Washington University
Cheney, WA 99004
`ynievergelt@ewu.edu`

Reviews Editor
James M. Cargal
Mathematics Dept.
Troy University—
Montgomery Campus
231 Montgomery St.
Montgomery, AL 36104
`jmcargal@sprintmail.com`

Chief Operating Officer
Laurie W. Aragón

Production Manager
George W. Ward

Director of Educ. Technology
Roland Cheyney

Production Editor
Pauline Wright

Copy Editor
Timothy McLean

Distribution
Kevin Darcy
John Tomicek

Graphic Designer
Daiva Kiliulis

Editor

Paul J. Campbell
Campus Box 194
Beloit College
700 College St.
Beloit, WI 53511–5595
`campbell@beloit.edu`

Subscription Rates for 2004 Calendar Year: Volume 25

Membership Plus

Individuals subscribe to *The UMAP Journal* through COMAP's Membership Plus. This subscription also includes print copies of our annual collection *UMAP Modules: Tools for Teaching*, our organizational newsletter *Consortium*, on-line membership that allows members to download and reproduce COMAP materials, and a 10% discount on all COMAP purchases.

(Domestic)	**#2420**	**$90**
(Outside U.S.)	**#2421**	**$105**

Institutional Plus Membership

Institutions can subscribe to the *Journal* through either Institutional Plus Membership, Regular Institutional Membership, or a Library Subscription. Institutional Plus Members receive two print copies of each of the quarterly issues of *The UMAP Journal*, our annual collection *UMAP Modules: Tools for Teaching*, our organizational newsletter *Consortium*, on-line membership that allows members to download and reproduce COMAP materials, and a 10% discount on all COMAP purchases.

(Domestic)	**#2470**	**$415**
(Outside U.S.)	**#2471**	**$435**

Institutional Membership

Regular Institutional members receive print copies of *The UMAP Journal*, our annual collection *UMAP Modules: Tools for Teaching*, our organizational newsletter *Consortium*, and a 10% discount on all COMAP purchases.

(Domestic)	**#2440**	**$180**
(Outside U.S.)	**#2441**	**$200**

Web Membership

Web membership does not provide print materials. Web members can download and reproduce COMAP materials, and receive a 10% discount on all COMAP purchases.

(Domestic)	**#2410**	**$39**
(Outside U.S.)	**#2410**	**$39**

To order, send a check or money order to COMAP, or call toll-free
1-800-77-COMAP (1-800-772-6627).

The UMAP Journal is published quarterly by the Consortium for Mathematics and Its Applications (COMAP), Inc., Suite 210, 57 Bedford Street, Lexington, MA, 02420, in cooperation with the American Mathematical Association of Two-Year Colleges (AMATYC), the Mathematical Association of America (MAA), the National Council of Teachers of Mathematics (NCTM), the American Statistical Association (ASA), the Society for Industrial and Applied Mathematics (SIAM), and The Institute for Operations Research and the Management Sciences (INFORMS). The Journal acquaints readers with a wide variety of professional applications of the mathematical sciences and provides a forum for the discussion of new directions in mathematical education (ISSN 0197-3622).

Periodical rate postage paid at Boston, MA and at additional mailing offices.

Send address changes to: info@comap.com

COMAP, Inc. 57 Bedford Street, Suite 210, Lexington, MA 02420

Vol. 25, No. 2   2004

Table of Contents

Editorial

Special Section on the ICM

COMAP

Guest Editorial

Building a Modeling Community: MATHmodels.org

Patrick J. Driscoll
Dept. of Systems Engineering
U.S. Military Academy
West Point, NY 10996
pat-driscoll@usma.edu

Our society has become more complex over the past 30 years, fueled by a global economy necessarily dependent upon efficient transportation, logistic, financial, and communication systems that must operate in conditions constrained by limited or diminishing resources. It is not surprising, therefore, that math modeling has gained popularity and importance as a means of quantitatively understanding problems that decision-makers must solve to succeed in this setting.

In its various forms, mathematical modeling has time and again demonstrated its ability to illuminate valuable and frequently hidden insights into the structure of these problems. With this in mind, one would conclude that conditioning our future leaders and managers to be comfortable with the techniques and best practices associated with a math modeling process, and to be confident in the information provided by this process, seems to be a no-brainer. Yet, despite the evidence and despite the continuous growth in participation that contests such as COMAP's HiMCM, MCM, and ICM have realized over the years, institutions have by and large been slow to capitalize on opportunities to build mathematical modeling into their curricula.

To be fair, a large proportion of mathematics faculty members are educated in programs that emphasize theoretical mathematics, thereby leaving any real-world application experience up to their own initiative and opportunity. This point, coupled with the geographical isolation experienced by some schools, means that faculty and their students frequently lack a ready connection to the community of practitioners and professionals outside of academia whose livelihoods depend on analyzing and solving problems using the very mathematics taught in the classroom.

The UMAP Journal 25 (2) (2004) 93–96.

Exposing a wider range of students to mathematical modeling at earlier education levels has been an explicit recommendation of professional organizations ranging from the American Mathematical Association of Two Year Colleges (AMATYC) [Writing Team. . . 1995, 31–35] to the undergraduate Accreditation Board for Engineering and Technology (ABET) [2000]. Moreover, presenting mathematics through applications and modeling has repeatedly proven effective both for teaching reasoning and quantitative skills and for retaining students in mathematically- and scientifically-based programs [Blum and Niss 1991; Boaler 1993]. This point was again made salient in an international context by an independent report on Mathematics in the University Education of Engineers [Kent and Noss 2003, 10–11] to the Ove Arup Foundation, which calls for "a shift in approach from teaching mathematical techniques towards teaching through modeling and problem-solving."

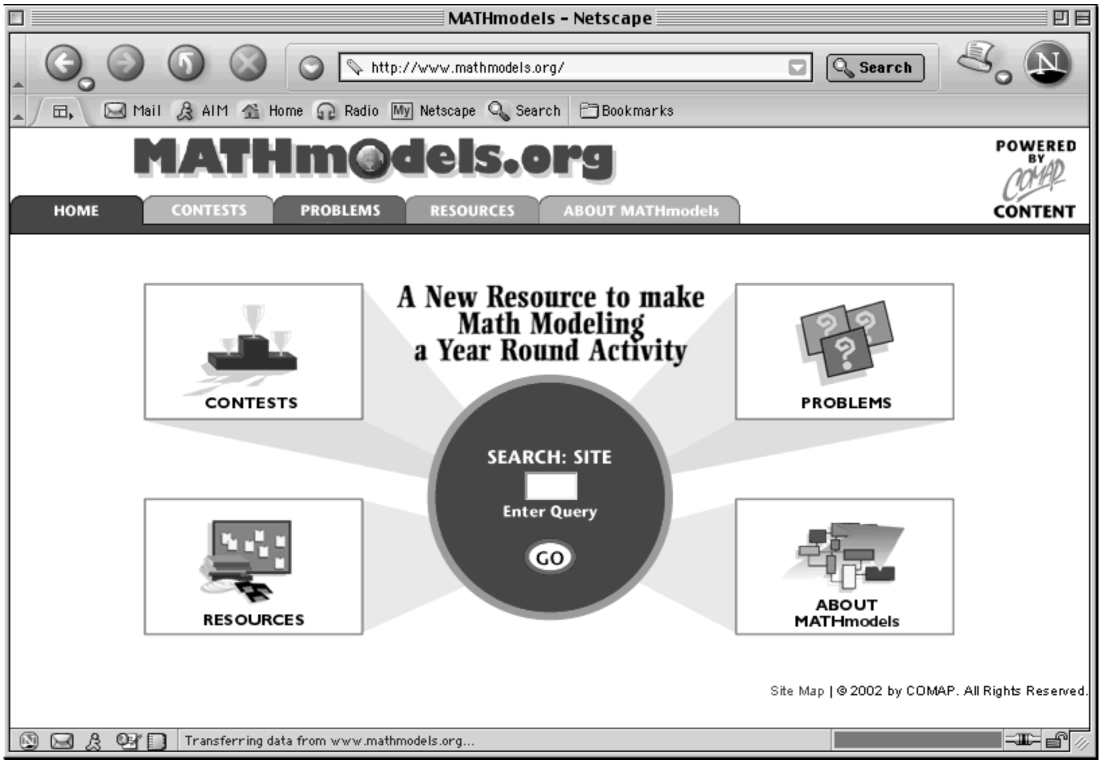
What appears to be needed is

- a *forum* for the exchange of ideas, curriculum to support modeling, and practical tools that can foster the inclusion of mathematical modeling into students, educational experiences; and
- *dynamic linking* in such a forum to embed mentoring relationships within which many new professional interactions can occur.

In response to this need at the undergraduate level, the National Science Foundation (NSF) has sponsored a three-year project for the development of a Web-based mathematical modeling community called `MATHmodels.org`. Hosted by COMAP and directed by Pat Driscoll and Henry Pollak, this site will provide a rich environment in which students and faculty can explore in-depth a wide variety of modeling problems coded by level of difficulty and application area, learning mathematics in the context of its contemporary use. Furthermore, the site will have experienced faculty and practitioner monitors from across the country, so that students working on these problems can post partial and full solutions, ask questions, and participate in extended discussions with fellow students, faculty, and practitioners in government and industry.

The triumvirate relationship between student-faculty-practitioner being developed within `MATHmodels.org` defines a mathematical modeling community that is laden with opportunity. Students and faculty can interact with other students, faculty, and practitioners; practitioners can gain an active awareness of the talents of an emerging generation; and all contribute to a growing body of knowledge and resources that subsequently fertilize and jump-start the efforts of new community members as time progresses.

This direct interaction meets a need that efforts like the HiMCM, the MCM, and the ICM could not reasonably accommodate: providing direct individual feedback to students at key points throughout the modeling process. This focus on improving the modeling process represents a significant departure of a Website away from simply providing resources to members of the modeling community. It is a step towards improving the community's capacity to teach, learn, and do mathematical modeling.



A New Resource to make Math Modeling a Year Round Activity

© 2002 by COMAP. All Rights Reserved.

Transferring data from www.mathmodels.org...

Figure 1. Home page of `MATHmodels.org` .

Although the project is currently in the beginning stages, the prototype design site is online now at `http://www.mathmodels.org` (see **Figure 1** above) and will continue to add functionality through 2006.

The Institute for Operations Research and the Management Sciences (INFORMS) is supporting and endorsing the creation of this site to complement both their Education Committee objectives and their long-term goals of recruiting and retaining young members into the professional OR/MS career field worldwide.

References

Accrediting Board for Engineering and Technology (ABET). 2000. ABET Criteria 2000. Baltimore, MD: Accrediting Board for Engineering and Technology. `http://www/abet.ba.md.gov` .

Blum, W., and M. Niss. 1991. Applied mathematical problem solving, modeling, applications, and links to other subjects—state, trends, and issues in mathematics instruction. *Educational Studies in Mathematics* 22: 37–68.

Boaler, J. 1993. Encouraging the transfer of “school” mathematics to the “real world” through the integration of process and content, context and culture. *Educational Studies in Mathematics* 25: 341–373.

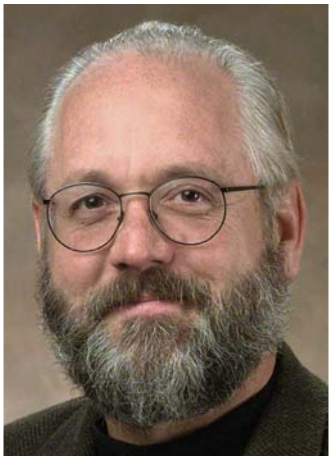
Kent, P., and R. Noss. 2003. Mathematics in the university education of engineers. Report to the Ove Arup Foundation, London, England. `http://www.engc.org.uk` .

Writing Team and Task Force of the Standards for Introductory College Mathematics Project (Don Cohen, ed.). 1995. *Crossroads in Mathematics: Standards for Introductory College Mathematics Before Calculus*. `http://www.imacc.org/standards/` . Executive summary at `http://www.amatyc.org/Crossroads/CrsrdsXS.html` . Memphis, TN: American Mathematical Association of Two-Year Colleges.

Acknowledgment

This editorial is reprinted from COMAP's *Consortium: The Newsletter of the Consortium for Mathematics and Its Applications* No. 85 (Fall/Winter 2003): 16–17.

About the Author



Pat Driscoll is Professor of Operations Research in the Dept. of Systems Engineering at the U.S. Military Academy. Formerly an Academy Professor in the Dept. of Mathematical Sciences, he has also served as the Director of the Mathematical Sciences Center of Excellence and theAssociate Dean of Information and Educational Technology. He received both an M.S. in Operations Research and an M.S. in Engineering Economic Systems from Stanford University, and a Ph.D. in Industrial and Systems Engineering from Virginia Tech. He is a member of the Operational Research Society (ORS) of the United Kingdom, the Institute for Operations Research and the Management Sciences (INFORMS), the Military Operations Research Society (MORS), and the honor societies Phi Kappa Phi and Pi Mu Epsilon. He is an Associate Director for the Mathematical Contest in Modeling (MCM) and one of the designers of the High School Mathematical Contest in Modeling (HiMCM). He serves on the Board of Directors for the Driscoll Foundation, Inc., and Media Knowledge, Inc., is a partner in Winemates & Company, LLC, has three cats, and is continuing to have more fun than should be legally allowed.

Modeling Forum

Results of the 2004 Interdisciplinary Contest in Modeling

Chris Arney, Director
Dean of the School of Mathematics and Sciences
The College of Saint Rose
432 Western Avenue
Albany, NY 12203
arneyc@mail.strose.edu

Introduction

A total of 143 teams of undergraduates, from 82 institutions in 5 countries, spent an extended second weekend in February working on an applied mathematics problem in the 6th Interdisciplinary Contest in Modeling (ICM).

This year's contest began at 8:00 P.M. (EST) on Thursday, Feb. 5, and ended at 8:00 P.M. (EST) on Monday, Feb. 9. During that time, the teams of up to three undergraduates or high-school students researched and submitted their solutions to an open-ended interdisciplinary modeling problem involving the security and costs of maintaining accurate and reliable information systems by organizations (universities and businesses). Teams registered, obtained contest materials, and downloaded the problem and data at the prescribed time through COMAP's ICM Website. After a weekend of hard work, solution papers were sent to COMAP.

The four papers judged to be Outstanding appear in this issue of *The UMAP Journal*. Results and winning papers from the first five contests were published in special issues of *The UMAP Journal* in 1999 through 2003.

The ICM is an extension of the Mathematical Contest in Modeling (MCM), which is held on the same weekend. The ICM is designed to develop and advance interdisciplinary problem-solving skills, as well as competence in written communication. Information about the two contests can be found at

The UMAP Journal 25 (2) (2004) 97–113.

`www.comap.com/undergraduate/contests/icm`
`www.comap.com/undergraduate/contests/mcm`

The problems in the first four ICM contests involved concepts from mathematics, environmental science, environmental engineering, biology, chemistry, and/or resource management. Last year's ICM problem began a shift to operations research, information science, and interdisciplinary issues in security and safety, which will continue for another year (in the 2005 contest). Each team is expected to have advisors and team members who represent a range of disciplinary interests in applied problem-solving and modeling.

This year's Information Technology Security Problem involved understanding, designing, and analyzing the security systems for networked information systems of information-rich organizations. The problem proved to be challenging, in that it contained various modeling and writing tasks to be performed, specific requirements needing scientific and mathematical connections, and the ever-present requirements to use data analysis, creativity, precision, and effective communication. The authors of the problem, computer scientists Daniel Ragsdale and Ronald Dodge, have studied and researched this problem for several years. Information security expert Daniel Ragsdale was a member of the final judging team and his and Prof. Dodge's Authors' Commentary appears in this issue.

All 143 of the competing teams are to be congratulated for their excellent work and enthusiasm for scientific and mathematical modeling and interdisciplinary problem solving. This year's judges remarked that the quality of the modeling and presentation in the papers was extremely high, making it difficult to select just four Outstanding papers.

Start-up funding for the ICM was provided by a grant from the National Science Foundation (through Project INTERMATH) and COMAP. Additional support is provided by the Institute for Operations Research and the Management Sciences (INFORMS). The research that motivated this year's problem was supported by the Office of Artificial Intelligence Analysis and Evaluation at the U.S. Military Academy.

COMAP's Interdisciplinary Contest in Modeling and its Mathematical Contest in Modeling are unique among modeling competitions in being the only international contests in which students work in teams to find a solution. Centering its educational philosophy on mathematical modeling, COMAP uses mathematical tools to explore real-world problems. It serves the educational community as well as the world of work by preparing students to become better informed—and prepared— citizens, consumers, and workers.

Problem: The Information Technology Security Problem

To Be Secure or Not to Be?

You probably know about computer hackers and computer viruses. Unless your computer has been targeted by one, you may not know how they could affect an individual or an organization. If a computer is attacked by a hacker or virus, it could lose important personal information and software.

The creation of a new university campus is being considered. Your requirement is to model the risk assessment of information technology (IT) security for this proposed university. The narrative below provides some background to help develop a framework to examine IT security. Specific tasks are provided at the end of this narrative.

Computer systems are protected from malicious activity through multiple layers of defenses. These defenses, including both **policies** and **technologies** (**Figure 1**), have varying effects on the organization's risk categories (**Figure 2**).

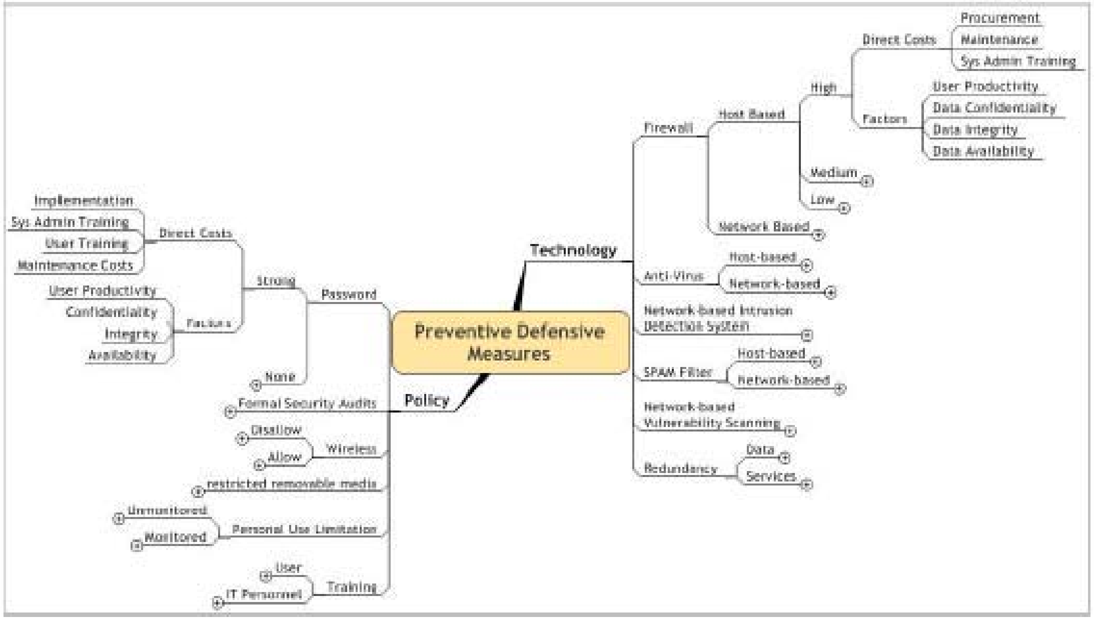


Figure 1. Preventive defensive measures.

Management and usage policies address how users interact with the organization's computers and networks and how people (system administrators) maintain the network. Policies may include password requirements, formal security audits, usage tracking, wireless device usage, removable media concerns, personal use limitations, and user training. An example of password policy would include requirements for the length and characters used in the password, how frequently they must be changed, and the number of failed log-in attempts allowed. Each policy solution has direct costs associated with its

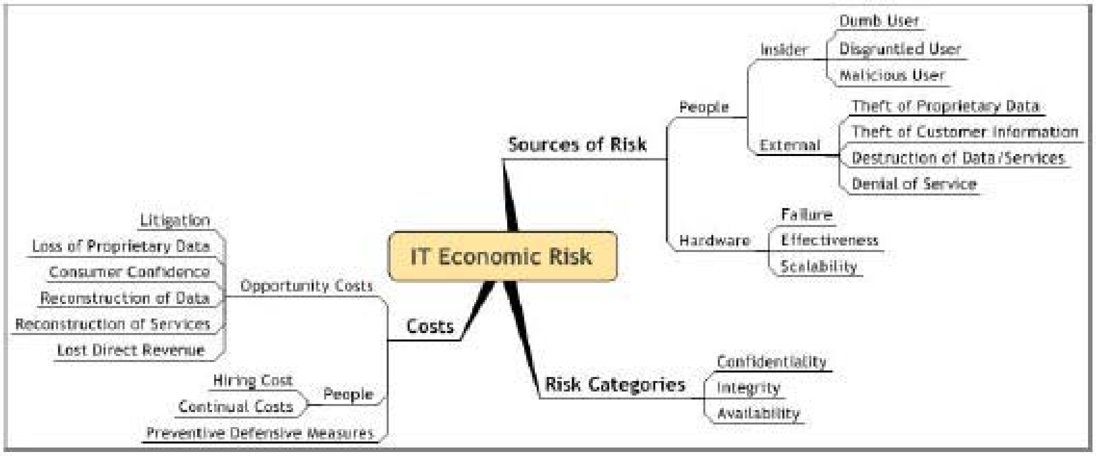


Figure 2. Economic risk schematic for IT systems.

implementation and factors that impact productivity and security. In **Figure 1**, only the topmost branch is fully detailed. The structure is replicated for each branch.

The second aspect of a security posture is the set of technological solutions employed to detect, mitigate, and defeat unauthorized activity from both internal and external users. Technology solutions cover both software and hardware and include intrusion detection systems (IDS), firewalls, anti-virus systems, vulnerability scanners, and redundancy. As an example, IDS monitors and records significant events on a specific computer or from the network examining data and providing an "after the fact" forensic ability to identify suspect activity. SNORT (`www.snort.org`) is a popular IDS solution. **Figure 1** provides a sample of key defensive measures (management/usage policies and technology solutions). As with a policy, a technology solution also has direct costs, as well as factors that impact productivity and security.

Sources of risk to information security include, but are not limited to, people or hardware within or outside the organization (**Figure 2**). Different preventive defensive measures (**Figure 1**) may be more effective against an insider threat than a threat from a computer hacker. Additionally, an external threat may vary in motivation, which could also indicate different security measures. For example, an intruder who is trying to retrieve proprietary data or customer databases probably should be combated much differently from an intruder who is trying to shut down a network.

Potential costs due to information security that an organization may face (**Figure 2**) include opportunity cost, people, and the cost of preventive defensive measures. Significant opportunity costs include: litigation damages, loss of proprietary data, consumer confidence, loss of direct revenue, reconstruction of data, and reconstruction of services. Each cost varies based on the profile of the organization. For example, a health-care component of the university might have a greater potential for loss due to litigation or availability of patient medical records than with reconstruction of services.

An organization can evaluate potential opportunity costs through a risk analysis. Risks can be broken down into three risk categories: *confidentiality*, *integrity*, and *availability*. Combined, these categories define the organization's security posture. Each of the categories has different impacts on cost depending on the mission and requirements of the organization.

- *Confidentiality* refers to the protection of data from release to sources that are not authorized with access. A health care organization could face significant litigation if health care records were inadvertently released or stolen.
- The *integrity* of the data refers to the unaltered state of the data. If an intruder modifies pricing information for certain products or deletes entire data sets, an organization would face costs associated with correcting transactions affected by the erroneous data, the costs associated with reconstructing the correct values, and possible loss of consumer confidence and revenue.
- Finally, *availability* refers to resources being available to an authorized user, including both data and services. This risk can manifest itself financially in a similar manner as confidentiality and integrity.

Each measure implemented to increase the security posture of an organization will impact each of the three risk categories (either positively or negatively). As each new defensive security measure is implemented, it will change the current security posture and subsequently the potential opportunity costs. A complicated problem faced by organizations is how to balance their potential opportunity costs against the expense of securing their IT infrastructure (preventive defensive measures).

Task 1

You have been tasked by the Rite-On Consulting Firm to develop a model that can be used to determine an appropriate policy and the technology enhancements for the proper level of IT security within a new university campus. The immediate need is to **determine an optimal mix of preventive defensive measures that minimizes the potential opportunity costs** along with the procurement, maintenance, and system administrator training costs as they apply to the opening of a new private university. Rite-On contracted technicians to collect technical specifications on current technologies used to support IT security programs. Detailed technical data sheets that catalog some possible defensive measures are contained in Enclosures A and B. The technician who prepared the data sheets noted that as you combine defensive measures, the cumulative effects within and between the categories confidentiality, integrity, and availability cannot just be added.

The proposed university system has 10 academic departments, a department of intercollegiate athletics, an admissions office, a bookstore, a registrar's office (grade and academic status management), and a dormitory complex capable of housing 15,000 students. The university expects to have 600 staff and faculty (non IT support) supporting the daily mission. The academic departments will maintain 21 computer labs with 30 computers per lab, and 600 staff and faculty computers (one per employee). Each dorm room is equipped with two (2) high speed connections to the university network. It is anticipated that each student will have a computer. The total computer requirements for the remaining department/agencies cannot be anticipated at this time. It is known that the bookstore will have a Website and the ability to sell books online. The Registrar's office will maintain a Website where students can check the status of payments and grades. The admissions office, student health center, and the athletic department will maintain Websites.

The average administrative employee earns $38,000 per year and the average faculty employee earns $77,000 per year. Current industry practice employs three to four system administrators (sysadmin) per subnetwork and there is typically one (1) sysadmin (help-desk support) employee per 300 computers. Additionally, each separate system of computers (for Web hosting or data management) is typically managed by one (1) sysadmin person.

The current opportunity cost projection (due to IT) with no defensive measures is shown in **Table 1**. The contributions of various risk categories—Confidentiality (C), Integrity (I), and Availability (A)—to a given cost are also shown in **Table 1**.

Table 1.
Current opportunity costs and risk Category contributions.

Opportunity Cost (due to IT)	Amount ($ millions)	Risk category contribution		
		C	I	A
Litigation	3.8	55%	45%	
Proprietary data loss	1.5	70%	30%	
Consumer confidence	2.9	40%	30%	30%
Data reconstruction	0.4		100%	
Service reconstruction	0.08		100%	
Direct revenue loss	0.25		30%	70%

Task 2

We know that technical specifications will change rapidly over time. However, the relations and interplay among costs, risk categories, and sources of risk will tend to change more slowly. Create a model for the problem in Task 1 that is flexible enough to adapt to changing technological capabilities and can be applied to different organizations. Carefully describe the assumptions that you make in designing the model. In addition, provide an example of how the university will be able to use your model to initially determine and then periodically update their IT security system.

Task 3

Prepare a three-page position paper to the university President that describes the strengths, weakness, and flexibility of your model in Task 2. In addition, explain what can be inferred and what should not be inferred from your model.

Task 4

Explain the differences that may exist in the initial Risk Category Contributions (**Table 1**) if you model IT security for a commercial company that provides a search engine for the World Wide Web (e.g., Google, Yahoo, AltaVista, . . .). Will your model work for this type of organization?

Task 5

Honeynets are designed to gather extensive information on IT security threats. Write a two-page memo to your supervisor advising whether a university or a search engine company should consider using a honeynet.

Task 6

To become a leader in IT security consulting, Rite-On Consulting must also take an active role in anticipating the future direction of information technology and advising companies on how to respond to future security risks. After performing your analysis, write a two-page memo to the President of Rite-On to inform him of the future of IT security. In addition, describe how your model can be used to anticipate and respond to the uncertain future.

Enclosure A

Technology Preventive Defensive Measures

[Editor’s Note: We omit the 11 pp of tables of Enclosure A, which are available in their entirety at `http://www.comap.com/undergraduate/contests/mcm/contests/2004/problems/icm2004.pdf` . We give a sample in **Table 2**, together with (below) the instructions for reading the table.]

How to read this table: The Qualitative Values are a judgment based on the assessment from industry experts on the tools’ effectiveness. Each defensive measure has several instances that vary in costs and effectiveness. The Low, Mean, and High values represent a characterization of reviews found in different consumer review periodicals as they relate to user productivity, confidentiality, integrity, and availability. The variability indicates the concentration of the data about the mean. The Low and High are the minimum and maximum possible values, respectively. Costs are in U.S. dollars. A factor value of 5.00% indicates an improvement of 5%. A value of -5.00% indicates that the

Table 2.
Sample from Enclosure A.

				Quantitative Values			
				Low	Mean	High	Variability
Host-based Firewall							
	Intelli-Scan	Direct Costs					
			Procurement/computer	n/a	$45.00	n/a	
			Maintenance/year/computer	n/a	—	n/a	
			Training/year/sys admin	n/a	$1,000.00	n/a	
		Factors					
			User Productivity	−2.00%	−1.00%	0.00%	Low
			Confidentiality	9.00%	28.00%	38.00%	High
			Integrity	9.00%	28.00%	38.00%	High
			Availability	9.00%	18.00%	28.00%	Med

factor is degraded by 5%. These values are modifiers to the existing levels. For example from a base Confidentiality level of .8 a factor value of −25% would result in a new Confidentiality factor of $0.8 - (0.8 \times 0.25) = 0.6$. A positive value results in a positive change in the factor.

Enclosure B

Policy Preventive Defensive Measures

[EDITOR'S NOTE: We omit the 2 pp of tables of Enclosure B, which are available in their entirety at the Web address noted earlier. We give a sample in **Table 3**; the instructions for reading the table are the same as for Enclosure A.]

Table 3.
Sample from Enclosure B.

			Quantitative Values			
			Low	Mean	High	Variability
Strong Passwords						
	Costs					
		Policy implementation	n/a	$45,000	n/a	Low
		Training/year per Sys Admin	$8,000	$12,000	$15,000	Med
		Training/year per user	$3	$5	$12	Med
		Maintenance costs	$10,000	$12,000	$20,000	Med
	Factors					
		User Productivity	9.00%	28.00%	38.00%	Med
		Confidentiality	9.00%	28.00%	38.00%	Low
		Integrity	9.00%	28.00%	38.00%	Low
		Availability	9.00%	18.00%	28.00%	Low

The Results

Solution papers were coded at COMAP headquarters so that names and affiliations of authors would be unknown to the judges. Each paper was read preliminarily by at least two "triage" judges at the U.S. Military Academy at West Point, NY. At the triage stage, the summary, the model description, and the overall organization are the primary elements in judging a paper. If the judges' scores diverged for a paper, the judges conferred; if they still did not agree on a score, additional triage judges evaluated the paper.

Final judging by a team of modelers, analysts, and subject-matter experts took place March 5 and 6, again at the U.S. Military Academy at West Point, NY. The judges classified the papers as follows:

			Honorable	Successful	
	Outstanding	Meritorious	Mention	Participation	Total
IT Security	4	26	51	62	143

The four papers that the judges designated as Outstanding appear in this special issue of *The UMAP Journal*, together with commentaries. We list those teams and the Meritorious teams (and advisors) below; the list of all participating schools, advisors, and results is in the **Appendix**.

Outstanding Teams

Institution and Advisor	**Team Members**
"It's All About the Bottom Line" Harvey Mudd College Claremont, CA Hank Krieger	Eli Bogart Cal Pierog Lori Thomas
"Making the CIA Work for You" Harvey Mudd College Claremont, CA Jon Jacobsen	Warren Katzenstein Tara Martin Michael Vrable
"Firewalls and Beyond: Engineering Information Technology Security" United States Military Academy West Point, NY Elizabeth W. Schott	Dennis Clancey Daniel Kang Jeffrey Glick

"Catch Thieves Online: IT Security"
University of Electronic Science and Technology
Chengdu, Sichuan, China
Du Hongfei

Zhao Qian
Su Xueyuan
Song Yunji

Meritorious Teams (26 teams)

Asbury College, Wilmore, KY (David L. Coulliette)
Beijing University of Chemical Technology, China (Jiang Xinhua)
Beijing University of Posts and Telecommunications, Beijing, China (He Zuguo)
Beijing University of Posts and Telecommunications, Beijing, China (Sun Hongxiang)
Carroll College, Helena, MT (Kelly Slater Cline)
Harbin Institute of Technology, Harbin, Heilongjiang, China (Jiao Guanghong)
Harbin Institute of Technology, Harbin, Heilongjiang, China (Shang Shouting)
Jilin University, Changchun City, Jilin, China (Liu JinYing)
Maggie Walker Governor's School, Richmond, VA (John A. Barnes)
Montana Tech, Butte, MT (Richard J. Rossi)
Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, China (Yang Zhenhua)
Olin College of Engineering, Needham, MA (Burt S. Tilley)
Peking University, Beijing, China (Liu Yulong)
Peking University Health Science Center, Beijing, China (Zhang Xia)
Rowan University, Glassboro, NJ (Hieu D. Nguyen)
Shanghai Jiaotong University, Shanghai, China (Zhou Guobiao)
South China University of Technology, Guangzhou, Guangdong, China (Qin Yongan)
Sun Yat-Sen University, Guangzhou, Guangdong, China (Wang Qi-Ru)
Tianjin University, Tianjin, China (Liu Zeyi)
Tianjin University, Tianjin, China (Rong Ximin)
Tsinghua University, Beijing, China (Deng Xi)
University of Science and Technology of China, Hefei, Anhui, China (Zhang Ziyu)
University of Science and Technology of China, Hefei, Anhui, China (Yang Zhang)
Xidian University, Xi'an, Shaanxi, China (Wang Xinhui)
Xidian University, Xi'an, Shaanxi, China (Ye Ji-Min)
Zhejiang University College of Science, Hangzhou, Zhejiang, China (Ji Min)

Awards and Contributions

Each participating ICM advisor and team member received a certificate signed by the Contest Directors and by the Head Judge. Additional awards were presented to the Harvey Mudd team advised by Hank Krieger from the Institute for Operations Research and the Management Sciences (INFORMS).

Judging

Contest Directors
Chris Arney, Dean of the School of Mathematics and Sciences,
The College of Saint Rose, Albany, NY
Gary W. Krahn, Dept. of Mathematical Sciences, U.S. Military Academy,
West Point, NY

Associate Directors
Richard Cassady, Dept. of Industrial Engineering, University of Arkansas,
Fayetteville, AR
Kathleen Snook, U.S. Army (retired), MA

Judges
Daniel Ragsdale, Dept. of Electrical Engineering and Computer Science,
U.S. Military Academy, West Point, NY
Caroline Smith, Dept. of Mathematics and Statistics,
James Madison University, Harrisonburg, VA
Frank Wattenberg, Dept. of Mathematical Sciences, U.S. Military Academy,
West Point, NY

Triage Judges
U.S. Military Academy, West Point, NY:
Dept. of Electrical Engineering and Computer Science
David Barlow, Ronald Dodge, Aaron Ferguson, Kenneth Fritzsche, James Jackson, Michael Lanham, Brian Layton, Thomas Morel, Timothy Nix, Daniel Ragsdale, and William Suchan

Dept. of Mathematical Sciences
Mike Arcerio, John Billie, Gabe Costa, Mason Crow, Jeff Fleming, Andy Glen, Paul Goethals, Alex Heidenberg, Mike Huber, Michael Johnson, Gary Krahn, Tom Lainis, Howard McInvale, Barbara Melendez, Chris Moseley, Joe Myers, Mike Phillips, Jack Picciuto, Tim Povich, Tyge Rugenstein, Raymond Smith, Bart Stewart, Frank Wattenberg, and Brian Winkel

Source of the Problem

The Information Technology Security Problem was contributed by Daniel Ragsdale and Ronald Dodge (Dept. of Electrical Engineering and Computer Science, U.S. Military Academy, West Point, NY).

Acknowledgments

Major funding for the ICM is provided by a grant from the National Science Foundation through COMAP. Additional support is provided by the Institute for Operations Research and the Management Sciences (INFORMS).

We thank:

- all the ICM judges and ICM Board members for their valuable and unflagging efforts, and
- the staff of the Dept. of Mathematical Sciences, U.S. Military Academy, West Point, NY, for hosting the triage judging and the final judging.

Cautions

To the reader of research journals:

Usually a published paper has been presented to an audience, shown to colleagues, rewritten, checked by referees, revised, and edited by a journal editor. Each of the student papers here is the result of undergraduates working on a problem over a weekend; allowing substantial revision by the authors could give a false impression of accomplishment. So these papers are essentially au naturel. Light editing has taken place: minor errors have been corrected, wording has been altered for clarity or economy, style has been adjusted to that of *The UMAP Journal*, and the papers have been edited for length. Please peruse these student efforts in that context.

To the potential ICM Advisor:

It might be overpowering to encounter such output from a weekend of work by a small team of undergraduates, but these solution papers are highly atypical. A team that prepares and participates will have an enriching learning experience, independent of what any other team does.

Editor's Note

As usual, some Outstanding papers were much longer than we can accommodate in the *Journal* (one was 129 pp long!); so space considerations forced me to edit the Outstanding papers for length. The code and raw output of computer programs is omitted, the abstract is often combined with the summary, and usually it is not possible to include all of the many tables and figures.

In addition, I have omitted the position papers and most of the other supplementary materials requested in Tasks 3–6, since they do not include new mathematical modeling not already present in the bodies of the reports.

In all editing, I endeavor to preserve the substance and style of the paper, especially the approach to the modeling.

—Paul J. Campbell, Editor

Appendix: Successful Participants

KEY:

P	=	Successful Participation
H	=	Honorable Mention
M	=	Meritorious
O	=	Outstanding (published in this special issue)

INSTITUTION	CITY	ADVISOR	I
CALIFORNIA			
Harvey Mudd College	Claremont	Art Benjamin	H
		Jon Jacobsen	O
		Hank Krieger	O
COLORADO			
University of Colorado at Denver	Denver	William L. Briggs	P
ILLINOIS			
Greenville College	Greenville	George R. Peters	P
Monmouth College, Physics	Monmouth	Michael Kroupa	H
IOWA			
Luther College	Decorah	Eric R. Westlund	P
Simpson College, Bio. & Geology	Indianola	Jeffrey Parmelee	P,P
KENTUCKY			
Asbury College	Wilmore	David L. Coulliette	M,H
		Ken P. Rietz	P
MASSACHUSETTS			
Olin College of Engineering	Needham	Burt S. Tilley	M
MARYLAND			
Villa Julie College	Stevenson	Eileen C. McGraw	H
MONTANA			
Carroll College	Helena	Mark R. Parker	H
		Kelly Slater Cline	M
		Holly S. Zullo	H
Montana Tech	Butte	Richard J. Rossi	M
NEVADA			
Sierra Nevada College, Env'l Eng.	Incline Village	Christopher John Damm	P
NEW JERSEY			
Rowan University	Glassboro	Hieu D. Nguyen	M

INSTITUTION	CITY	ADVISOR	I
NEW YORK			
Concordia College—New York	Bronxville		
Computer Info. Services		Daniel Burroughs	P
United States Military Academy	West Point		
Mathematical Sciences		Michael J. Smith	P
		Sakura Sen Therrien	P
Systems Engineering		Elizabeth W. Schott	O
NORTH CAROLINA			
North Carolina State University	Raleigh	Jeffrey S. Scroggs	P
Western Carolina University	Cullowhee	Erin K. McNelis	P
OHIO			
Ohio Wesleyan University	Delaware	Richard S. Linder	P
Youngstown State University	Youngstown		
Mathematics		George Yates	P,P
Physics		Michael Crescimanno	H
VIRGINIA			
Maggie Walker Governor's School	Richmond	John A. Barnes	M,H
CHINA			
Anhui			
Anhui University, Electronics	Hefei	Chen Mingsheng	H
Hefei University of Technology	Hefei		
Applied Mathematics		Yang Liu	P
Computing Mathematics		Bao Chaowei	P
		Ding Xiaojing	P
Univ. of Science and Technology of China	Hefei		
Electronic Science and Technology		Zhang Yang	M
Special Class for the Gifted Young		Zhang Ziyu	M
Beijing			
Beijing Institute of Technology	BeiJing	Li Bingzhao	P
		Cui Xiaodi	H
Beijing Jiaotong University	Beijing		
Chemistry		Bing Tuan	P
Information Science and Computation		Liu Minghui	P
Physics		Guochen Feng	H,P
Transportation		Wang Xiaoxia	H,P
Beijing University of Chemical Technology	Beijing		
Applied Chemistry		Cheng Yan	H
Chemical Engineering		Jiang Xinhua	M
Electric Science		Shi Xiaoding	P

INSTITUTION	CITY	ADVISOR	I
Beijing Univ. of Posts and Telecomm.	Beijing		
Institute of Information Engineering		Ding Jinkou	P
School of Science		He Zuguo	M
		Sun Hongxiang	M
Beijing University of Technology	Beijing	Xue Yi	P
Peking University	Beijing		
Health Science Center		Zhang Xia	M,H
Mathematical Science		Guo Maozheng	H
		Liu Yulong	M,P
		Yang Jiazhong	H
Tsinghua University	Beijing		
Applied Mathematics		Xi Deng	M
Mathematics	Huang Hongxuan	H	
		Jiang Qi-yuan	H
		Lu Mei	P
Chongqing			
Chongqing University	Chongqing		
Computer Science		Yang Xiaofan	H
		Wu Kaigui	H
Mathematics and Physics, Statistics		Liu Qiongsun	P
Mathematics and Science		Yang Dadi	P
Guangdong			
Jinan University	Guangzhou		
Electronics		Ye Shiqi	P
Mathematics		Fan Suohai	H
		Ju Daiqiang	H
South China University of Technology	Guangzhou		
Applied Mathematics		Qin Yongan	M
Applied Physics		Liang Manfa	H
College of Science		Tao Zhisui	P
Sun Yat-Sen University	Guangzhou		
Mathematics		Wang Qi-Ru	M
Physics		Bao Yun	P
Scientific Computing & Computer Appl.		Chen ZePeng	P
Heilongjiang			
Harbin Institute of Technology	Harbin	Jiao Guanghong	M,H
		Shang Shouting	M
Harbin Univ. of Science and Technology	Harbin	Li Dongmei	H
		Tian Guangyue	H,P
Harbin Engineering University	Harbin	Gao Zhenbin	H

INSTITUTION	CITY	ADVISOR	I
Harbin Normal University, Information Science	Harbin	Liu Huanping	P
		Zeng Weiliang	P
Northeast Agricultural University	Harbin		
Biological Engineering		Tang Yan	
Industrial Engineering		Li FangGe	P
Hubei			
Wuhan University of Technology	Wuhan		
Mathematics		Huang Xiao wei	P
Statistics		Li Yuguang	P
Jiangsu			
Nanjing University of Posts and Telecomm.	Nanjing		
Applied Mathematics and Physics		Qiu ZhongHua	P
Computer Science and Technology		Li Xinxiu	P
Optical Information Technology		Yang Zhenhua	M
Nanjing University of Science & Technology	Nanjing		
Applied Mathematics		Wang Pinling	H
Mathematics		Chen Peixin	H
		Huang Zhengyou	P
Southeast University	Nanjing	Cao Hai-yan	P
		Sun Zhi-zhong	P
		Wang Li-yan	P
Jilin			
Jilin Univerisity	Changchun City		
Applied Mathematics		Yang Guang	H
Machinery and Engineering		Pei Yongchen	H
Mathematics		Liu JinYing	M
Telecommunication		Cao Chunling	P
Liaoning			
Dalian University	Dalian		
Applied Mathematics		He Mingfeng	P
		Wang Yi	P
		Zhao Lizhong	H
Info. Engineering		Zhang Changjun	P
Shaanxi			
Northwestern Polytechnical University	Xi’an		
Applied Mathematics		Xu Wei	H
Applied Physics		Lu Quanyi	P
		Xiao Huayong	H
Institute of Natural & Applied Science		Zhao Xuanmin	P

INSTITUTION	CITY	ADVISOR	I
Xidian University	Xi’an		
Applied Mathematics		Wang Xinhui	M
Computer Science		Ye Ji-Min	M
Shandong			
Shandong University, Math & Sys. Sci.	Jinan	Huang Shu xiang	H
Shanghai			
East China Univ. of Science and Tech.	Shanghai	Su Chunjie	H
		Sun Jun	H
Fudan University	Shanghai	Cai Zhijie	H
		Cao Yuan	H
Shanghai Jiaotong University	Shanghai	Huang Jianguo	H
		ZhouGuobiao	M
Sichuan			
Univ. of Electronic Science & Technology	Chengdu	Qin Siyi	P
		Zhang Yong	H
		Du Hongfei	O
Tianjin			
Nankai University	Tianjin		
Mgmnt Information Systems		Huo Wenhua	P
Computer Science		Liu Zeyi	M
Information Management		Rong Ximin	M
Zhejiang			
Hangzhou University of Commerce			
Information & Computing Science		Zhao Heng	P
Mathematics		Zhu Ling	H,H
Statistics		Zhao Heng	P
Zhejiang University			
Applied Math.	Hangzhou	Tan Zhiyi	H
City College, Computer Science		Huang Waibin	H
		Kang Xusheng	H,H
Mathematics		Ji Min	M,H
FINLAND			
Mathematical High School of Helsinki	Helsinki	Johannes Kärkkäinen	H,P
Päivölä College	Tarttila	Merikki Lappi	P,P
INDONESIA			
Institut Teknologi Bandung	Bandung	Sapto Wahyu Indratno	H
		Edy Soewono	H
		Kuntjoro Adji Sidarto	P

INSTITUTION	CITY	ADVISOR	I
IRELAND			
University College Dublin	Dublin	Rachel Quinlan	P

Editor's Note

Unless otherwise specified, the sponsoring department is the Dept. of Mathematics, Mathematical Sciences, or Mathematics and Computer Science.
For team advisors from China, we have endeavored to list family name first.

It’s All About the Bottom Line

Eli Bogart
Cal Pierog
Lori Thomas
Harvey Mudd College
Claremont, CA

Advisor: Hank Krieger

Summary

A brand-new university needs to balance the cost of information technology security measures with the potential cost of attacks on its systems. We model the associated risks and costs, arriving at an equation that measures the total cost of a security configuration and then developing two algorithms that minimize the cost. Both algorithms give a total cost just over half the cost of no security and just over 1.5 times the theoretical minimum cost.

Our model’s lack of assumptions about the structure of the university allows the model to be used with any kind of organization, requiring only a set of opportunity costs and statistics about the size of the organization. Our model can even suggest upgrades to existing security systems by changing the costs associated with current security measures.

We consider two extreme cases that bound our solution area and also test the sensitivity of our results by varying the parameters to see the impact on the security configurations chosen by the algorithms. In addition, we analyze equal-cost configurations that lead to different levels of risk.

Introduction

We develop a model to evaluate and optimize choices of security systems for a new university, which could easily be extended to another organization.

- We make assumptions to simplify the problem.
- We present our method for calculating the cost of a combination of security measures.

- We develop a reduced-search-space brute-force algorithm and an iterative algorithm that use the cost formula to find an optimal security configuration.
- We report and analyze the results of these algorithms.
- We discuss the extensibility and flexibility of our approach, with particular attention to how it could be applied to an organization of considerably different priorities, such as a major commercial Internet search engine.
- We discuss improvements and further developments.

Assumptions

A university's computer systems must support activities ranging from word-processing to scientific simulation, from Web-hosting to accounting, for tens of thousands of users on a day-to-day basis. Our client may have as many as 35,000 networked computers [Levine et al. 2003], differing in their operating systems, configurations and primary purposes, and extensively organized into subnetworks and departments. This scope and complexity, combined with the ever-increasing number and diversity of threats to information security, and the wide variety of countermeasures available to combat those threats, make precise optimization of the school's information technology security a challenge. To simplify this process, we make several assumptions:

- **All security measures are applied universally.** We assume that a single, uniform package of defensive measures and policies is implemented for every computer on campus (although our model supports the ability to individually analyze subsystems). This assumption allows us to disregard any security-related interactions between differently-protected subsystems.
- **At most one security measure of each type.** Two security measures designed to protect against the same category of threat are highly likely to have overlapping capabilities. If we have two spam filtering programs, we would expect spam email detected by one program to be be flagged by the other, so that it is unlikely that operating both is profitable. On the other hand, this sort of redundancy could be desirable as a protection against system failure.
- **No redundancy or synergy among security measures of different types.** The presence or absence of a security measure or policy of one type cannot impact the effectiveness of a security measure or policy of any other type. In practice, system administrators could use the information provided by a network intrusion detection system to adjust the configuration of a firewall, improving its performance; but in the absence of any relevant data, ignoring these effects seems to be a relatively benign simplification of the problem.
- **Five-year time frame.** The procurement and installation of a security measure is a one-time cost, while the associated maintenance costs and security

benefits accumulate over time. Given the rapidly changing nature of security threats and computer technologies, it is reasonable to compare the net costs of security measures over five years.

- **Costs of security measures are independent.** The prices of different security products are independent, and we neglect any financial effects of installing multiple products at one time—simply put, there is no bulk discount. In this respect, our model is overly pessimistic; apart from any discounts, bulk installation would also be faster and cheaper. However, this assumption allows us our model to encompass systems with pre-existing components.

Cost Equation

Any analysis of risk requires a way to compare two security configurations and choose the better one. Our model accomplishes this by measuring the dollar amount that a security system will save over the next five years. This dollar amount has two components: attack costs and sunk costs. *Attack costs* accrue from information attack and the resulting litigation, data loss, loss of consumer confidence, and so on. *Sunk cost* is the price of implementing the security system plus the cost of maintaining it over five years. Additionally, the sunk cost includes the dollar estimate of the gain or loss in productivity caused by the security system. The sum of these two costs is total cost.

Attack Cost

To measure the cost of an attack, we could lump all costs together and assume that all security measures reduce that total cost. To do so would be overly simplistic, since three security measures that all reduce the same aspect of cost are not necessarily as effective as three that reduce different components.

We break the total risk into three components: information confidentiality, data integrity, and system availability [Levine et al. 2003]. The relative importance of the indices for confidentiality, integrity, and availability (C, I, and A) for a given company will drive its choices in security measures.

Table 1 of the problem statement allows us to break down the baseline cost (of no security whatever) into the three risk categories: $BaseCostC$ = \$ 4.3 million, $BaseCostI$ = \$ 3.585 million, and $BaseCostA$ = \$ 1.045 million, corresponding to confidentiality, integrity, and availability.

Each security device or policy affects C, I, and A in terms of percentage changes dC, dI, and dA from the initial values of 1. Positive changes reflect higher levels of confidentiality, integrity, and availability, so costs from attacks should decrease as the indices increase. We offer the following equation for the cost of an attack given n categories of security features and policies:

$$AttackCost = years \times \left(\frac{BaseCostC}{\prod_{i=1}^{i=n}(1+dC_i)} + \frac{BaseCostI}{\prod_{i=1}^{i=n}(1+dI_i)} + \frac{BaseCostA}{\prod_{i=1}^{i=n}(1+dA_i)} \right)$$

With no security features, the indicated products are all 1 and we get the baseline attack costs.

Sunk Cost

There are two aspects to sunk costs: money spent on security measures and change in productivity. The money spent includes the one-time cost of purchasing or implementing the measure or policy, maintaining it, and training individuals in its use. This amount can depend on the number of users, computers, and IT staff trained to work with the measure. We divide IT staff into two categories, help-desk workers and system administrators. The cost of training IT staff for each product is assigned to the appropriate category of staff. This provides a bit more realism for the model, as help-desk workers in general do not require as much training as system administrators.

The second aspect of the sunk cost is the change in productivity, P, which works much like the C, I, and A indexes used to determine attack costs. Increases in productivity should lead to decreases in the sunk costs, since increased productivity lessens the cost of the security feature, and the increase in productivity depends only on the existence of the security features, not on attacks. To calculate the change in productivity from the baseline, we subtract the base productivity value, getting

$$\begin{aligned} SunkCost = &\sum_{i=1}^{n}(procureCost + maintCost + trainCost) \\ &+ years \times \left(\frac{BaseValueP}{\prod_{i=1}^{n}(1+dP_i)} - BaseValueP \right) \end{aligned}$$

The $BaseValueP$ is the product of the number of users and the productivity per user, obtained by estimating the number of hours per year that the average user spends using the university's IT services and the replacement cost of those services (as estimated by our team).We arrived at $BaseValueP = \$12$ million. (Later, we analyze the sensitivity of the model to this value.)

The costs to purchase or implement and maintain security depends on the numbers of computers, users, and IT staff. **Table 1** lists the values that we chose to simulate the university.

Table 1.

Fixed input parameters for the model.

Variable	Value	Variable	Value
Computers	17,900	$BaseCostC$	\$4.3 million
System administrators	16	$BaseCostI$	\$3.585 million
Help-desk staff	55	$BaseCostA$	\$1.045 million
Users	17,000	Productivity per user	365
Years	5		

Total Cost

Combining our two equations, we get

$$TotalCost = \sum_{i=1}^{n}(procureCost + maintCost + trainCost)$$
$$+\ years \times \left(\frac{BaseCostC}{\prod_{i=1}^{i=n}(1+dC_i)} + \frac{BaseCostI}{\prod_{i=1}^{i=n}(1+dI_i)} + \frac{BaseCostA}{\prod_{i=1}^{i=n}(1+dA_i)} \right.$$
$$\left. +\ \frac{BaseValueP}{\prod_{i=1}^{n}(1+dP_i)} - BaseValueP \right)$$

Input

The C, I, and A multipliers and prices for each security measure are obtained from Enclosures A and B of the problem statement. We reduce the values for P by a factor of 10 to reflect reasonable changes in productivity due to any single product. We also ensure that each security category has a null option, with a cost of zero and values for C, I, A and P of 1. We create two categories of IT staff and split training costs for system administrators between the two categories.

Models and Approaches

We explore several approaches to optimizing the university's security configuration using the cost formula above.

Brute-Force Computation

Calculating the net cost of every combination of security features allowed by our assumptions and picking the best would be guaranteed to find the best security configuration within the parameters of our model. However, evaluation of the cost formula would be computationally intensive. If j_i security features (including the null feature) are available in the ith category, one feature can be chosen from each category in $j_1 \times j_2 \times \cdots \times j_n$ distinct ways. Once a set of features has been chosen, calculating the resulting effects on confidentiality, integrity, availability, and productivity requires $4(n-1)$ multiplications. Comparison of all possible security configurations thus requires

$$4(n-1)\prod_{i=1}^{n} j_n$$

multiplications. For the security features available to the university, this would be 4.77×10^{12} multiplications.

While many of these multiplications are repeated many times, allowing a good algorithm to reduce the total number of calculations drastically, the brute-force approach is nonetheless too numerically intensive to produce results within a reasonable time frame.

Refined Brute Force

Reducing the number of security features under consideration could substantially reduce the number of calculations required for a brute-force approach. To do this, we calculate the net cost of each security feature in isolation. If a feature, installed alone, results in more costs due to procurement, maintenance, and lost productivity than savings due to increased security, we assume that the feature will not become profitable as part of the optimal security configuration.

This assumption is plausible but not guaranteed. A security policy such as allowing wireless networking, which allows a great increase in productivity at the expense of confidentiality, integrity and availability, might become profitable in combination with a (hypothetical) inexpensive combination of security measures that increase the C, I, and A indexes more than enough to compensate. But most of the security measures that we are considering have small effects on productivity; their net cost is determined primarily by their installation and maintenance costs and their security benefits, which are proportional to C, I, and A. Such measures, if unprofitable on their own, are almost certain to become even less profitable in combination with other measures that reduce C, I, and A. We decided that such security features are safe to neglect. This eliminates 34 of 83 technological measures and settles 4 of the policy choices studied—many of which would have cost well over $1 million over five years—reducing the number of necessary multiplications to 600,000.

Cherry-Picking

As an alternative to reducing the size of the search space, we created an iterative algorithm to construct a security configuration. Starting from an undefended network, we repeatedly add the most profitable security feature available until one technological measure (possibly null) from each category had been acquired and all policy choices had been made. In addition to producing an effective overall security system, this process also provides an outline for acquiring security features piecewise, as could be required on a limited budget.

Results

Model Results

We ran both the Refined Brute Force and Cherry-Picking algorithms on the data set provided in the problem statement. The resulting total costs can be compared to each other but are not useful without a frame of reference. To provide that sort of framework, we ran both algorithms again, this time minimizing only one component of the cost, either attack cost or sunk cost. In both cases, both algorithms produced exactly the same security configuration and total cost, thereby giving lower bounds on the attack cost and the sunk cost for with the data set. We illustrate tradeoffs between attack costs and sunk costs in **Figure 1**. Lines of slope -1 consist of points with the same total cost. **Table 2** shows the security configurations for points A, B, C, and D.

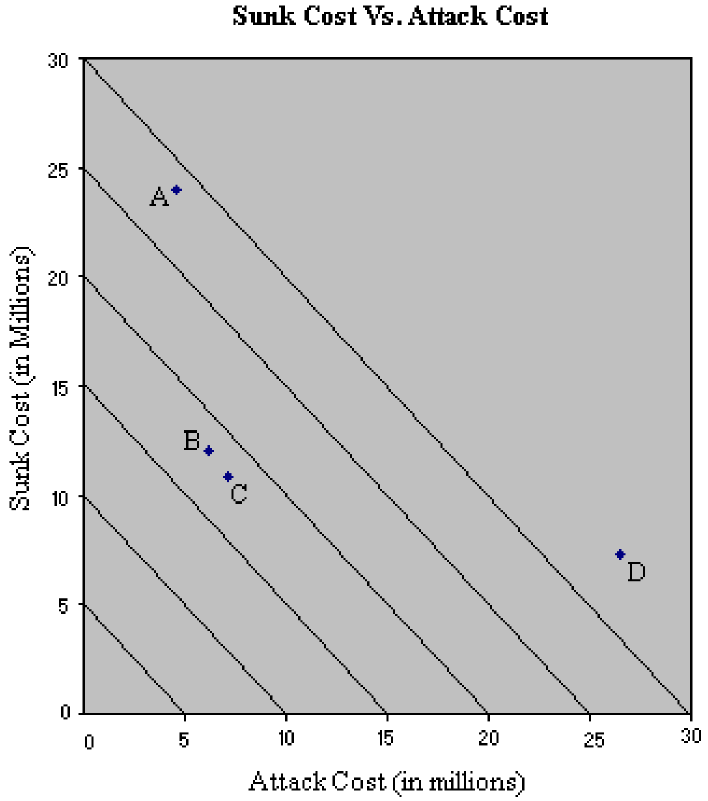


Figure 1. Sunk costs vs. attack costs. Diagonal lines are made up of points with equal cost. Point A which minimizes the cost of an attack regardless of the sunk cost. Point B is chosen by the Cherry-Picking algorithm. Point C is chosen by the Refined Brute Force algorithm. Point D minimizes the sunk cost, regardless of the cost of an attack.

No configuration can have an attack cost lower than that of point A nor sunk costs lower than that of point D. The vertical line through A and the horizontal line through D intersect at the theoretical lowest total cost—a combination of security features that costs almost nothing and reduces the cost of attack to almost nothing.

Table 2.

Products and policies for points A, B, C, and D in **Figure 1**.

category	A	B	C	D
Host Firewall	Intelli-Scan	Lava	Barrior	none
Net Firewall	EnterpriseLava	EnterpriseLava	none	none
Host Anti-Virus	BugKiller	Anti-V	Anti-V	none
Net Anti-Virus	Enterprise Stopper	System Splatter	System Splatter	none
Net IDS	Network Eye	Watcher	Watcher	none
Net Spam Filter	Spam Stopper	Spam Stopper	SpamStopper	none
Net Vulnerability Scan	none	none	none	none
Data Redundancy	none	none	none	none
Service Redundancy	none	none	none	none
Password Policy	Strong	Strong	Strong	Strong
Security Audit?	Formal	Formal	Formal	none
Wireless?	none	none	none	none
Removable Media?	none	none	none	none
Personal Use?	Restricted	Restricted	Restricted	Restricted
User Training?	Required	Required	Required	none
IT Staff Training?	Required	none	none	none

Deviation from Expected Attack Rates

In **Figure 1**, points B and C fall almost on the same line, so their total costs are almost equal. We would like to be able to distinguish between two points with similar total costs but different divisions of this total between sunk and attack costs. One way to do so is to consider what happens if the rate of successful attacks is different than expected.

- Suppose that the government cracks down on computer crime and only half as many attackers manage to break into the university networks; costs due to attacks will be half as much as before, benefitting those who spent more on attack costs than sunk costs.

- On the other hand, suppose that the number of attackers is more than anticipated. In this case, the amount spent on attacks is much larger than expected, so those who spent more on attack costs than sunk costs end up spending more than they had planned.

Figure 2 illustrates this point. A subscript 1 corresponds to cutting the rate of attack in half, a 2 to expected attack rates, and a 3 to doubling the attack rate.

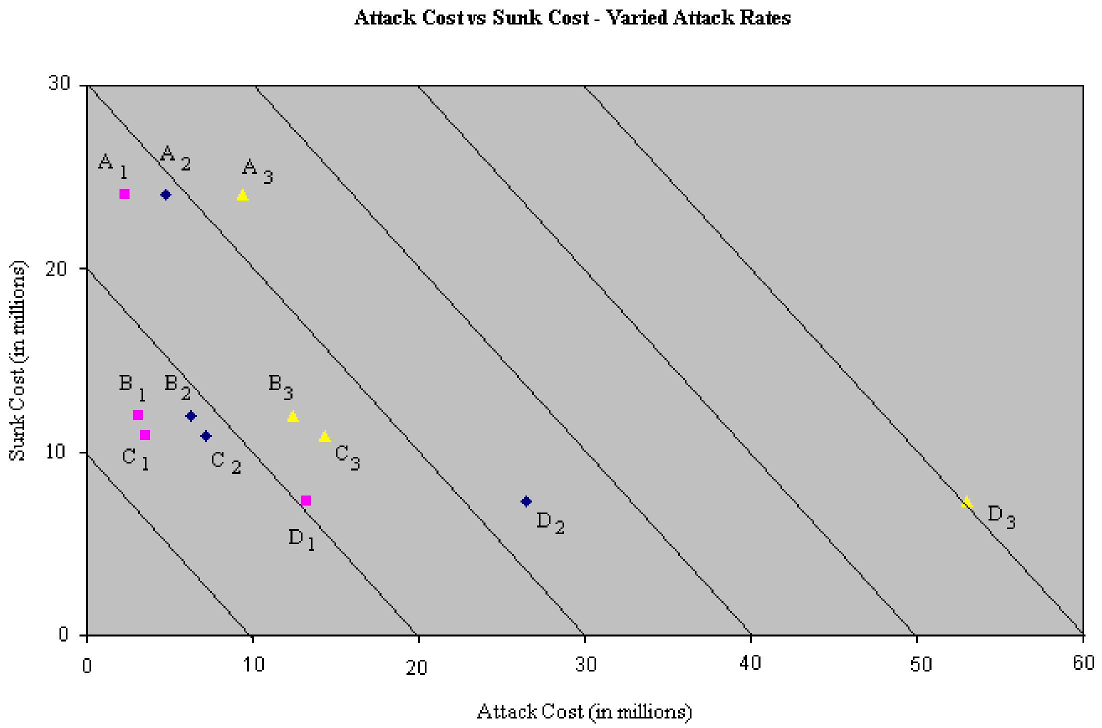


Figure 2. Points A, B, C and D correspond to minimizing attack costs, the total cost using the Cherry-Picking algorithm, the total cost using the Refined Brute Force algorithm and the sunk costs, respectively. Subscript 1 corresponds to half as much cost from attacks as expected, 2 to the expected cost from attacks, and 3 to twice the cost expected.

Among the points with halved attack rate, C_1 has the lowest total cost. However, when the attack rate is increased to twice the expected value, B_3 overtakes C_3, indicating that although the Brute Force algorithm (C) is best for low attack rates, the Cherry Picking algorithm (B) surpasses it when the attack rate increases.

Variation of Parameters

To test the robustness of our results, we individually varied $BaseCostC$, $BaseCostI$, $BaseCostA$ and $BaseValueP$ by a factor of 2 and by a factor of 1/2. These variations had a small effect on the security configurations chosen by the Refined Brute Force algorithm. The choice of host-based firewall varied the most in response to changes in values, with five of the nine configurations choosing Barrior, one choosing Watertight, and three choosing Lava. The next most varied was the choice of network-based firewall, with six choosing none and three choosing Enterprise Lava. Two of the configurations had single choices that differed from the other eight. These results suggest that our model is only somewhat sensitive to variations in these parameters with the restricted data set used by the Refined Brute Force algorithm.

We varied the same parameters by the same factors using the Cherry-Picking algorithm. Though the actual security configuration changed less than with the Refined Brute Force algorithm, the order in which each security feature was chosen varied from the norm in all but one case. Even when the order differed, it usually did not do so until the seventh or eighth purchase out of 16.

The two algorithms responded similarly to variation in the parameters except in the firewall categories, where there were consistent differences. The Refined Brute Force algorithm chose Barrior and no network-based firewall, where the Cherry-Picking algorithm chose Lava and Enterprise Lava in 10 instances out of 18. Thus, the two algorithms give generally consistent results and the inconsistencies are systematic to some degree.

Extensibility

The model makes no assumptions about the kind of organization under analysis and thus is highly adaptable and can be used to analyze any company or organization's computing resources. Our model simply requires three pieces of data to do its computations:

- A list of the currently available technologies and their expected impacts on confidentiality, integrity, availability, and productivity.
- The number of computers, users, and system administrators that the system is expected to support.
- How much the organization currently spends on confidentiality, integrity, and availability, as well as the estimated value of each user's productivity.

Since these parameters are not specific to any type of company or organization, any organization can be modeled, from universities to on-line banking to Internet search engines (see below).

Subsystems

What's more, our model can also analyze the security tradeoff of applying security features to only a subset of a larger system, such as buying a firewall for only one subnet on a university campus.

Using this method of breaking down a larger system into smaller subsystems, we can more effectively secure each subsystem, because we can choose a completely custom set of security measures for each subsystem individually. This means that each part of the organization's computing facilities can implement only the security that is most effective rather than following global security policies that only slightly benefit the particular subsystem, thereby not only increasing the overall security of the system but also substantially decreasing the cost of the security system.

Our model can also be utilized if the organization later decides to merge two subsystems or divide an existing system into several parts, even after the initial security system is in place.

New Technology

The constantly changing face of security makes periodic updating essential. Fortunately, our model allows analysis of security systems already in place, so it can re-evaluate an existing security system to see if it can be updated. Systems already in place receive an implementation cost of zero. Due to their presumed age, their effective confidentially, integrity, and availability must be recalibrated in light of emerging technologies.

Once we enter the old systems into the database, we use our analysis to determine if they are still financially viable. If maintenance costs exceed estimated utility, the systems' use should be discontinued. The analysis will additionally suggest upgrades or additional security systems that would be profitable to install.

Implementation Costs

However, projected income is not the only concern. Companies must also consider their limited cash on hand. For example, a security system that would save money over the next five years might be infeasible because the company does not currently possess enough financial reserves to cover the initial costs.

The Cherry-Picking Algorithm deftly addresses this concern, picking the most profitable systems first before others. In this manner, the company can most effectively allocate its limited financial reserves to the systems that will effect the largest profit increases. They need only start picking at the top of the list and working their way down until their security budget is expended.

Web Search Engines

The priorities of web search engines are very different from those of universities. Therefore a search engine's opportunity costs (as presented in the problem statement's **Table 1**) are quite differently distributed.

Consumer Confidence

Consumer confidence is of paramount importance to Web search engines. Nearly all search engines rely on advertising as their primary source of income. However, publicists are interested in advertising only with popular search engines, where the most users will see their ad. The financial situation of a search engine is intimately tied to its consumer confidence (usage), so it follows that a search engine's opportunity costs are primarily proportional to the consumer confidence category.

Service Reconstruction

Service reconstruction is closely related to consumer confidence. After all, a search engine can be viewed as a company that provides a solitary service: searching the Web. If a search engine is unable to provide this service to its users because of a security breach, it will lose consumer confidence: The longer the outage, the worse its effects. Thus, service reconstruction is another consumer confidence category in which search engines are interested.

Direct Revenue Loss

Although especially vulnerable to attack that damages consumer confidence, such as a denial-of-service attack, search engines are not susceptible to financial attacks such as a salami attack. The search engines' relative immunity to such attacks stems from the lack of financial transactions that involve the Website. Simply put, search engines do not have any sensitive data such as credit-card and bank-account numbers. This means that there is really no way for an attacker to steal money from the search engine, rendering the direct revenue loss category rather inconsequential.

Proprietary Data Loss

Not only do search engines not store sensitive financial data, they do not store any private data at all. The purpose of a search engine is to allow people to quickly find data that is available to everyone. Therefore, all the information cached by a search engine is freely available to anyone with an Internet connection, meaning that search engines have very little proprietary data to lose. Attackers are therefore unlikely to cause proprietary data loss.

Data Reconstruction

This complete lack of proprietary data also helps the search engines with regard to data reconstruction. Since all the information housed by a search engine is freely available, attackers are unlikely to attempt to corrupt or sabotage the data. Moreover, if any data is corrupted, it can be restored by downloading a fresh copy from the Internet. From a search engine's point of view, the entire Internet is a backup copy.

Litigation

The majority of a search engine's users pay no fee, and so have little grounds for litigation since the search engine has no legal obligations to them.

More problematic from a legal perspective are the advertisers. The search engine is contracted by the advertiser to display an ad in a certain manner. If the search engine is unable to do so because of the nefarious work of an attacker, then the advertisers have grounds for lawsuit. However, the situations that would earn the ire of advertisers are exactly the same ones that would lower consumer confidence, that is, the site going offline. Therefore, while some attention must be paid to legal ramifications, the defensive measures involved would be the same as the consumer confidence category.

Directions of Further Work

The first priority of future work is to remove our assumption that one set of security features will be applied to every computer system within the organization. At present, entire categories of features (data and system redundancy) are excluded from configuration because they are far too expensive to implement campus-wide. In fact, those features are not intended to be applied on such a large scale but only to critical systems and services. Our model is entirely capable of handling the implementation of different security features on subsets of an organization's computer systems; doing so would require only a breakdown of the university's computing needs into subnetworks, each with its own productivity and costs associated with confidentiality, integrity, and availability.

Another valuable refinement of this model would be in the method for assessing $BaseCostC$, $BaseCostI$, $BaseCostA$ and $BaseValueP$ for different components of the university or other organization. Hsiao [1979] assigns to each component of the IT network not only a value but also a probability of attack; the product of the two gives the expected cost of attack for that component. This cost could be broken down into costs due to C, I, and A, allowing us to consider each feature individually and its ideal security configuration. We could then go a step further and figure out how to group different components to share security features or policies in a cost-effective manner.

The value of our results would also be enhanced by relaxing our assumptions regarding redundancy and synergy among security features. Two security features could interact, with effects difficult to judge from information on the individual effect of each. Quantitative estimates of such interactions could be obtained in the same way as the data on individual security features, by polling of industry experts or experienced system administrators.

To highlight a particularly important synergy effect, a more-detailed model would acknowledge that as an organization's systems become more resistant to attack, not only will fewer attacks succeed but the organization will present a less-appealing target and fewer attacks will be launched. The provided estimates of security effects may take this into account for individual security features, but a successful combination of many security measures will have an even greater effect.

We have ignored the variation in the expert estimates of the effects of different security measures and policies. A more-detailed analysis could easily produce estimates of the uncertainty in our predictions of the savings resulting from each security configuration we propose. An improved version of our model would give priority to a security feature whose effects are known with reasonable certainty over a feature which is expected on average to be more beneficial but in which we can have no confidence.

Finally, to make this model more effective, it is essential to expand the number of security measures and policies considered. The nine types of technological defensive measures and seven policy defenses considered here hardly represent the entire spectrum of approaches. For example, no consideration has been given to physically protecting the university's hardware, a legitimate information technology concern with definite potential effects on the C, I, and A factors considered in the model. Perhaps worse, currently we consider only one nonspecific "user training" policy. Some form of user training is the best defense against "social engineering" attacks, which are already a major unrealized vulnerability and likely to become only more common in the future. Research into available measures to address physical and other security factors, and a closer examination of user training possibilities, would make our model potentially much more powerful.

References

Greenberg, Eric. 2003. *Mission-Critical Security Planner: When Hackers Won't Take No for an Answer*. New York: Wiley.

Honeynet Project. 2003. Know your enemy: Honeynets—What a Honeynet is, its value, how it works, and risk/issues involved. http://project.honeynet.org/papers/honeynet/index.html . Last modified 12 November 2003.

Hsiao, David K. 1979. *Computer Security*. New York: Academic Press.

Levine, John, Richard LaBella, Henry Owen, Didier Contis, and Brian Culver. 2003. The use of honeynets to detect exploited systems across large enterprise networks. *Proceedings of the 2003 IEEE Workshop on Information Assurance*, United States Military Academy, West Point, NY, June 2003. http://www.tracking-hackers.com/papers/gatech-honeynet.pdf .

Spitzner, Lance. 2003. Honeypots: Simple, cost-effective detection. http://www.securityfocus.com/infocus/1690 . Last updated 30 April 2003.

Making the CIA Work for You

Warren Katzenstein
Tara Martin
Michael Vrable
Harvey Mudd College
Claremont, CA

Advisor: Jon Jacobsen

Summary

We develop a general model for formulating network security systems with minimal costs. Applying the model to a hypothetical university results in a security system that costs 35% less than no security system. For a search-engine company, we create a system that costs 55% less than no security system.

Our model uses the standard categories of confidentiality, integrity, and availability (CIA) to create a security profile for a company. We determine an optimal combination of security measures from a set database. The result is a model that is flexible enough to initially and periodically assess a variety of company models and incorporate changes in security technology.

Our database groups defense measures into categories and the model selects at most one from each category. To combine measures, we assume that the essential functions of each category do not overlap. We rely on estimated CIA values and costs over a fixed length of time to compare defense measures. We use sensitivity analysis to indicate in which categories a particular product is most effective and in which categories the choice does not matter.

To improve our analysis of a university campus network, we next divided the university into departments of subnetworks. We analyze each separately, providing a $2 million reduction in savings over the whole-campus analysis.

The model can also be used to find appropriate updates to an existing security system; however, decrease in the effectiveness of the proposed security system over time is not taken into account.

The UMAP Journal 25 (2) (2004) 129–142.

Introduction

We propose a risk assessment model to evaluate the costs associated with network defense and to suggest a cost-optimal set of defense measures, according to the needs of an organization. We apply our model to a university network and Web search-engine company.

Network Security Risk Assessment Model

Terminology

Defense or Defensive Measure: A technical measure or a policy used by the organization to limit the potential cost of security problems.

Defense Class: A group of related defensive security measures, such as a host-based firewalls or anti-virus programs.

Confidentiality (C): The need to protect sensitive data from falling into the wrong hands.

Integrity (I): The need to prevent data modification by those who are not authorized to do so.

Availability (A): The need for computer systems to function properly and be available for use by authorized users.

Assumptions

- **We use reasonable estimates,** based on the provided potential costs of security attacks.
- **The effect of each defensive security measure on system security can be quantified.**
- **Four-year network lifespan** over which costs should be minimized.
- **Estimates remain valid for the duration of the time period.** The security risks and effectiveness of defensive measures do not appreciably change over time.

Basic Model

We are concerned with three types of costs faced by the university:

Risk Cost: Also referred to as “opportunity cost,” this is the potential cost of dealing with security problems, including litigation, data loss, reconstruction, and direct revenue loss.

System Cost: The cost to implement the defensive security measures.

Productivity Cost: Costs associated with a loss in productivity from various security policies.

The goal is to minimize the total of these three costs.

Estimating System Costs

We use

$$\sum_{\text{defense measures}} (\text{procurement} + \text{annual cost} \times \text{time}).$$

Estimating Risk Costs

We break risk costs down into whether the risk is due to a loss of confidentiality, integrity, or availability (CIA) in the system. Our procedure is:

- **List possible costs** that may be incurred.
- **Estimate the monetary loss** that would result if that event occurred when no security measures were in place for each possible cost.
- **Estimate the likelihood** of an event occurring, expressed as the expected number of times the cost would be incurred per year. Multiply this by the monetary cost to get the *scaled risk cost*.
- **Proportion the total risk** between the three risk factors (confidentiality, integrity, and availability). Divide the scaled risk cost up according to these proportions to give the scaled risk contribution to each risk factor.

Summing up the scaled risk contributions for each risk factor gives the total initial risk cost per factor. That is, if F is a risk factor (one of CIA) and R_F is the risk cost due to F then:

$$\begin{aligned} R_F = \sum_{\text{all incidents}} & [(\text{cost of a security incident}) \\ & \times (\text{expected number of incidents}) \\ & \times (\text{importance of factor } F \text{ in attack})] \end{aligned}$$

We introduce three risk factors, denoted C, I, and A, for confidentiality, integrity, and availability. By convention, a risk factor of 1 denotes no change from the initial risk cost; values larger than 1 denote improved security (and hence lower cost). The final adjusted risk cost is calculated by dividing the initial risk cost for each category by the corresponding risk factor.

The addition of network and computer security measures lowers the risk costs. Each defensive security measure is evaluated according to how well it protects the confidentiality and integrity of data and the availability of systems.

Estimating Total Costs

The total cost may depend on the number of computers, number of system administrators (sys admins), and other variables. Some costs are one-time procurement costs, while others are ongoing (yearly) costs. In our model, we consider the costs for a fixed number of years but report the average yearly costs. We spread one-time procurement costs over the number of years modeled.

Each defensive measure has a potential impact on the productivity of users, which is measured as a percentage. This percentage is interpreted as measured relative to the salaries of the affected users. To compute productivity costs, a productivity factor P is computed in the same manner as C, I, and A, and then the total salary of all users is divided by P. We report the difference between this value and the original total.

Interaction Between Defenses

A defensive strategy combines many different measures, so it is important to understand how combinations of measures affect the total cost.

In some cases, defensive measures are complementary: Anti-virus software and a firewall protect differently against threats, and so the total effect can be treated as cumulative. But installing 10 anti-virus products on a single computer does not provide 10 times the protection of a single product, since most anti-virus products protect against the same types of attacks.

We use at most one defensive measure of each type (host-based anti-virus, spam filter, etc.). We allow host-based and network-based products of the same type to co-exist, since their strengths are somewhat distinct.

To evaluate the total change in C, I, A, and P due to a set of defenses, we use the following rule. Let S be a set of defensive measures and let ΔC_s denote the change in confidentiality provided by defense $s \in S$. For this single defense, we say that

$$C = C_{\text{old}} + C_{\text{old}} \Delta C_s = C_{\text{old}}(1 + \Delta C_s).$$

We generalize to say that for the collection of defenses,

$$C = \prod_{s \in S} (1 + \Delta C_s)$$

and similarly for I, A, and P.

Refined Model Using Subnetworks

Different parts of the university have different security requirements (e.g., the registrar vs. a computer lab), so it does not make sense to choose a single uniform security plan for the entire university.

We treat the university as a collection of different "departments" and specify the initial risks of each department separately (**Table 1**).

Table 1.

Each department's fraction of the total risk of each type. Key:
1. Litigation 2. Proprietary data loss
3. Consumer confidence 4. Data reconstruction
5. Service reconstruction 6. Direct revenue loss

	(1)	(2)	(3)	(4)	(5)	(6)
Academic	0.20	0.90	0.15	0.20	0.35	—
Labs	—	—	0.10	—	0.30	—
Athletics	—	—	0.05	0.05	0.05	0.02
Admissions	0.15	0.10	0.30	0.20	0.05	0.40
Registrar	0.30	—	0.10	0.40	0.05	—
Book Store	0.05	—	0.15	0.10	0.05	0.40
Student Health	0.30	—	—	0.05	0.05	—
Dorm Network	—	—	0.15	—	0.10	—

For the most part, we compute costs separately for each department and add to get the total cost; but departments are not analyzed completely independently. Any cost that does not depend on the number of computers is paid only once, even if multiple departments use it; such a one-time cost could represent a site-license cost.

Search Method

We seek a minimum-cost solution over all possible defensive strategies. An exhaustive comparison of all strategies is not practical; even treating the entire university as a single unit, there are 50 billion possibilities to compare. Fortunately, it is not necessary to test all of these to develop a good defensive strategy.

In most cases, which defense (within a single defense class) is best is not sensitive to what other defenses are employed. That is, usually one or two network-firewall products will be best for an organization regardless of which anti-virus products, spam filters, and other products are also used. This allows us to optimize separately for each defense class; the resulting combination of defenses should then be very near to the global optimum.

We determine for each defense class the measure that seems to function best (averaged over multiple runs, with random selections of other defensive measures). The combination of all "best" defensive measures becomes the candidate best overall method. We then perform one or more "reoptimization" passes, where for each defense class we systematically evaluate all possibilities in the context of the current best guess at an optimum, to see if changes occur.

Other Extensions

- **Network lifespan:** We minimize the costs over a fixed number of years, typically four, in our simulations.

- **Updating systems:** While our model plans the security for a new network before it is built, it can also analyze the security of an existing network and suggest changes to lower the future costs.
- **Continual re-evaluation:** By running the model whenever changes in available technology or the security profile of the organization take place, the security system can always be maintained at the most up-to-date status.

Model Strengths

The model

- is flexible, designed to work in different situations from universities to companies,
- can be adjusted easily to incorporate new defensive security measures,
- can recognize differing security needs within an organization,
- can be used to evaluate both new planned networks and existing networks, and
- functions much more efficiently than a brute-force search.

Model Weaknesses

- We relate possible attack types, defenses against them, and risk costs only through the C, I, and A parameters.
- The model is sensitive to the quality of the data.
- We do not account for changes in the parameters with time.
- We do not account for all the ways that defensive measures may interact.

Results

University Results

We analyze the best defensive strategy in two cases: when the university is considered as a single unit **Table 2**, and when different groups within the university have different security requirements (**Table 3**).

The overall costs for the two strategies (in millions of dollars) are:

	Single-Unit Model	**Departmental Model**
Risk cost	2.34	2.03
System cost	6.14	3.82

Table 2.
Recommended system configuration for the university, treating all computers in the university equally.

Category	Product
Host-based firewall	Intelli-Scan
Host-based anti-virus	Anti-V
Network-based anti-virus	System Doctor
Network-based spam filter	Email Valve
Policies	Strong passwords, allow wireless, restricted personal use, user training, sys admin training

Table 3.
Recommended system configuration for the university when differing security requirements of different groups are considered.

Academics:
HB Firewall: Intelli-Scan
HB AV: Anti-V
NB AV: System Doctor
Spam: Spam Stoper
Policies: Strong Passwords, Allow Wireless, Restrict Personal Use, User Training, Sys Admin Training
Admissions:
HB Firewall: Intelli-Scan
NB Firewall: network Defense
HB AV: Anti-V
NB AV: System Splatter
IDS: Watcher
Spam: Spam Stoper
Policies: Strong Passwords Disallow Wireless, Unmonitored Personal Use, User Training, Sys Admin Training
Athletics:
HB Firewall: Intelli-Scan
HB AV: Anti-V
NB AV: Enterprise Stomper
NB Spam: Spam Stoper
Policies: Strong Passwords, Allow Wireless, Unmonitored Personal Use, User Training, Sys Admin Training
Bookstore:
HB Firewall: Intelli-Scan
NB Firewall: network Defense
HB AV: Anti-V
NB AV: System Splatter
IDS: Watcher
Spam: Spam Stoper
Policies: Strong Passwords, Disallow Wireless, Unmonitored Personal Use, User Training, Sys Admin Training
Dorms:
HB AV: Fogger
NB AV: System Splatter
IDS: Watcher
Spam: Spam Stoper
Policies: Strong Passwords, Disallow Wireless, Unmonitored Personal Use
Health:
HB Firewall: Intelli-Scan
NB Firewall: network Defense
HB AV: Anti-V
NB AV: System Splatter
Spam: Email Valve
Policies: Strong Passwords, Disallow Wireless, Restrict Personal Use, User Training, Sys Admin Training
Labs:
HB Firewall: Watertight
HB AV: Anti-V
NB AV: Bug Zapper
IDS: Watcher
Policies: Strong Passwords, Disallow Wireless, Unmonitored Personal Use, User Training
Registrar:
HB Firewall: Intelli-Scan
NB Firewall: network Defense
HB AV: Anti-V
NB AV: System Splatter
IDS: Watcher
Spam: Spam Stoper
Policies: Strong Passwords, Disallow Wireless, Unmonitored Personal Use, User Training

There is a cost savings of $0.31 million in risk costs and $2.32 million in system costs by considering different parts of the university separately. Considering requirements separately, security can be increased at the same time that costs are decreased, because necessary security measures are used where appropriate and cheaper defensive measures are used where more complex ones are not needed.

Web Search Engine

We also analyze the defensive measures that should be employed by a Web-search company. The initial risk costs are given in **Table 4**. These data were estimated based on our research into various search-engine companies; we also estimated appropriate risk costs and C, I, A values. Finally, to obtain an optimum security defense, we created two subnetworks.

Table 4.

Initial risk costs for a search engine. For each category of risk, the fraction of the risk due to confidentiality, integrity, and availability problems is given. The last column gives the contribution of that risk category to the total company risk.

Category	C	I	A	Fraction of total ($10 M)
Litigation	20%	20%	60%	5%
Proprietary Data Loss	70%	30%	—	5%
Consumer Confidence	—	30%	70%	30%
Data Reconstruction	—	100%	—	20%
Service Reconstruction	—	100%	—	10%
Direct Revenue Loss	—	10%	90%	30%

The rationale for this cost breakdown is:

- **Confidentiality:** Since search-engine companies have the majority of their data available to consumers, confidentiality is not as important as for a university. Confidentiality is important for financial records and in research and development.

- **Integrity:** A search-engine company depends on large data sets, so integrity of the data is important. However, accuracy (and hence integrity) of the data plays only a minor role in consumer confidence, direct revenue loss, and litigation.

- **Availability:** Search engines are utterly reliant on being available to consumers, so the CIA values reflect this, and any opportunity costs directly associated with consumers or advertisers are heavily weighted towards availability.

The recommended configuration suggested by our model is given in **Table 5**. The risk cost with this setup is $2.8 million (reduced from $10 million), at a system cost of $1.8 million.

Table 5.

Defensive security measures chosen for a web search engine.

Servers:	**Administrative:**
HB Firewall: Lava	*HB Firewall:* Intelli-Scan
HB AV: Bug Killer	*HB AV:* Anti-V
NB AV: System Splatter	*NB AV:* Blue Sky
IDS: Watcher	*Spam:* Spam Stoper
Spam: Spam Stoper	*Policies:* Strong Passwords, Allow Wireless, Restrict Personal Use, User Training, Sys Admin Training
Policies: Strong Passwords, Disallow Wireless, Unmonitored Personal Use, User Training	

No data or service redundancy measures are selected by our algorithm. The commercial data and service redundancy measures in our database are generally quite expensive; for a search-engine company with thousands of computers, the cost is prohibitive. More likely, a search-engine company would develop its own redundancy schemes tailored to its needs.

Sensitivity

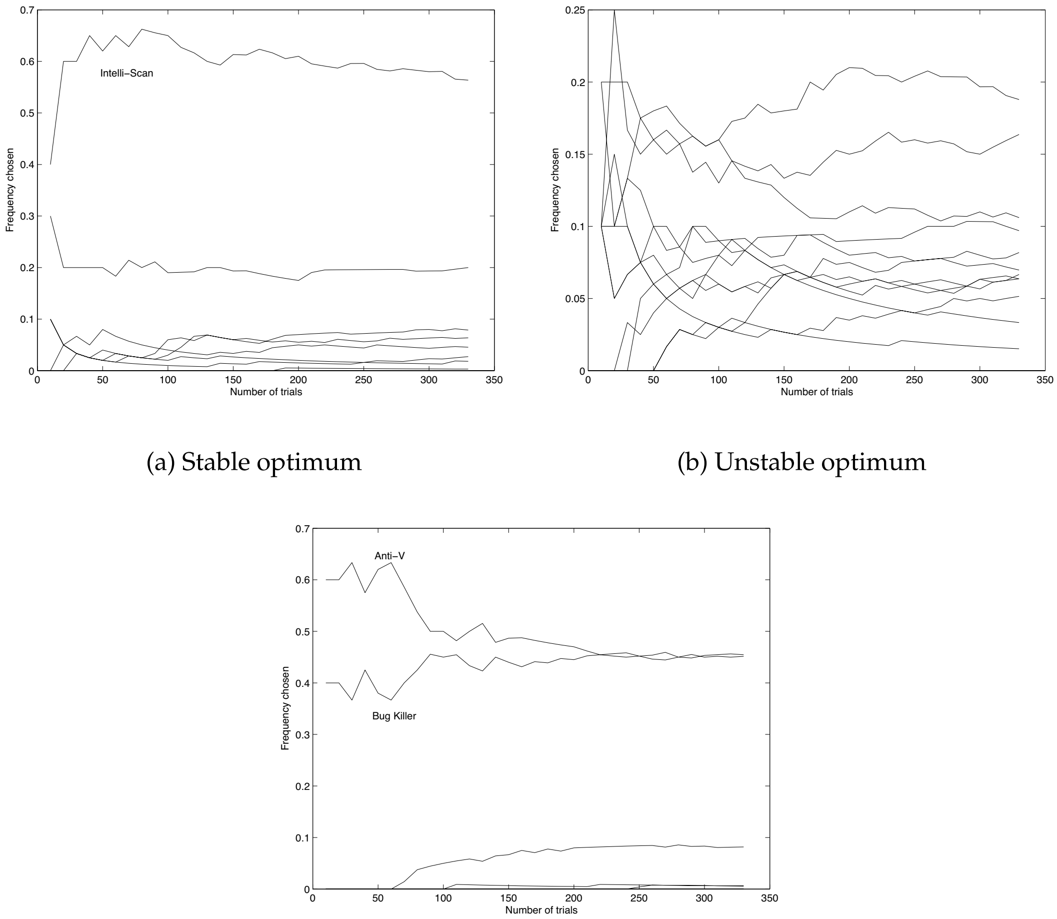
Factor values such as C, I, A, and P, as well as cost estimates for policy decisions, are estimates only. To incorporate the uncertainty in these values, we perform a sensitivity analysis using the estimated minimum and maximum factor values for defense measures. (Policy decisions were omitted for this analysis.)

- Each parameter value was randomly chosen from a uniform distribution between the specified minimum and maximum estimate values.
- Using these values, the network security system was optimized with the previously described method.
- The solution defense measures were logged.
- This process is iterated approximately 330 times.

Results are in **Figure 1**, with frequency that a defense measure is optimal plotted vs. number of trials. After sufficiently many trials, the frequency generally stabilizes, indicating theoretical stabilities.

Although the sensitivity analysis was done at the departmental level, several trends were consistent:

- Host-based firewall selection is generally stable, with Intelli-Scan preferred 60% of the time when a firewall is implemented.
- Decisions not to use a network based firewall are stable, but particular defense measures are not (40–50%).
- Host-based anti-virus is usually split between Anti-V and Bug Killer, with each being chosen in 45–50% of trials.



(a) Stable optimum

(b) Unstable optimum

(c) Split optimum

Figure 1. Sensitivity analysis using randomly chosen parameters, giving frequency that a defense measure is selected as the optimal choice vs. number of trials. (a) Intelli-Scan is chosen as the best host-based firewall for the academic departments in about 60% of trials. (b) Different network-based anti-virus software programs function about equally well in the academic departments. (c) In the dorms, the optimum host-based anti-virus is split between Anti-V and Bug Killer.

- Network-based anti-virus choices are highly unstable (20–30%).
- Intrusion-detection systems choices are stable in areas with a large number of computers (dorms, labs, academics), but much less so in smaller departments (admissions, bookstore, registrar).
- Spam-filter, network vulnerability scanning, data redundancy, and service redundancy choices are all very stable (90–100%).

Conclusion

To help an organization determine the appropriate set of security measures given its own security needs, we have developed a model for determining the total cost of any security policy. This model:

- **takes into account all costs:** risk costs, system costs, and productivity costs.
- **can distinguish between several types of security problems**, arising from failures in confidentiality, integrity, or availability.
- **can treat different parts of an organization separately.** Not all computers within an organization have the same security requirements; our model can assign them different security policies.
- **is flexible enough to satisfy the needs of a range of organizations, whether academic or commercial.**
- **can be used to choose the security measures for a completely new system or analyze and suggest improvements to an existing system.**
- **can efficiently determine a near-optimum solution**.

Using our system, we suggest security measures appropriate for a new university and a Web-search company:

- For the university, we suggest a system that **reduces expected costs by a third** relative to no security system.
- By tailoring the security policy to the different needs of each university sub-network, **we provide a further $2 million savings over a uniform security policy**.
- For the Web-search company, our proposed security policy **reduces costs by 55%**.

Memorandum on Honeynets

To: Mia Boss, Rite-On Consulting Executive
From: Awes Ome, Lowly Assistant

An organization should consider a honeynet to assess possible attack techniques and as a tool for determining already-compromised systems. Honeynets have been proven useful in a university setting but can be applied to any organization, provided methods for data control and data capture are in place.

Description

A honeynet is in one sense a decoy and in another a tool. It is a network of computers used solely to monitor attempts to gain access or to control the system. Since the honeynet network is passive, any activity detected is considered a threat. By monitoring and analyzing threats, system administrators can identify how their network can be compromised [Project Honeynet 2003]. Honeynets are thus a tool to identify the weaknesses of a system, new techniques that intruders have developed, and the compromised parts of a network.

Implementation

To implement a honeynet, one merely implements the architecture (**Figure 2**).

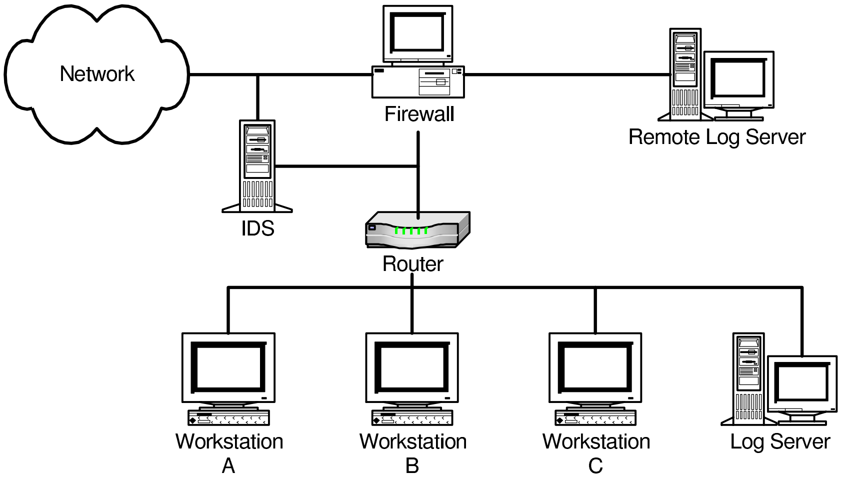


Figure 2. Honeynet architecture.

The two requirements that must be met are:

- **Data Control:** Limiting the amount of data that enters or leaves the system, so as to mitigate risk

- **Data Capture:** Monitoring and recording all activity within the honeynet system, since recorded data is what makes honeynets useful.

Risks

The two main risks an organization would be subjected to in implementing a honeynet system are liability and exposure.

Liability

Organizations can be held liable for any damages a compromised honeynet inflicts on other establishments. If the honeynet is compromised and the intruder is able to bypass the data controls, then the honeynet can be used to initiate malicious attacks on other companies or universities.

Exposure

A poorly implemented honeynet can also expose the organization and its network to an increased risk of attack. Once an intruder has compromised the honeynet, he is in the system's network and thus can use the honeynet to explore other areas [Brenton 2003; Project Honeynet 2003]. Thus, there are risks associated with a honeynet, and this is the reason why great care needs to be taken in implementing the data control aspect of the honeynet.

Benefits

The main benefits the honeynet would provide to the organization are:

- A method to monitor the types of attacks its network is vulnerable to and to detect computers and sub-networks that have already been compromised.
- By analyzing the data collected by the honeynet, system administrators can identify weaknesses in their system and develop methods to eliminate those weaknesses.
- The data a honeynet collects can help system administrators identify data patterns that are indicative of compromised systems and identify systems on the network that are compromised [Levine et al. 2003; Project Honeynet 2003].

In six months of operation, a honeynet system recently implemented at Georgia Institute of Technology detected 16 compromised systems [Levine et al. 2003]. This experiment has shown that honeynets can be effective in a university setting, if deployed properly. Since a university's network is similar to a search engine's, at least in terms of bandwidth and data throughput, companies with large infrastructures also stand to benefit from a honeynet.

References

Brenton, Chris. 2003. Honeynets. http://www.ists.dartmouth.edu/IRIA/knowledge_base/honeynets.htm .

Briesemeister, Linda, Patrick Lincoln, and Phillip Porras. 2003. Epidemic profiles and defense of scale-free networks. In *Proceedings of the 2003 ACM Workshop on Rapid Malcode*, 67–75. New YorK: ACM Press.

Carnegie Mellon Software Engineering Institute. CERT Coordination Center. http://www.cert.org/ .

Cooley, Al. 2004. Network security whitepaper: Using integrated solutions to improve network security and reduce cost. Astaro Internet Security. http://techlibrary.networkcomputing.com/detail/RES/1084902218_671.html .

Levine, John, Richard LaBella, Henry Owen, Didier Contis, and Brian Culver. 2003. The use of honeynets to detect exploited systems across large enterprise networks. In *Proceedings of the 2003 IEEE Workshop on Information Assurance*. http://users.ece.gatech.edu/~owen/Research/Conference%20Publications/honeynet_IAW2003.pdf .

Lipson, Howard F., and David A. Fisher. 2000. Survivability: A new technical and business perspective on security. In *Proceedings of the 1999 Workshop on New Security Paradigms*, 33–39. New York: ACM Press.

Moore, David, Colleen Shannon, Geoffrey Voelker, and Stefan Savage. 2003. Internet quarantine: Requirements for containing self-propagating code. In *Proceedings of the 2003 IEEE Infocom Conference*. http://www.cse.ucsd.edu/~savage/papers/Infocom03.pdf .

Honeynet Project. 2003. Know your enemy: Honeynets. http://www.linuxsecurity.com/feature_story-95-page2.html .

Schneier, Bruce. 2003. *Beyond Fear*. New York: Copernicus Books.

Shoniregun, Charles Adetokunbo. 2002. The future of Internet security. *Ubiquity* 3 (37): 1–13.

Teo, Lawrence, Gail-Joon Ahn, and Yuliang Zheng. 2003. Dynamic and risk-aware network access management. In *Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies*, 217–230. New York: ACM Press.

Zou, Cliff Changchun, Lixin Gao, Weibo Gong, and Don Towsley. 2003. Monitoring and early warning for Internet worms. In *Proceedings of the 10th ACM conference on Computer and communication security*, 190–199. New York: ACM Press.

Firewalls and Beyond: Engineering IT Security

Dennis Clancey
Jeffrey Glick
Daniel Kang
United States Military Academy
West Point, NY

Advisor: Elizabeth W. Schott

Abstract

Problem

A new university requires defensive measures to protect its network from unauthorized access, alteration of data, and unavailability. Without implementing defensive measures, the university is exposed to an expected loss of $8.9 million per year. Rite-On Consulting Firm has been tasked to conduct a risk analysis of information technology security for the university and to propose a model that minimizes costs while maintaining the highest possible level of security. This analysis addresses emerging technologies as an implied task.

Considerations

Our model stresses flexibility and simplicity. The model is run in Microsoft Excel, common software. Any company can cheaply tailor this powerful model to its individual needs. It can easily be updated to accommodate new tools and policies that reduce an organization's risk.

Results

Our model optimizes the mix of security tools and procedures. For the network-based measures, the new university should use the Network Defense Firewall, Enterprise Inoculation anti-virus program, Network Eye IDS, and a strong password policy. Additionally, the university should disallow wireless connections, have unmonitored personal use, and require user training.

The UMAP Journal 25 (2) (2004) 143–156.

The host-based decisions are divided into three subnetworks.

- The first subnetwork (admissions office, registrar, and health center) should use the Lava firewall, Bug Killer Anti-virus, and Robust Solutions service redundancy.
- Both the second subnetwork (academic departments and dormitories) and the third subnetwork (athletic department and bookstore) should use Intelliscan firewall, Bug Killer AV, Sonic Data data redundancy, and Web King SR.

Conclusions

The model provides the optimal balance of security and risk, based on associated costs. By simply altering the relative importance of security to each network resource, our model can recalculate an optimal solution with three clicks of a button. We are confident that the model for determining the optimal set of security tools and policies will greatly enhance the profitability of the new university for which it is designed. Our procedure and methodology could be used by other universities, businesses, and organizations trying to establish an optimal level of security in an information network.

Introduction

The creation of a new university requires the development of an information technology network with defensive measures protecting the university's assets from unauthorized access, alteration of data, and availability. The new university is expected to lose $8.9 million per year if no effective defensive measures are implemented. However, each defensive measure is extremely costly, and designing an affordable and effective defense requires careful analysis of the costs and benefits of various combinations of defensive measures.

We develop a model to minimize the costs and maximize the benefits in creating a secure network. The model assumes a law of diminishing return with every additional defensive measures.

Using a Monte Carlo simulation, the development of the model requires several critical assumptions. We ran 500 iterations of the simulation to find the optimal combination of defensive mechanisms.

The model reveals that the optimal suite of defensive measures costs $1.4 million and is expected to lower expected losses to $1.7 million, for a net savings of $5.9 million.

Problem Assumptions

- **All policies are network-wide.** For example, if we decide on a strong password policy, all resources on the network will be in accordance with that policy. Different policies for different departments are not allowed.

- Likewise, **network-based security measures (tools) are employed across the entire network.** If a particular type of network-based firewall is chosen, it is used to protect the entire network.
- Moreover, **each type of network-based tool can be chosen only once.** That means only one option for firewall can be used (and it can only be used once). Vertically stacking identical security measures at a network level produces no added benefit.
- **Normally distributed observations:** The performance data of each tool will follow a normal distribution if additional observations are taken. This was the basis for our creation of iterations; these iterations of independently performing tools was the basis of our Monte Carlo approach.
- **Sub-networks:** The network is additionally divided into three subnetworks, and we assume that each asset on a particular subnetwork has similar vulnerabilities. This assumption simplifies the use of host-based tools while making it easier for administrators to control uniform defensive measures.
- **Combinations:** A combination of tools that cover the same defensive measure is not allowed. For instance, two different firewalls cannot be employed at the same time. This is a model simplification that recognizes that the benefits of similar tools will do little to improve the systems when used together.

Problem Approach

We develop a model that uses marginal-benefit/marginal-cost analysis and considers both the cost of defensive measures and the opportunity cost associated with assumed risks. We create and implement a four-step method to develop the model: Network Infrastructure, Data Analysis, Risk Analysis, and Cost Analysis.

Network Infrastructure

The network infrastructure depends on the number and function of the computers within each department. This breakdown of computers by department was founded on both given information and estimates:

Departments are grouped into subnetworks based on similar functions and security needs. The network topology (**Figure 1**) creates constraints for the implementation of defensive measures. All hosts in each subnetwork must assume identical defensive measures. The model allows each subnetwork to select an optimal array of defensive measures best suited to its hosts.

Table 1.

Breakdown of computers by department.

Department	Computers
10 Academic Departments	1,230
Dormitory Complex	15,000
Department of Intercollegiate Athletics	30
Bookstore	15
Admissions Office	40
Registrar's Office	35
Health Center	35
TOTAL	16,385

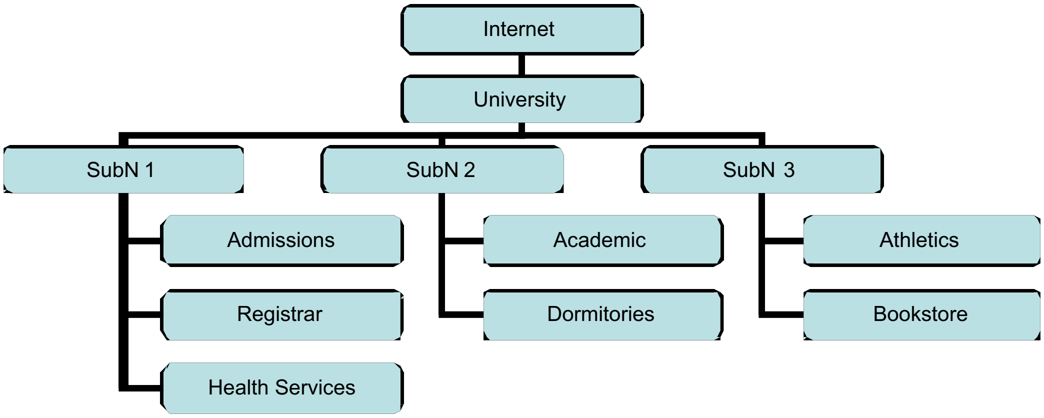


Figure 1. Proposed university network topology.

Data Analysis

Every tool and policy has associated costs and benefits. The direct costs come in the form of procurement costs, maintenance costs, and training costs. The benefits are measured by the degree to which a tool can improve (or detract from) user productivity, confidentiality, integrity, and availability. An improvement results in reduction in opportunity cost. For instance, if a particular tool improves confidentiality by 9%, then the opportunity costs associated with confidentiality will be reduced by 9%.

Quantitative information was provided in the problem statement enclosures for each piece of data: upper bound value, lower bound value, mean value, and variability level (concentration of the data about the mean).

Not knowing the standard deviation, the number of data observations, and the exact distribution, we simulate values, using Crystal Ball (a spreadsheet add-in with random-number generator capabilities [Decisioneering 2004]) and taking into account the possible range, the mean, and the variability. The Central Limit Theorem implies that if the number of observations is sufficiently large, then both their sum and their mean have approximately normal distributions, even when individual variables themselves are not normally distributed [Devore 2000].

We also consider issues relating to the spread of the data (distance between the minimum and maximum measured values). Extreme levels of variability do not necessarily follow the normal distribution; in cases of high variability, the distributions are likely to be flatter ("fatter in the tails") than the normal distribution. In cases of low variability, the curves will be more sharply peaked than the normal distribution.

The function `CB.Normal`(μ,σ,min,max) in Crystal Ball returns a value from a truncated normal distribution with mean μ and standard deviation σ and minimum and maximum values as specified.

To estimate the standard deviations, we divide the range $(\max - \min)$ by a specified factor depending on the level of variability. We wanted nearly all of the spread to be covered by three standard deviations. We settled on the values in **Table 2**.

Table 2.

Estimation of standard deviation.

Variability	Typical	Estimate of st'd dev.
high	0.32	range/6
medium	0.20	range/5
low	0.10	range/4

We were concerned about the accuracy of the simulated data in instances of an asymmetrical distribution (e.g., min = 0.05, mean = 0.17, max = 0.20). Crystal Ball creates a normal distribution with the inputted mean and standard deviation and then truncates it at the upper and lower boundaries. The mean of the resulting distribution can differ from the intended mean, as we confirmed from trial simulations After all considerations, we designed a spreadsheet that would generate actual values for all relevant costs and factors, taking into account levels of variability and ranges of values.

Risk Analysis

Table 1 of the problem statement quantifies the opportunity costs in dollars for various risks and apportions the risk to the categories of confidentiality, integrity, and availability. The university projects a total opportunity cost of \$8.93 million if a network is built without defensive measures.

The next step in the risk analysis process involves the calculation of a subjective vulnerability score for each department. Vulnerability "is a weakness in the security system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm . . . a particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access" [Pfleeger and Pfleeger 2003, 6]. A vulnerability differs from a threat, which is a "set of circumstances that has the potential to cause loss or harm" [Pfleeger and Pfleeger 2003, 6]. We use a threat/vulnerability work table to quantify each risk based on a 1–9 scale, thereby allowing each asset and risk category to be prioritized based on a summed value of the vulnerability scores. The priority system allows the model to focus control measures on risks that have the greatest impact (highest opportunity cost) and highest probability of affecting the asset. **Table 3** shows the assigned vulnerability scores.

Table 3.

Vulnerability work table.

		Impact		
		Low	Med	High
Probability	High	3	6	9
	Med	2	5	8
	Low	1	4	7

The table breaks vulnerability into two factors, probability and impact. Probability refers to the likelihood of the threat occurring, while the impact is the cost associated with a manifestation of that actual threat. A category with low probability and high impact is something that doesn't occur very often, but if it does happen, could be fairly costly. Something with high probability and low impact could happen all the time but the costs would be minimal.

Another worksheet, entitled "Risk Analysis Vulnerability Weighting System," allows the person conducting the risk assessment to give each department a vulnerability score.

Cost Analysis

Cost analysis creates a relationship between the opportunity cost associated with assuming risks and the cost of implementing defensive measures. Our model calls for a cost-benefit optimization. The sum of all these costs (in dollars) that the university is still exposed to in the form of risk (given a particular security combination) is represented by C_R.

The second main category of costs is the total cost C_T of security tools, which includes all aspects of security (training costs, tools, policies implementation, etc.).

The sum of the two main categories of cost is the total expected expenditure on security related matters, $E(TC_S)$:

$$E(TC_S) = C_T + C_R.$$

The total cost C_T is the sum of each tool cost, multiplied by the quantity:

$$C_T = \sum(\text{amt}_T \times \text{cost}_T).$$

For network-based security measures, the amount of the tool is always assumed to be 1. On the contrary, many host-based measures have multiple costs (per computer or per network).

The risk cost C_R has three components: confidentiality, integrity, and availability. The implementation of each tool leads to a corresponding change in opportunity cost associated with each component. The specific opportunity costs that make up C_R (e.g., litigation, service reconstruction, consumer confidence, etc.) are not necessarily important. However, the model is concerned with the degree to which a particular security measure changes opportunity costs in terms of confidentiality, integrity, and availability. Thus, C_R can be broken down as

$$C_R = C_{R_c} + C_{R_i} + C_{R_a}.$$

The subcosts that make up C_R depend on two pieces of information:

- the total original cost of each component in the absence of security measures (T_oC_c, T_oC_i, T_oC_a); and
- the degree to which that original value is decreased, the ξ-factor.

So we have

$$C_{R_c} = T_oC_c - \xi_c.$$

The complexity of this model is increased when you consider all possible combinations of multiple tools. Most notably, you cannot simply add the percentages of improvement when multiple tools are used. If you use two tools, each with a confidentiality improvement of 20%, it would be inaccurate to assume that the combined improvement is 20% + 20% = 40%; in particular, the improvement to risk cannot reach 100%.

We assume that the magnitude of incremental addition would decrease more slowly with lower levels of improvement than with higher levels. The best formula we could find to replicate this phenomenon is the $\tanh function$. The function $y = \tanh 1.05x$ is very nearly equal to x very closely until a 40% degree of improvement ($x = 0.40$), at which point the function starts to level off toward an asymptote of 1. Since $\tanh$ is symmetrical about 0, this formula performs in the same fashion for factors than detract or improve a given factor level.

The final step in this model is creating a formula for optimization. As the opportunity cost of risk decreases, the cost of tools increases. We need to minimize the overall costs incurred by the system,

$$\min(C_T + C_R).$$

We use the `Solver` function in Microsoft Excel to perform the optimization.

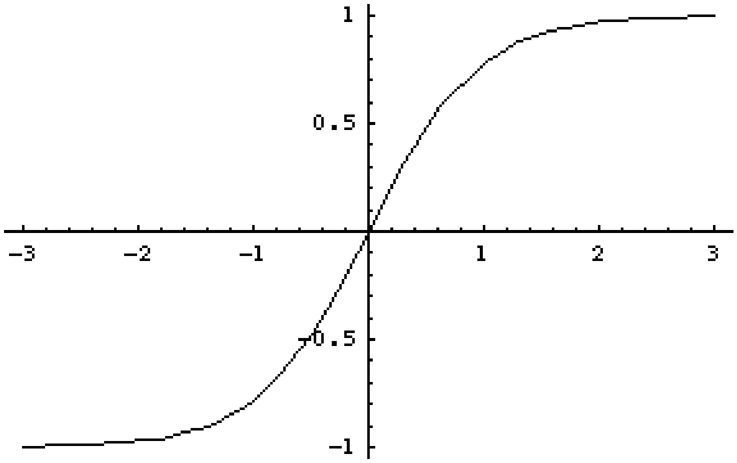


Figure 2. Net improvement vs. sum of improvement effects ($y = \tanh 1.05x$).

We use the truncated normal distributions to generate 500 random numbers (based on that distribution) for each data item, with each number representing a different iteration.

The decision variables are the amount of each tool that the network would use. Excel would search through all the possible combinations of decision variables and choose the set of decision variables that minimizes the cost equation over the 500 iterations.

We constrained the `Solver` function to

- force all decision variables to be integers (to eliminate the possibility of `Solver` recommending the use of a fraction of a resource, such as 54.34% of a firewall);
- force all decision variables to be nonnegative (so we would not recommend -2 firewalls); and
- choose each tool at most once for the network or each subnetwork (to avoid `Solver` recommending relying on 16 network firewalls), via constraining that the sum of all decision variables for a given tool should be less than or equal to 1.

The network policies have additional constraints. For instance, we assumed that we must select either a strong password policy or no password policy, so the sum of their decision variables must equal 1. Similar constraints apply to the use of wireless- and personal-use policies. Network-based decision variables are split into the subnetworks, for which similar constraints are made. `Solver` could choose a different combination of security measures for each subnetwork's host computers.

The degree to which a host-based system used on a particular network improved the overall network was based on the relative weight of importance of that subnetwork. For instance, if Subnetwork 1 accounts for 50% of the risk to overall confidentiality, and a tool improves it 20%, then the use of that tool improves the overall network by 20% × 50% = 10%. It was in this use of weights that the host-based options were chosen along side network-based tools and policies. The sum of factor improvements renders the value of ξ.

`Solver` ran every possible combination and found which combination minimized total cost the most over the 500 iterations.

Results

The optimal suite of defensive measures costs $1.37 million and is expected to lower its expected losses to $1.70 million, for a net savings of $5.86 million.

The tools recommended are:

- **Network Based Tools**
  - Network Defense Firewall
  - Enterprise Inoculation Anti-Virus
  - Network Eye IDS
- **Network Policies**
  - Strong Password Policy
  - Disallow Wireless
  - Unmonitored personal use
  - User training required
- **Host Based Tools**

Subnetwork 1	**Subnetwork 2**	**Subnetwork 3**
(Adm., Reg., Hlth)	(Acad. and Dorm)	(Athl. and Bkstr)
Lava Firewall	Intelliscan Firewall	Intelliscan Firewall
Bug Killer Anti-virus	Bug Killer AV	Bug Killer AV
Robust Solutions SR	Sonic Data DR	Sonic Data DR
	Web King SR	Web King SR

Strengths and Weaknesses

Strengths

The optimization model takes into account the delicate balance between the opportunity costs of the security risks (value of the assets) and the costs of implementing each additional defensive measure.

The model takes into account the proper use of the defensive measures by optimizing each subnetwork according to its function and requirements. The risk category of integrity would not affect Subnetwork 2 (Academic Departments and Dormitory Complex) as significantly as Subnetwork 1 (Registrar's Office and Admissions Office). Thus, different defensive measures are utilized for each subnetwork and the respective host computers.

By generating reliable observations (based on the normal distribution of supplied data), we simulated the performance of each allowable combination of tools and all possible defensive performances. Every possible outcome of these two factors was considered (over 500 iterations) to produce an optimal solution.

Weaknesses

University Infrastructure: The proposed infrastructure is a simplified topology of the university's network, but perhaps not the best.

Economics

The optimization model takes into account opportunity costs and the cost for the implementation of each defensive measure. However, information technology security cannot always be quantified. Certain human factors, behaviors, and other x-factors cannot necessarily be incorporated into a quantitative model.

Human Factors

When building the model, we did not differentiate between inside and outside attacks. For instance, users in the dormitory complexes are probably more likely to "hack" the system than users in the admissions dept. The optimal security design probably would have been altered if our model accounted for these specific considerations.

User Productivity

The technical data sheets provided give scores that indicate the degree to which each defensive product reduces opportunity costs in terms of integrity, confidentiality, and availability. Our model picks an optimal array of these products by considering costs broken down into these three categories. However, our model fails to consider another metric, User Productivity. For every product, the data sheets give a score that indicates the degree to which user productivity would be hindered by that defensive measure. Certain designs could lead to excessive slowing of the network, user frustration, prohibition of routine transactions, or reduction of potential profits. We certainly considered this factor, and the model even calculated the net reduction in user productivity (7%); but we did not assign a cost to user productivity and incorporate it into the objective function. Fortunately, 7% is not excessively large, so the reduction in user productivity appears to be acceptable.

Improvement by Combinations

The model did not fully explore the degree to which the combination of different tools would effect overall performance of the system. As a partial solution, we disallowed the use of a single defensive measure twice on the same network. We did not explore the overlap which might be present between separate measures, opting instead for modeling this phenomenon in terms of diminishing degrees of improvement (via the $\tanh$ function).

Conclusion

Our model for the security of the new university's network provides the optimal balance of security and risk, based on associated costs. As new technologies arise, they can be added to our current decision matrices.

Appendix: Honeynet Analysis

Purpose

To determine whether a university or a search-engine company should consider using a honeynet. This memorandum provides a basic introduction to honeynet strategies. In addition, we highlight innovative techniques for deploying these strategies in a myriad of applicable fields.

Introduction

Bears like honey. Honey is made by bees; bees hate bears.

The bears of IT are blackhats (hackers). Their objective is to wallow neck-deep in a vat of warm, sweet honey. In this analogy, honey is a forbidden commodity—restricted information. True hackers claim a benevolent mission; others, called "crackers," have malicious aims to compromise network resources.

Regardless of an intruder's aims, all can pose threats to a target system. Network administrators (white hats) need to monitor for instances of suspicious activity. On busy networks, the task of pinpointing unauthorized use is incredibly difficult. A hacker can appear and vanish across busy resources like a thief disappearing in the bustling crowd of a Chinese street market. To level this playing field, administrators snipe hackers in open fields, who are lured by the sight of "easy" honey. Here is how:

Honeypot: an information system resource with value that lies in the unauthorized or illicit use of that resource [Spitzner 2003]]. The honeypot resources have no production activity, no authorized activity. Since the honeypot is not a productive system, any interaction with that resource implies malicious or unauthorized use [Honeynet Project 2003]. This assumption of wrongdoing allows administrators to set up complex systems for observing intruder behavior. In doing so, administrators can learn from observations of new hacker techniques. This information fuels the development of updated anti-intrusion systems.

Honeynet: a network of honeypots created for an intruder to interact with.

Honeytoken: While honeypots are traditionally thought of as computers, (and other physical resources), a honeytoken broadens that paradigm. Honeytokens can be credit-card numbers, Excel spreadsheets, or even a bogus login [Spitzner 2003]. An example might be a medical file database containing an entry “John F. Kennedy.” Since there is no actual patient with that name, any interaction with that file is assumed to be unauthorized. These tokens can be spread over the network like honey barbecue sauce.

Honey farm: a configuration in which traditional honeypot locations serve as portals, secretly redirecting intruders to one centralized honeynet system. This organization makes the monitoring of a single environment much easier.

Benefits and Risks

Benefits [Project Honeynet 2003]

The advantage of a honeynet is that it allows an administrator to gain extensive data on the abilities and tactics of system intruders. The architecture of a honeynet is much like a fishbowl. It allows administrators to focus completely on a set of unauthorized actions. The traditional method of searching for hackers involved looking through gigabytes of data of a busy network (busied mostly by legitimate use). Searching busy resources is like searching for a needle in a haystack. The honeypot concept serves as a magnet to those needles—no searching necessary. The compilation of information on intruders allows a system administrator to tailor the defense of the network.

Risks [Project Honeynet 2003]

Harm: An attacker may break into a honeynet and then launch an attack that the system cannot forestall. In this case, an attacker will successfully harm the intended victim. Data control is the primary method of reducing this susceptibility to system failure. Each organization must decide which level of control they want. More control allows the intruder to do less, leaving less to be observed. Less control allows the intruder more flexibility but increases the possibility of an administrator losing control.

Detection: If an intruder is able to identify a honeynet, the value of that resource is dramatically reduced (to an observing administrator). An intruder can introduce false or bogus data into the honeynet, causing confusion for an administrator. In addition, an intruder might be able to identify the data-control and data-capture tools employed by the honeynet. If this occurs, an intruder can exploit the system architecture to gain access to non-honeynet resources.

Disable: There is risk that an intruder will disable the honeynet functionality. The intruder might be able to do this without the honeynet administrator realizing. This risk can be mitigated by having multiple layers of data control and capture.

Violation: If a honeynet is compromised, an intruder may attempt to use that resource for illegal activity. For example, the intruder might choose to upload and distribute illegal material, such as stolen credit cards or child pornography. This might cost the company painful litigation and additional penalties if they are found to be negligent in securing the resources involved.

Discussion

Although there are many risks associated with creating a honeynet, these risks can be mitigated by using a customized and random configuration, layering, some type of dynamism, or other creative means to make detection of the honeynet and countermeasures against it tough to accomplish. Any organization can find and tailor a honeynet to their acceptable risk exposure.

Recommendation

A university, search-engine company, or any other information system should employ some form of honeypot tactics. Combinations of the strategies allow white hats to seize the initiative in the battle against hackers, crackers, and dishonest employees. Additional cost/benefit analysis should be conducted to create an optimal honeynet configuration.

References

Decisioneering, Inc. 2004. Crystal Ball. Add-in software to Microsoft Excel under Microsoft Windows. `http://www.crystalball.com/crystal_ball/index.html` .

Honeynet Project. 2003. Know your enemy: Honeynets—What a Honeynet is, its value, how it works, and risk/issues involved. `http://project.honeynet.org/papers/honeynet/index.html` . Last modified 12 November 2003.

Devore, Jay L. 2000. *Probability and Statistics for Engineering and the Sciences.* Pacific Grove, PA: Brooks/Cole.

Peltier, Thomas R. 2001. *Information Security Risk Analysis.* New York: CRC Press.

Pfleeger, Charles P., and Shari Lawrence Pfleeger. 2003. *Security in Computing.* 3rd ed. Upper Saddle River, NJ: Prentice Hall.

Ragsdale, Cliff T. 2004. *Spreadsheet Modeling and Decision Analysis.* 4th ed. Mason, OH: South-Western.

Spitzner, Lance. 2003. Honeytokens: The other honeypot. `http://www.securityfocus.com/infocus/1713` . Last updated 21 July 2003.

Catch Thieves Online: IT Security

Zhao Qian
Su Xueyuan
Song Yunji
University of Electronic Science and Technology
Chengdu, Sichuan, China

Advisor: Du Hongfei

Summary

We construct an optimal defensive system for IT security for a university network. After estimating whether the security measures' effect is worth the expense, we develop a model to seek the minimum sum of opportunity costs and defensive system expense.

The model is composed of three modules.

- Module 1 mainly deals with the risk evaluation. We apply the Analytic Hierarchy Process (AHP) to clarify the miscellaneous risks and separate the complex university network into nine simple subsystems.
- Module 2 employs a fast search algorithm to determine a technological defensive system for each subsystem.
- Module 3 determines the policies for the whole university network system and calculates the total cost.

By using our model, we cut down the expense from an initial \$8.9 million to \$3.4 million. At the same time, this model is flexible enough to adapt to changing technological capabilities and can be applied to different organizations. Although the model has strengths such as modularization, high efficiency, and flexibility, it is a pity that we can only play defense—we do not have the initiative. If we want to change that fact, we urgently need new technologies, such as honeynets.

The UMAP Journal 25 (2) (2004) 157–169.

Introduction

Risks to IT security can be broken down into the three categories of confidentiality, integrity, and availability; hence, we face a problem in multiple-objective programming. Risk evaluation is very complex; there are not only quantitative standards of evaluation, but also qualitative standards that are difficult to measure. At the same time, the evaluation is affected by people's economic ideas, so a benchmark cannot be easily determined. In addition, the task of evaluation is dynamic, since it changes with the development of society. Hence, what we should do is analyze the cost and estimate whether the security system's effect is worth the expense. After the risk evaluation, we can set up a defensive system that balances the opportunity costs and the defense system expense, minimizing the total cost.

Assumptions

- Any complex computer network system can be separated into several unrelated subsystems by different functions. For example, the bookstore and the registrar's office are two different subsystems of a university.
- Different defensive measures play different roles in IT security system. For example, a network-based firewall and a host-based firewall perform different functions.
- Each new defensive measure has been evaluated before being made available; so we can use a new defensive measure in our model directly, because its effect is known.
- New defensive measures can only decrease the loss due to the aging of old defensive measures.

Table 1.
Symbol table.

Symbol	Meaning
T	Total cost of the whole network defensive system
c	Opportunity cost contributed by the Confidentiality risk
i	Opportunity cost contributed by the Integrity risk
a	Opportunity cost contributed by the Availability risk
d	Defensive expense, including procurement, maintenance, and system administrator training costs
T_j	Total cost for subsystem j
c_j	Confidentiality risk cost for subsystem j
i_j	Integrity risk cost for subsystem j
a_j	Availability risk cost for subsystem j
d_j	Defensive expense for subsystem j

Dealing with the Data

Enclosures A and B describe the technology and policy preventive defensive measures. The information was obtained by interviewing consumers, who gave each measure a rating. The data are summarized in terms of Low (minimum), Mean, and High (maximum) values, together with Variability (indicating the concentration of the data about the Mean), which is recorded as Low, Med, or High.

We need to determine a single value for each measure:

- If the Variability is Low, the opinions of different consumers are almost the same. We use the Mean value.
- If the Variability is Med, we assume that 10% gave the Low value, 10% the High value, and the rest the Mean. We calculate the value of the measure as

$$\text{Value} = 0.10 \times \text{Low value} + 0.80 \times \text{Mean value} + 0.10 \times \text{High value.}$$

- If the Variability is High, we assume that 20% gave the Low value, 20% the High value, and the rest the Mean. We calculate the value of the measure as

$$\text{Value} = 0.20 \times \text{Low value} + 0.60 \times \text{Mean value} + 0.20 \times \text{High value.}$$

Although the specific numerical values of 10% and 20% may not be suitable for all cases, the specific values in fact will not affect the models that we develop.

Optimal Defensive Measures for a University

If there are no defensive measures, the opportunity cost projection is as shown in **Table 2** and the total cost is

$$T = 3.8 + 1.5 + 2.9 + 0.4 + 0.08 + 0.25 = \$8.93 \text{ million.}$$

The initial Confidentiality risk cost is

$$c = 3.8 \times 0.55 + 1.5 \times 0.70 + 2.9 \times 0.40 = \$4.3 \text{ million.}$$

Analogously, the initial Integrity risk cost and the initial Availability risk cost are

$$i = \$3.585 \text{ million,} \qquad a = \$1.045 \text{ milliion.}$$

Each defensive measure affects four factors: User Productivity, Confidentiality, Integrity, and Availability. However, the cumulative effects within and between the risk categories cannot just be added. Hence, we shift our focus from the effect on the four factors to the effect on the costs. For example, from an

Table 2.

Current opportunity costs and risk Category contributions (data from the problem statement).

Symbol	Opportunity Cost (due to IT)	Amount ($ millions)	Risk Category Contribution		
			C	I	A
P1	Litigation	3.8	55%	45%	
P2	Proprietary data loss	1.5	70%	30%	
P3	Consumer confidence	2.9	40%	30%	30%
P4	Data reconstruction	0.4		100%	
P5	Service reconstruction	0.08		100%	
P6	Direct revenue loss	0.25		30%	70%

initial Confidentiality opportunity cost of $10,000, a factor value of 25% would increase the Confidentiality level by 25% and at the same time result in a new Confidentiality opportunity cost of $\$10,000 \times (1 - 0.25) = \$7,500$. Thereby, improvements attributable to specific measures are directly associated with decreases in costs. Moreover, costs can be added directly.

Based on such ideas, we consider the effects of different defensive measures in economic terms. Our task can be described as structuring an optimal network defensive system to minimize the total cost $T = c + i + a + d$, where c, i, and a are potential opportunity costs and d is expense on defensive measures.

We organize our model into three modules. Each module completes a specific task:

- Module 1 separates the whole university network system into several subsystems by different functions. After analysis of these subsystems, the initial opportunity cost is distributed among the subsystems. Hence the aim of our task becomes to find
$$\min T = \sum_j T_j.$$
- Module 2 determines the technological measures used for each subsystem to minimize the cost of the subsystem, that is, for subsystem j the task is to find
$$\min T_j = c_j + i_j + a_j + d_j.$$
- Module 3 determines the policies for the whole university network system and calculates the total cost.

Module 1: Apply AHP to Subsystems

The university's various components have different functions and hence different requirements for Confidentiality, Integrity, and Availability. So based on the structure and functions of the network, we separate the whole university network system into nine subsystems (**Figure 1**), designated A1–A9 in **Table 3**.

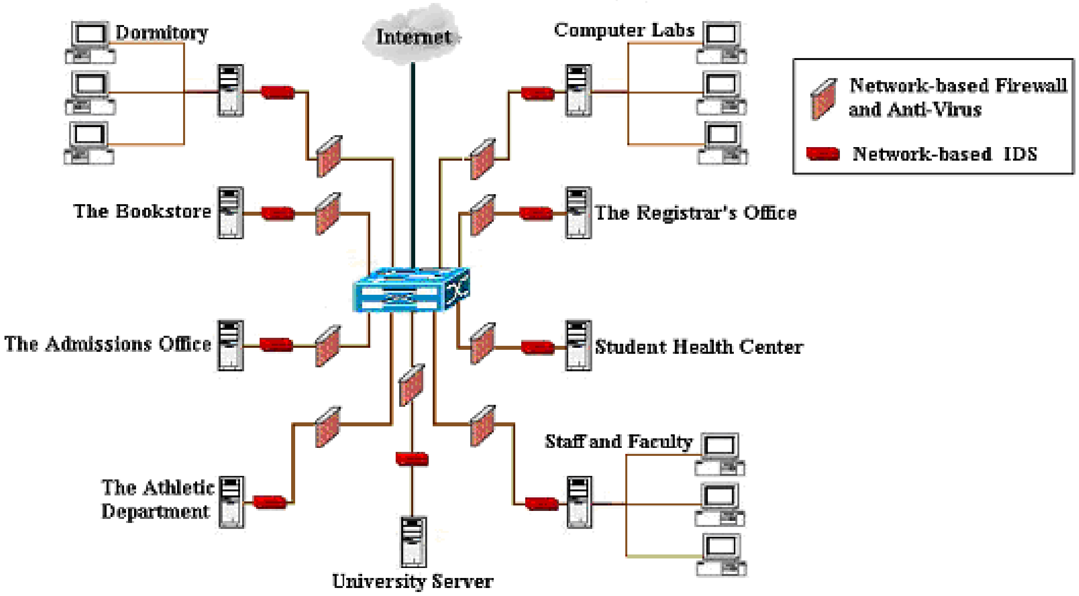


Figure 1. Separation of the network system.

Table 3.
Subsystems of the university network system.

Symbol	Subsystem
A1	Computer Labs
A2	Staff and Faculty Computers
A3	Dormitory Network
A4	Bookstore
A5	Registrar's Office
A6	Admissions Office
A7	Student Health Center
A8	Athletic Department
A9	University Server

We install a set of defensive systems for each subsystem. Such a defensive system defends against attacks on just that particular subsystem, so the cost of each subsystem can be calculated separately. We distribute the initial opportunity cost among the subsystems. We determine the weights for the subsystems by application of the Analytic Hierarchy Process (AHP) [Saaty 1980], a way to evaluate systems that involves both quantitative analysis and qualitative analysis. It exhibits the analytic and synthetic thoughts in decision-making strategy.

The hierarchy of the system is shown in **Figure 2**; A1–A9 stand for the nine subsystems in **Table 2** and P1–P6 represent the six kinds of opportunity costs in **Table 1**.

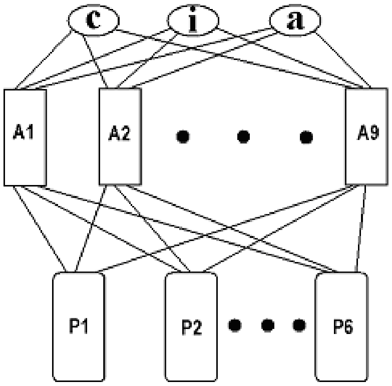


Figure 2. Hierarchy of the network system.

Our aim is to determine the weights for the risk categories distributed into each subsystem. As an example, we describe the calculation for the Confidentiality risk cost c. **Figure 3** shows the detailed c branch.

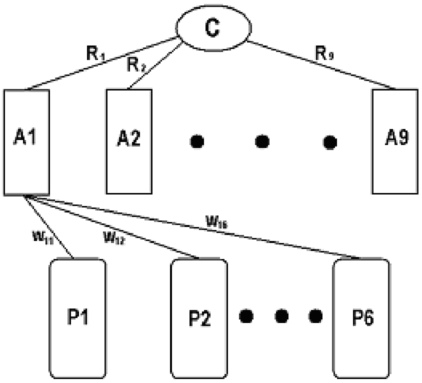


Figure 3. Detailed c branch.

We set up the equation

$$WR = T,$$

or

$$\begin{pmatrix} w_{11} & \dots & w_{91} \\ \vdots & & \vdots \\ w_{91} & \dots & w_{96} \end{pmatrix} \begin{pmatrix} R_1 \\ \vdots \\ R_9 \end{pmatrix} = \begin{pmatrix} t_1 \\ \vdots \\ t_6 \end{pmatrix}.$$

The elements w_{mn} are the weights of the six kinds of opportunity costs in each subsystem, where m is the subsystem and n is the kind of opportunity cost. For example, $w_{34} = P_4/c_4$ in subsystem A3, that is, w_{34} = (Data reconstruction loss)/(Confidentiality risk cost) in the dormitory network.

The elements R_m are the weights of the nine subsystems in risk categories. For example, $R_3 = c_3/c$.

The elements t_n are the weights of the six kinds of opportunity costs in the whole system. For example, $t_4 = P_4/c$, that is, t_4 = (Data reconstruction loss)/(Confidentiality risk cost) in the whole system.

Based on the analysis of the functions of each subsystem, we develop nine judging matrices to analyze the weight of each subsystem. Take A1 (Computer Labs), for example: The element P_{mn} represents the importance of P_m to P_n.

A_1	P_1	P_2	P_3	P_4	P_5	P_6
P_1	1	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}
P_2	$1/P_{12}$	1	P_{23}	P_{24}	P_{25}	P_{26}
P_3	$1/P_{13}$	$1/P_{23}$	1	P_{34}	P_{35}	P_{36}
P_4	$1/P_{14}$	$1/P_{24}$	$1/P_{34}$	1	P_{45}	P_{46}
P_5	P_{15}	P_{25}	P_{35}	$1/P_{45}$	1	P_{56}
P_6	$1/P_{16}$	$1/P_{26}$	$1/P_{36}$	$1/P_{46}$	$1/P_{56}$	1

Commonly, we use 1, 2, 3, . . . , 9 and their reciprocals to represent different degrees of importance: The larger the number, the more important the factor. While P_{mn} represents the importance of P_m to P_n, the importance of P_n to P_m is $1/P_{mn}$.

We normalize the column vectors in the judging matrix,

$$\overline{P_{mn}} = \frac{P_{mn}}{\sum_{k=1}^{6} P_{kn}},$$

and then add the normalized matrix in rows:

$$\overline{W_{mn}} = \sum_{k=1}^{6} \overline{P_{kn}}.$$

We normalize again to get

$$w_m = \frac{\overline{W_m}}{\sum_{k=1}^{6} \overline{W_k}},$$

The eigenvector w represents the opportunity costs' weights in the subsystem. Use the judging matrix P and eigenvector w, we calculate the maximum eigenvalue

$$\lambda_{\max} = \sum \frac{(PW)_m}{6W_m},$$

where $(PW)_m$ is the mth element of the vector Pw obtained as the product of the matrix P and the vector w.

Last, we check the coherence of the judging matrix. For a six-row matrix, the standard of coherence, CI, is calculated as

$$\text{CI} = \frac{\lambda_{\max} - 6}{5},$$

and if CI < 0.124, then the coherence of the judging matrix is suitable; otherwise, the judging matrix needs to be adjusted.

Following the approach indicated, we calculate the eigenvector of each subsystem's judging matrix and combine them into matrix W to get

$$W = \begin{pmatrix} 0.2756 & 0.0795 & 0.0795 & 0.4817 & 0.0502 & 0.0335 \\ 0.4290 & 0.2093 & 0.2093 & 0.0817 & 0.0415 & 0.0291 \\ 0.4606 & 0.0429 & 0.3384 & 0.0724 & 0.0429 & 0.0429 \\ 0.1057 & 0.0638 & 0.5650 & 0.0638 & 0.0396 & 0.1621 \\ 0.4334 & 0.2147 & 0.2147 & 0.0640 & 0.0433 & 0.0299 \\ 0.2463 & 0.1252 & 0.4579 & 0.0569 & 0.0294 & 0.0843 \\ 0.4547 & 0.2440 & 0.1771 & 0.0349 & 0.0349 & 0.0544 \\ 0.0949 & 0.0581 & 0.5641 & 0.1528 & 0.0949 & 0.0378 \\ 0.4455 & 0.1604 & 0.2306 & 0.0800 & 0.0288 & 0.0547 \end{pmatrix}$$

For the matrix T, we get

$$T = (0.4406 \;\; 0.2238, \;\; 0.2238 \;\; 0.0373 \;\; 0.0373 \;\; 0.0373)^T.$$

We calculate R as

$$R = W^{-1}T.$$

Two conditions must be fulfilled:

- The elements in matrix R must be nonnegative.
- The sum of the elements in R must equal 1.

Some adjustments may be needed to fulfill the conditions. At last, we get

$$R = (0.1674 \;\; 0.0435 \;\; 0.0000 \;\; 0.1915 \;\; 0.6120 \;\; 0.5364 \;\; 0.0000 \;\; 0.0000)^T.$$

The process described above is for the Confidentiality risk cost (c). The results for all opportunity costs are shown in **Table 4**.

Table 4.
Distribution details of opportunity costs.

	A1	A2	A3	A4	A5	A6	A7	A8	A9
c	0	16.74%	4.35%	0	19.15%	6.12%	53.64%	0	0
i	11.04%	9.84%	43.24%	0	0	0	18.91%	0	16.97%
a	0	0	0	73.18%	0	0	0	26.82%	0

From **Table 4**, we can know the distribution of initial opportunity costs among subsystems. For example, for A1 (Computer Labs), the Integrity risk cost is

$$i_1 = \$3.585 \text{ million} \times 11.04\% = \$0.395 \text{ million}.$$

With the distribution of initial opportunity costs among subsystems now available, we can determine the defensive system for each subsystem.

Module 2: Perform a Fast Search Algorithm

Defensive measures include technologies and policies. Technologies are hardware and software installed to protect the network; policies are guidelines publicized to instruct users' activities. Technologies should be different in each subsystem, according to the function it realizes; but policies should be the same throughout the whole network system.

Technologies

Technologies consist of host-based firewall (HF), network-based firewall (NF), host-based anti-virus (HA), network-based anti-virus (NA), network-based intrusion detection system (IDS), spam filter (SPAM), network-based vulnerability scanning (NVS), data redundancy (DR), and service redundancy (SR). We need to structure these technologies into several defensive layers.

Firewalls defend against attack from hackers, while anti-virus protects the server from the virus. Their effects must be considered together, since they form one defensive layer.

SPAM filtering, vulnerability scanning, data redundancy, and service redundancy are not real-time technologies. The form another defensive layer.

The defensive layers are shown in **Figure 4**.

The configurations of each subsystem are the same; the difference lies in which measure should be chosen in each defensive layer. Hence, the search process is the same for each subsystem. We describe our fast search algorithm:

1. For the first layer, we search the measure to minimize the total cost, finding a locally optimal solution.

2. We go on to the next layer. Based on the result of the previous layer, we combine the effects of different measures in this layer to find another locally optimal solution.

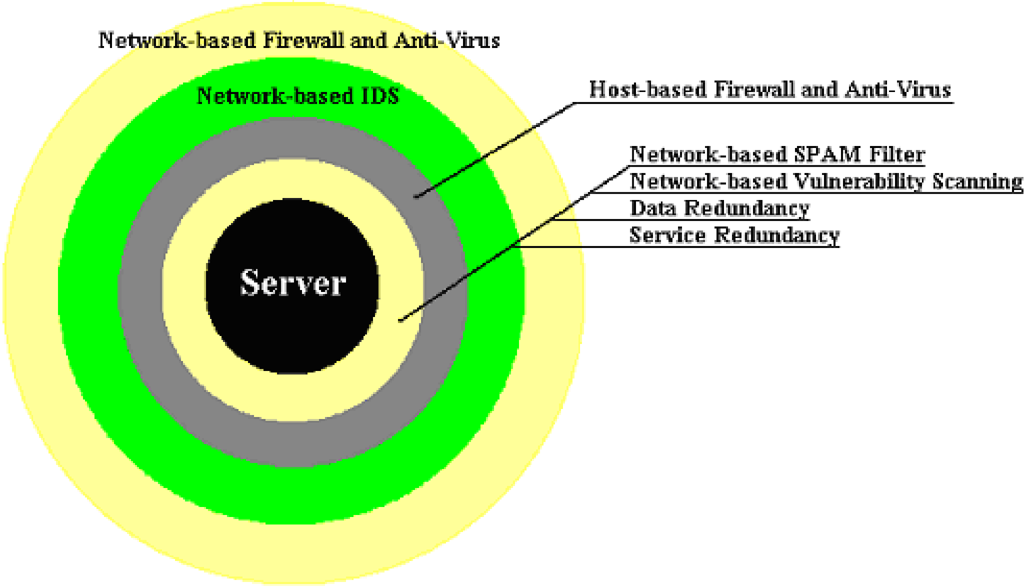

Network-based Firewall and Anti-Virus
Network-based IDS
Host-based Firewall and Anti-Virus
Network-based SPAM Filter
Network-based Vulnerability Scanning
Data Redundancy
Service Redundancy
Server

Figure 4. Technologies defensive layers.

3. Iterate Step 2 until all four defensive layers have been examined.
4. If all the measures of a technology cannot cut down the cost, it means that this technology is not needed. After the iterative search, the locally optimal solution will approach the globally optimal solution at last.

Following the search algorithm, we determine the technological measures suitable for each subsystem. The result is shown in **Table 5**.

Table 5.

Technological measures for each subsystem.

	NF	NA	IDS	HF	HA	SPAM	NVS	DR	SR
A1	2	2	8	1	1	0	0	0	4
A2	2	2	8	1	2	0	0	0	4
A3	2	2	8	1	1	0	0	0	4
A4	3	2	9	7	3	1	0	0	4
A5	2	3	9	1	2	0	0	0	0
A6	2	3	9	1	2	0	0	0	0
A7	2	2	2	1	2	0	0	0	4
A8	3	2	9	7	3	0	0	0	4
A9	2	2	8	1	1	0	0	0	4

This table shows the optimal defensive systems for each subsystem. The numbers in the table represent the sequence number of measures in each technology. For example, for A1 (Computer Labs), we choose the 2nd measure (Network defense) for Network-based Firewall and 8th measure (Network eye) for Network-based Intrusion Detection System. Note that 0 means that none of the measures of such technology is suitable, so this technology is not needed for the subsystem; for example, SPAM, NVS, and DR are not needed for A1.

Using the technological measures in **Table 5**, we calculate the effect of such measures for each subsystem. By adding such effects, we get the effect for the whole system (**Table 6**).

Table 6.
Effects of technologies (in millions of dollars).

	c	i	a		Total
Initial opportunity cost	4.3	3.6	1.0		8.9
Opportunity cost after technology defenses	1.5	1.0	0.4		
plus cost in technologies				0.5	3.4

Module 3: Determine the Policies

Policies to instruct users' activities should be the same throughout the whole network system. There are seven kinds: Passwords, Formal Security Audits, Wireless, Restrict Removable Media, Personal use, User Training and Sys Admin Training.

We check the effect of each policy by following the search algorithm that we used in Module 2. The result is shown in **Table 7**.

Table 7.
Policies for the network system.

Area	Policy
Password	Strong
Formal Security Audits	No need
Wireless	Disallow
Restrict Removable Media	No restriction
Personal Use	Unmonitored
User Training	Needed
Sysadmin	No need

The economic effect of this set of policies, after adoption of the technologies prescribed, is shown in **Table 8**.

Table 8.
Effects of policies (in millions of dollars), after adoption of recommended technologies.

	c	i	a		
Opportunity cost before policies	1.5	1.0	0.4		2.9
Opportunity cost after policies	0.8	0.5	0.2		
plus cost of policies				1.3	2.9

In all, the effect of the recommended defensive system is shown in **Table 9**.

Table 9.
Effect of the whole defensive system (in millions of dollars).

	c	i	a	d	Total
Cost with no defensive system	4.3	3.6	1.0	0	8.9
Cost under recommended defensive system	0.8	0.5	0.2	1.8	3.4

The minimized total cost is

$$T = c + i + a + d = 0.8 + 0.5 + 0.2 + 1.8 = \$3.4 \text{ million.}$$

Updating the IT Security System

Every organization has a potential opportunity cost that can be broken down into the three categories of Confidentiality, Integrity and Availability, which costs we choose as parameters. Additionally, the model separates the whole network system into subsystems by network structure and functions. These issues do not change in different organizations. So this model has a universal character and can be used in defensive system design for all kinds of organizations.

At the same time, technical specifications change over time. With the progress of technology, new attack measures are taken by hackers, and our security system will lose its power. Hence, we should update the security system regularly. But two questions lie before us:

- Which kind of new technology do we need?
- How often should we update the security system?

To answer the questions, we assume that the effect of all technologies decreases periodically and new technologies appear at the same time. Based on these assumptions, we describe our measure as follows:

- The first technology to replace is the one with the poorest effect.
- The time to update the system is not fixed but is based on the current security system's state and the capability of the new technology.
- We evaluate the cost when new technology appears. If the application of new technology can decrease the total cost further, then the old technology should be replaced.

We take the bookstore (A4) as an example to describe our approach. From the earlier result, we know that the opportunity cost of the bookstore is $.7318 \times \$1{,}045{,}000 = \$765,000$, all of it contributed by Availability (**Table 1**). Hence, when new technology appears, only the effect on availability should be taken into consideration. Suppose that every month a new kind of host-based firewall appears and the effect on availability of the firewall in use decreases by 3%. With the rapid decrease of effect, host-based firewall becomes the weakness of the security system.

- Suppose that the security system of the bookstore is established in April. The host-based firewall in use is "watertight" and its effect on availability is 19.4%.

- In May, the effect reduces to 16.4%. If there were no firewall, the opportunity cost of the bookstore would be $16,839 this month. Firewalls defend against attack from hackers, while antivirus protects the server from viruses, so their effects are additive. We assume that firewalls and antivirus protects each have 50% of the protective effect, so the current firewall reduces the opportunity cost by $\$16{,}839 \times .164 \times 50\% = \$1{,}381$. At the same time, a new host-based firewall appears whose effectiveness on Availability is 20.3%, while it costs $1,045 to install. If the new firewall is installed, considering the installation cost, it reduces the opportunity cost by $\$16{,}839 \times .102 - \$1{,}045 = \$1{,}709 - 1{,}045$ = $664. It is clear that keeping the old firewall is more suitable.

- Things change again in June. Since the effect of the original firewall reduces to 13.4%, it can cut down the cost by only $1,128. In this month, another new host-based firewall appears; assume that its effectiveness on Availability is 19.2%, while it costs $1,015 to install. So, the application of the new firewall reduces the cost by $1,617 − $1,015 = $602. It is still not worth the expense.

- In July, we again evaluate the opportunity cost. The effect of the original firewall is 10.4%, so it can save just $876. The effect of the new firewall is 23%, and it costs $1,045 to install. The application of the new firewall saves $1,937 − $1,045 = $892. With the new firewall, we can save $16 more. So we should update the firewall in July.

References

Brin, Sergey, and Lawrence Page. 2000. The anatomy of a large-scale hypertextual Web search engine. `http://www-db.stanford.edu/~backrub/google.html` .

Curtin, Matt. 1998. Introduction to network security. `http://www.interhack.net/pubs/network-security/network-security.html` . Last revised 16 July 1998.

Honeynet Project. 2003a. Know your enemy: Honeynets—What a honeynet is, its value, how it works, and risk/issues involved. `khttp://project.honeynet.org/papers/honeynet/index.html` . Last modified 12 November 2003.

Honeynet Project. 2003b. Know your enemy: Defining virtual honeynets: Different types of virtual honeynets. `http://www.honeynet.org/papers/virtual/` . Last modified 27 January 2003.

Mitra, Sanjit Kumar. 2001. *Digital Signal Processing: A Computer-Based Approach*. 2nd ed. New York: McGraw-Hill.

Oppenheim, Alan V., and Alan S. Willsky. 1996. *Signals and Systems*. 2nd ed. Englewood Cliffs, NJ: Prentice-Hall.

Saaty, T.L. 1980. *The Analytic Hierarchy Process.* New York: McGraw-Hill.

Authors' Commentary: The Outstanding Information Technology Security Papers

Ronald C. Dodge, Jr.
Information Technology and Operations Center
United States Military Academy
West Point, NY 10996
`ronald.dodge@usma.edu`

Daniel J. Ragsdale
Dept. of Electrical Engineering and Computer Science
United States Military Academy
West Point, NY 10996
`daniel.ragsdale@usma.edu`

Introduction

Information Assurance (IA) education and training in today's world is increasingly important. Several incidents in the past few years, such as data theft, malicious worms and viruses, denial of service attacks, and defacement of corporate and government web pages highlight the need to educate users and administrators of information systems. IA is more than just the simple application of technical measures to secure an information system; it is the combination of defensive technologies; well-conceived policies and procedures, and properly trained users [Maconachy et al. 2001].

Computer networks are ubiquitous, but aside from a relatively small number of network engineering professionals, few understand the fundamentals of information assurance (IA). Many institutions of higher learning that offer degrees in computer science offer courses that address the topic of computer networks. Often these courses focus on network protocols and theory, with little emphasis on the policy and hands-on application that individuals in organizations face every day. The integration of security practices into the business model of an organization is laden with tradeoffs. The implementation of security measures often has both direct costs and productivity costs as affected

The UMAP Journal 25 (2) (2004) 171–174.

information systems become more difficult to use or are degraded with the introduction of enhanced security measures.

Formulation and Intent of the Contest Question

The main goal of this year's interdisciplinary modeling problem was for competitors to reduce the potential costs associated with malicious behaviors in an simulated organization. This reduction results from the implementation of the set of preventative measures that were identified by the contest participants. The problem of how an organization maximizes its IT security posture while considering the overall economics impact on its mission requires an analysis of the known, expected, and potential costs. Organizations must analyze this problem in three primary areas: First, the organization must define the areas of risk in the IT infrastructure. Typically these are data confidentiality, data integrity, and service availability. Next the sources of risk need be identified, for example a malicious outside hacker, a "clumsy" insider, or hardware/software failure. Finally, the costs must be enumerated. This includes both the costs associated with security measure implementation (such as direct costs, training and productivity) and the potential costs if any or all of the areas of risk are compromised.

This is a complex problem that requires a thorough analysis of many variables that have positive impacts in one area and negative impacts in another [Bishop 2002, 17–18; Garfinkel and Spafford 1996, 27–40]. Additionally, an organization might have missions that vary within its structure that require different security measures. The problem of how to design and implement the security architecture of an organization is further complicated by the dynamic nature of the problem. The evaluation conducted in the early stages of an assessment will be modified over time by changes in the organization mission and advances in technology. In building the framework for this year's modeling question, we attempted to generalize many factors to enable the students to build tractable models.

The problem posed to the teams described a generic organization (a university) that consisted of several competing components that in some ways required completely different and competing security measures. The organization required both an open environment for information distribution and student access and a more secure system for grades, tuition, and book store management. Additionally, a hybrid solution was required for a third group made up of staff and faculty. The specific identification of these needs and several others was left to the teams as part of the analysis process.

The teams were then required to examine the efficacy of various technical solutions and security policies in light of the various organization requirements. The solutions were then balanced against the overall potential for loss due to security failings and the direct costs of the security architecture. This underlines the fundamental premises that: the total cost of a security solution is the sum of the direct financial costs and the indirect costs due to usefulness and productivity and an organization should not spend more on a solution that it is at risk for losing. For example one would not be wise to install a $10,000 alarm system on an item valued at $1,000.

Lastly, the ICM teams were required to analyze their proposed solutions model's ability to withstand technology changes as time passes.

References

Maconachy, V., C. Schou, D. Welch, and D.J. Ragsdale. 2001. A model for information assurance: An integrated approach. In *Proceedings of the 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop* (West Point, NY, June 5–6, 2001), 306–310.

Bishop, Matt. 2002. *Computer Security: Art and Science*. Boston, MA: Addison-Wesley.

Garfinkel, Simson, and Gene Spafford. 1996. *Practical Unix and Internet Security*. 2nd ed. Sebastopol, CA: O'Reilly and Associates.

About the Authors

The authors of this year's contest question have been working in the area of Information Assurance for a combined 18 years. The foci of their research include:

- Information assurance simulation development. The problem posed in this year's modeling contest closely mirrors the scenario used to frame simulation being developed under an NSF grant. Various components of the simulation have been under development since 2001 and have been the topic of five conference papers.
- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) analysis and implementation, including the development and deployment of innovative IDS and IPS solutions, such as honeynets, layer-2 bridges, and attribution technologies.
- Virtual machine technology. The authors have pioneered the use of virtual machines (VMs) to overcome resource constraints encountered by computer science programs enabling each student to manage and administer a robust collection of servers and workstations.

- Information assurance curriculum development. The authors have integrated the use of VMs into a hands-on curriculum consisting of a variety of introductory and technical computer science courses as well as policy-based analysis courses. The development and use of VMs is the topic of six conference and journal publications.
- Competitive cyber defense exercises. The authors developed and implemented the U.S. Military Academy Cyber Defense Exercise. This model is being used as the benchmark for an NSF-funded effort to introduce competitive cyber exercises to civilian universities.

Major Ronald C. Dodge, Jr., has served for more than 16 years as an Aviation officer and is a member of the Army Acquisition Corps in the United States Army. His military assignments range from duties in an attack helicopter battalion during Operation Just Cause in the Republic of Panama to the United States Military Academy. Currently, he is an Assistant Professor and Director of the Information Technology and Operations Center (ITOC) at the United States Military Academy. Ron received his Ph.D. from George Mason University, Fairfax, Virginia in Computer Science. His current research focuses are on information warfare, network deception, security protocols, internet technologies, and performance planning and capacity management. He is a frequent speaker at national and international IA conferences and he has published many papers and articles on IA topics.

Colonel Daniel J. Ragsdale has served for 23 years as an officer in the U.S. Army. He has served in a variety of important operational, and research and development assignments, including participation in Operation Urgent Fury in Grenada and Operation Enduring Freedom in Afghanistan. Currently, he is an Associate Professor and Director of the Information Technology Program, Professor in the Department of Electrical Engineering and Computer Science at the U.S. Military Academy. His current research focuses on information security, Information Assurance (IA), and Information Warfare. He is a frequent speaker and panelist at national and international IA conferences and he has published dozens of papers and articles on IA topics.

Judge's Commentary: The Outstanding Information Technology Security Papers

Frank Wattenberg
Dept. of Mathematical Sciences
United States Military Academy
West Point, NY 10996
Frank.Wattenberg@usma.edu

Introduction

The final judging for the 2004 Interdisciplinary Contest in Modeling took place at the United States Military Academy on Saturday, March 6, 2004. The judges spent an extensive and enjoyable day reading a very good and varied set of papers.

Bottom Line Up Front: There is Room at the Top

Although a number of submissions were very good and readers will recognize some well-known institutions among the Outstanding and Meritorious papers, there is room at the top. If this were a sporting event rated on a 10-point scale, it is quite likely that no one paper would have scored above 9.0. This IT Security Problem involved many complex issues, messy data, and several challenging tasks. Three points are crucial in addressing the requirements of this problem:

This is first and foremost a modeling competition. Modeling is often about ill-posed problems, in complex settings with uncertain data. Conclusions necessarily involve simplifications and uncertainties and confronting them is absolutely imperative. The papers were judged primarily on modeling.

The UMAP Journal 25 (2) (2004) 175–179.

The constraints of the contest are exactly the constraints in real life. In the real world, modelers always work with limited time and resources. Thus, real-world modeling requires making simplifications, justifying those simplifications, examining the impact of those simplifications and, above all, being intellectually honest about the shortcomings as well as the successes of the resulting models. Some submissions were marred by puffery.

Organization, clarity, and brevity are essential. The judges were surprised by the number of submissions that lacked a table of contents. Although a table of contents was not required, its omission usually reflected a general lack of organization. The summary too is particularly important for any report. Although many summaries were well-written, even the summaries in the Outstanding papers merited at best a grade of B; none talked about the potential shortcomings of their models due to modeling assumptions or uncertainties in the data.

The Problem

This year's problem dealt with information technology security for a new university campus. An undefended IT system is exposed to potential losses but, as usual, the costs of defense are considerable.

There are many possible approaches to this problem. The problem description focused on two categories of defenses—policies and technology.

- Policies include, for example, whether the network is wireless, as well as password policies—how complicated must passwords be and how often must they be changed.
- Technologies include things like firewalls and virus scanning.

The description also focused on risk in three areas—confidentiality, integrity, and availability. A breach of confidentiality can result in litigation or the costs associated with the release of proprietary or classified information. The integrity and availability of data and information are, of course, essential to their value.

In addition to a description of the structure of the situation, the problem included a 12-page enclosure with data about several alternatives in various categories—for example, it included data on eight different host-based firewalls. These data had two glaring features, and the judges looked specifically at how the submissions addressed the issues raised by these features:

- Alternative defensive measures were discussed individually with no information about how they might work in combination.

  The better submissions all addressed this issue at least briefly. In general, however, none of the submissions did an outstanding job. The fact is that there is a range of ways in which two alternatives might interact. For example, at one extreme, two different virus scanners might be completely redundant if they both picked up the same viruses; or, at the other extreme, they might protect from completely different viruses. The results are potentially very sensitive to whatever assumptions are made in this area.

This problem is compounded by the fact that assuming redundancy among measures in the same category reduces the computational complexity of the problem. Many submissions (including highly-rated ones) justified this assumption to make the problem computationally feasible. This is a reasonable assumption only if it is accompanied by a discussion of the sensitivity of the conclusions to this assumption.

- The data were based on multiple reviews of the measures and there was considerable variation in the conclusions of the various reviews.

  Here again, while most of the papers addressed this issue in some fashion, many of papers made simplifications without discussing the sensitivity of their conclusion to those simplifications.

Analysis

The different teams applied a variety of optimization techniques to their models. Some teams worked with models that were computationally infeasible and applied techniques—for example, simulated annealing—that led with relatively high probability to near optimal solutions; others made assumptions that led to computationally feasible optimization problems. Some teams used standard software and others wrote their own programs using C++ or other programming languages. Although some of the teams used sophisticated mathematics and algorithms (for example, simulated annealing) and others used sophisticated software effectively, neither was necessary for this problem. Many teams did first-rate work using straightforward implementations of their models with general-purpose tools.

The analytic part of this problem can be broken into two parts:

- evaluating the costs and the effectiveness of a mix of defensive measures, and

- searching the space of possible mixes of defensive measures to find an optimal or near optimal mix.

The first part rightfully drew the most attention in most of the submissions—this is the modeling part. This required considerable attention to details and to the extensive data provided. Most importantly, however, it required thoughtful analysis of the two difficulties mentioned earlier—the impact of combinations of defensive measures and how to handle the uncertainties in the data. This is also the first focus of the absolutely necessary sensitivity analysis. In its starkest form, an assumption that two measures are redundant leads to a recommendation that at most one measure should be employed, while an assumption that two measures cover disjoint sets of attacks may lead to a recommendation that both defensive measures should be employed.

The computational difficulty of the second part depended in part on the assumptions about how individual preventive measures interacted when used together. Other modeling assumptions also impacted this part of the problem. For example, some teams assumed that the same mix of defensive measures was used across the university, whereas others broke the problem up into different subnetworks. The new university's computing needs are diverse—ranging from student computers in dormitory rooms, to the commercial needs of a bookstore whose business skyrockets at the beginning of each semester, to the registrar's office and student health services that routinely deal with confidential data. In addition, the sophistication and professionalism of users is also very diverse—the registrar's office, bookstore, and student health services, for example, are more likely to accept stringent security measures than individual students, who might want to be able to install software of questionable origin.

We saw a wide variety of approaches to searching for an optimal or near-optimal solution and most had considerable merit. Here again, we focused on the implications of the underlying modeling assumptions and on an analysis of the sensitivity of the conclusion to the search procedure used in addition to the modeling assumptions.

Conclusions and Advice to Future Teams

This section is essentially an amplification of the same points made by Richard Cassady last year [2003, 188].

Assumptions Making simplifying assumptions is a critical part of modeling. In fact, good models are always the result of an iterative procedure beginning with fairly drastic simplifying assumptions to obtain some initial traction and then building progressively more sophisticated models based on sensitivity analysis and reality checks. Articulate your assumptions and their consequences. Your summary must identify clearly the assumptions made and their impact on your conclusions.

Analysis Analysis is not the last step. It is an integral part of the iterative modeling procedure. Do regular reality checks and above all use sensitivity analysis to guide your model development and to determine both the strengths and weaknesses of your conclusions.

Communication You must express and communicate your work well. Clarity of expression is a consequence of clarity of thought. If your summary and your paper are not clear then the modeling is almost certainly weak.

References As always, use proper citation and be careful about the provenance and worth of the work you use.

Congratulations are extended to all the participants on their accomplishments. Reading and judging the results of their weekend of interdisciplinary problem solving and modeling were enjoyable challenges for the judges.

Reference

Cassady, C. Richard. 2003. Judge's Commentary: The Outstanding Airport Screening Papers. *The UMAP Journal* 24 (2) 185–188.

About the Author

Frank Wattenberg is a professor in the Dept. of Mathematical Sciences at the United States Military Academy (USMA), West Point. He is particularly interested in modeling and simulation and in the use of technology for simulation and for education across the undergraduate curriculum. He is currently leading a team at the USMA that is developing on Online Book *Modeling in a Real and Complex World* to be published as part of the MAA Online Book Project. He is also working with colleagues at USMA and elsewhere to develop rich immersive environments for modeling and simulation. This project will produce environments with both virtual and hands-on components that students will revisit from middle school through college and from many different subject areas and levels. The architecture will support collaborative modeling and simulation based in part on the ideas of multiplayer games.

Editor's Note Regarding Submissions

From August 2004 through August 2005, I will be editing *The UMAP Journal* from the University of Augsburg in Germany. Postal mail can be sent directly to the address in Germany below; mail to the Beloit College address on the masthead will be sent on.

However, to avoid expense and delays, **please endeavor to send all correspondence by electronic mail—and manuscripts by email attachment—to the Beloit College email address**

`campbell@beloit.edu`

I will be retrieving email directly from this address, and email sent to it will be archived permanently against inadvertent loss.

MID-AUGUST 2004 THROUGH MID-AUGUST 2005

Paul J. Campbell
c/o Lst. Prof. Pukelsheim
Institut für Mathematik der Universität Augsburg
Universitätsstr. 14
D–86135 Augsburg
Germany
voice: 011-49-821-598-2206 fax: 011-49-821-598-2280
email: `campbell@math.uni-augsburg.de`
www: `http://cs.beloit.edu/campbell/`

About the Editor

Paul Campbell graduated summa cum laude from the University of Dayton and received an M.S. in algebra and a Ph.D. in mathematical logic from Cornell University. He has been at Beloit College since 1977, where he was Director of Academic Computing from 1987 to 1990. He is Reviews Editor for *Mathematics Magazine* and has been editor of *The UMAP Journal* since 1984.

He first visited Augsburg in 1967 on an exchange of young adults between the sister cities of Augsburg and Dayton, Ohio, where he had gone to high school and college. On his last sabbatical and in alternate summers since, he and his family have lived in Augsburg. He remains immensely grateful to the memory of Dr. Alfred Beigel (deceased), with whom he studied German for three years at the University of Dayton.

Reviews

Albert, Jim. 2003. *Teaching Statistics Using Baseball*. Washington DC: Mathematical Association of America; xi + 288, $45. ISBN 0–88385–727–8.

Albert, Jim, and Jay Bennett. 2003. *Curve Ball: Baseball, Statistics, and the Role of Chance in the Game*. Rev. ed. New York: Copernicus, 2003; xxii + 410, $19.95. ISBN 0–387–00193–X.

Lewis, Michael. 2003. *Moneyball: The Art of Winning an Unfair Game*. New York: W.W. Norton; xv + 288, $24.95. ISBN 0–393–32481–8.

The development of statistical inference in the twentieth century was spurred by agricultural research more than any other application; even today, many of the best statistics departments are at the schools with the best agricultural departments. The second application that comes to mind after agriculture—the application that generates most of the press and public controversy—is pharmaceuticals. But another application has generated a lot of intense scrutiny and passion by parts of the general public, and that is *baseball*.

Baseball has several characteristics that make it have greater statistical import than other sports.

- Major-league baseball has maintained a statistical record of every game and every inning since the late nineteenth century.
- Baseball has changed slowly enough that today's game resembles the game of 100 years ago much more closely than is the case for football, where significant differences can show up in a mere 10-year span.
- Perhaps most importantly, baseball lends itself to statistical questions, and it is this characteristic that makes it appropriate to education. For example:
  - How important is defense relative to hitting?
  - How much of the game is pitching?
  - Who are the greatest hitters that ever lived?
  - Who is the best player ever to play third base?
  - When is it smart to lay down a bunt?
  - And perhaps most important of all, who should the home team draft in 2005?

The UMAP Journal 25 (2) (2004) 181–184.

In the last 25 years, one figure has dominated the statistical analysis of baseball: Bill James. While employed as a security guard, he wrote his first baseball almanac in 1977, which he published himself and sold to 75 people; his second historical analysis of baseball [James 2003] was reviewed in both the *New York Times Book Review* [McGrath 2002] and in the *New York Review of Books*. There is more than a little irony in his story, and I'll return to that in a while.

Teaching Statistics Using Baseball is a textbook, with plenty of exercises and case studies. It is an effective introduction to exploratory data analysis at an elementary level, easily readable by the motivated high-school student. It would work very well in a course on data analysis specifically, perhaps as a secondary text. There is historical detail, and a great many questions are posed and then analyzed. I can't say how well it would work in the classroom, but I can imagine a student gripped by it. Prof. Albert is not just a statistician but a baseball enthusiast (saying "nut" could have negative connotations).

Curve Ball: Baseball, Statistics, and the Role of Chance in the Game by Jim Albert (again) and Jay Bennett won the 2001 SABR award (Society for American Baseball research) and has done quite well. This book is not a text and thus is much more interesting to readers who do not need a course in statistics. At the same time, it does serve as a course in data analysis and is not for the reader who is math-phobic. Both books cover some modeling and simulation. The second book, as implied by the title, spends more time and depth on the study of randomness. In particular, there has been much study in the last few years of streakiness in both baseball and basketball. The central question is: Do streaks really exist, or are they just a manifestation of ordinary random variation? *Curve Ball* is essential reading for any serious baseball fan who is also a nerd.

If the slightly pejorative connotations of "nerd" are seriously offensive to you, then you should stay in the ivory tower if you are a professor and should change your major to literature if you are a student (lots of employers seek the kind of critical thinkers churned out by literature departments).

Moneyball is very much about nerds and nerdiness. For a book that merely describes a handful of formulas, there is quite a bit here to interest statisticians. The author, Michael Lewis, writes books on management and business. While this book falls into that category, most bookstores put it in the baseball section. *Moneyball* has been something of a best-seller and has gained a great deal of notoriety both outside of baseball and inside, where it has been exceedingly controversial. Quite a few baseball fans and commentators have attacked the book, although most have not read it or did not understand it. It has made famous the general manager of the Oakland Athletics, a former major-league ball player named Billy Beane (not to be confused with another former player, Billy Bean, who recently wrote a book where he came out as gay).

Moneyball is the book to read. If you are interested as well in a superb monograph on baseball analysis and chance, then also read *Curve Ball*. If you want a text in data analysis using baseball, you might very much like *Teaching Statistics Using Baseball*. But *Moneyball* is one of the most exciting and fascinating books I have read in some time.

There are several caveats before I get started extolling *Moneyball*.

- Be warned that the language is rated R. A hard R.

  The book is quite elliptical. It will refer offhandedly to random variation, a term that is all too familiar to mathematicians and statisticians but generally is not appreciated by the lay person. It refers to theories of perfect market information, theories that are pivotal to investment theory but are lost again on lay people.

- Sprinkled throughout the book are simple statistical points that are left unsaid entirely.

I would love to discuss this book with seniors in mathematics. On the surface, it is book about major-league baseball; to me, it is about the real world. Academia is full of mathematics professors who have no knowledge of industry or about nonacademic jobs. Others, some top academics in particular, think of industry in terms of national labs and research environments that are themselves rather academic and often have fairly good job security. However, most graduates who go into industry, especially the non-Ph.D.s, do not go into national labs. They go into something that I long ago learned not to talk about with most academics. But whereas others will see *Moneyball* as merely describing baseball, I say that it is much more general than that, and clearly so does author Michael Lewis.

Whereas the first two books are about data analysis and are very fine examples of it, I am amazed about how well *Moneyball* conveys the spirit of data analysis and of analytical thinking, all amidst colorful anecdotes and profiles (not to mention the colorful language). It is this book that gives a necessary chapter to Bill James. The irony here is that a man without statistical training, but with a passion for analysis, found formulas that serious statisticians (at least one of whom was an academic superstar) who happened to be baseball nuts missed. In fact, one question that I've seen no one address is this: Why didn't statisticians running regression models find these formulas? Late in *Moneyball*, we have another Bill James-like character, Voros McCracken, who while unemployed and living with his parents developed a formula for ranking pitchers that was startling in its simplicity and its implications. (In particular, the existence of such a formula startled Bill James.) I found no mention of Mr. McCracken or his formula in the other two books.

A nice summary of James's attitude is given on p. 95:

> Intelligence about baseball had become equated in the public mind with the ability to recite arcane baseball stats. What James's wider audience had failed to understand was that the statistics were beside the point. The point was understanding; the point was to make life on earth just a bit more intelligible; and that point, somehow, had been lost. "I wonder," James wrote, "if we haven't become so numbed by all these numbers

> that we are no longer capable of truly assimilating any knowledge which might result from them."

This point is precisely what R.W. Hamming meant: "The purpose of computing is insight, not numbers" [1986, frontispiece].

The following are some of the points of *Moneyball*:

- Much of the common knowledge within baseball is wrong.
- In particular, baseball scouts have been relying on methods of evaluation that are nearly useless.
- On-base percentage (OBP) is a much better measure of a batter's offensive value than batting average. Although some people figured this out before Bill James, baseball clubs have relied almost exclusively on batting averages.
- Baseball has relied on batting averages because of a historical accident. A nineteenth-century cricket writer invented the batting average statistics partly because he made an incorrect assumption about the art of hitting. A very basic statistical study, quite within the range of any analytical thinker, could have shown this.
- Major-league baseball clubs in their entirety have been extremely inefficient in drafting, promoting, and paying their players.
- Baseball clubs have had nerds on their staffs who told them how to do things better, but the executives almost never listened to them.
- At least one major-league club had a front office that was simply stupid; that is, it was staffed by people with uniformly low cognitive ability.
- The single biggest mistake made in baseball was the belief that one's judgement is more reliable than the statistical record.

Lastly, I found *Moneyball* laugh-out-loud funny.

References

Hamming, R.W. 1986. *Numerical Methods for Scientists and Engineers.* New York: Dover.

James, Bill. 2002. *The New Bill James Historical Baseball Abstract.* 2003. Rev. ed. New York: Free Press.

McGrath, Ben. 2002. Where's Marv Throneberry? Review of James [2002]. *New York Times* (31 March 2002) Section 7, 12.

James M. Cargal, Mathematics Dept., Troy University–Montgomery Campus, Montgomery, AL 36121–0667; `jmcargal@sprintmail.com` .