# The State of Network Security Management: Issues and Directions

**Andrew T. Zhou**
**James Blustein**
**Nur Zincir-Heywood**

Technical Report CS-2003-06

May 20, 2003

Faculty of Computer Science
6050 University Ave., Halifax, Nova Scotia, B3H 1W5, Canada

# The State of Network Security Management: Issues and Directions

Andrew T. Zhou, James Blustein, Nur Zincir-Heywood
Faculty of Computer Science, Dalhousie University

{azhou, jamie, zincir}@cs.dal.ca

## Abstract

We describe the results of a survey of the state of practice in security management with a particular focus on intrusion detection systems (IDSs). We anonymously surveyed 17 system administrators from different countries and economic sectors (industry, government, etc.). The data is analysed in terms of administration team size and number of networks (single or multiple).

The results strongly indicate that the state of security management is poor and that sysadmins are satisfied with neither the performance nor the usability of their security administration tools. Many administrators do not perform regular checks of the networks they manage, and most of those checks require a great deal of time to perform. High false alarm rates are a serious problem with IDSs. However there is reason to believe that much of the resulting difficulty could be eliminated through the deployment of more suitable user interfaces. This analysis is the first step in the development of an improved interface for network intruder detection.

The survey and other work in the project are continuing.

# Contents

# Chapter 1

# Introduction

According to CERT [7], network security management is a hierarchical structure, which involves security policies, and various systems to implement those policies. Deployment and use of intruder detection systems (IDSs) is one of their recommended practices.

In the present work, we focus on the intruder detection aspect of security management. There are two ways to make significant improvements to the state of the art and the state of practice in IDSs: (1) the underlying technique in detecting attacks, and (2) the human interface to enable administrators to quickly and accurately detect and respond to attacks [5]. Our work is concentrated on this second method. To improve security through better user interfaces we must first understand the needs of network administrators working in security management. Hence, we conducted a survey to determine the needs of network professionals — how they manage network security and how it could be improved. To the best of our knowledge, this work is the only completed survey in the area. CERT's Incident Detection, Analysis, and Response project [8] is also conducting a survey but has not made the results public. Moreover, their objective is to factor the results into a knowledge base of their prototype computer system that will support novice systems administrators. In contrast, the aims of our survey are: to study the nature of human-computer interaction in security management, so as to enable systems administrators to efficiently and effectively manage network security, and make quick decisions when identifying potential intrusions.

In our project (of which the survey is a part), the improvement is sought through better user interfaces for IDSs. Thus the survey was developed to gather data that would be relevant to the three main aspects of usability

according to ISO: speed (efficiency), performance (efficacy), and user acceptance (affectiveness) [2]. For instance in network applications: efficiency could be defined by how fast system administrators can discover the security status of their systems; effectiveness can be determined in terms of reported accuracy; and acceptance can be predicted by the satisfaction of system administrators with a product.

The huge challenge that current security management procedures face is to keep pace with the evolution of modern networks. An ideal IDS would be able to detect a wide range of attacks with fewer false alarms and also effectively report attacks on large, fast, and rapidly changing networks. Along with approaches to seek better solutions to data collection issues and detection techniques, efforts to improve system response (which includes the interface characteristics and interaction mechanisms) will enable future IDSs to achieve those goals.

The rest of this article is organized as follows: Chapter 2 describes the survey, and Chapter 3 details the results. Finally, conclusions are drawn and future directions are given in Chapter 4.

# Chapter 2

# Method

This work presents a survey on state of the practice of security management in companies and institutions worldwide. Anonymous questionnaires are used to gather data from network professionals. Respondents were drawn from a pool of subscribers to a mailing list for university systems administrators and to some security specialists in international industry. Although our figures are drawn only from those professionals who replied to our survey, we have no reason to believe our sample to be anything but representative of network administrators in all but the most security-conscious institutions worldwide.

The questions were grouped into three parts: 13 questions were about the administrators themselves, 11 were about the networks they administer and groups they work in, while 16 were about the security polices at their sites. By December 2002, seventeen responses had been received. Our discussion of results also follows this order.

# Chapter 3

# Results

In this work, we aim to obtain accurate baseline estimates of usage of security management tools for intrusion detection by both large and small-to-medium size enterprises, irrespective of economic sector. We believe that the results of this survey identify the most pressing needs of administrators' interaction with the tools they need for network security administration.

## 3.1 About The Administrators

Our respondents ranged in age from 20 to 45. They had between one and eight years of experience at their current job. Their self-reported level of experience spanned the whole range from novice to advanced. More than half of them rated themselves as having advanced knowledge of security management. Figure 3.1 shows the relationship between age and experience among our respondents.

Although all of our respondents were at least partly responsible for security at their sites, only 18% (3 of 17) had the word '*security*' in their job titles; six of them were '*manager*'s or '*administrator*'s, and six were 'engineer's.

Figure 3.2 shows the composition of our respondent pool by economic sector. Nearly half of them work in the business sector, the bulk of the others work in education and research. Note that some respondents selected multiple sectors and one refused to answer.

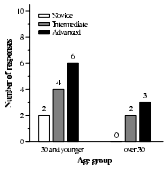



Figure 3.1: Number of Respondents by Age Group and Experience Level

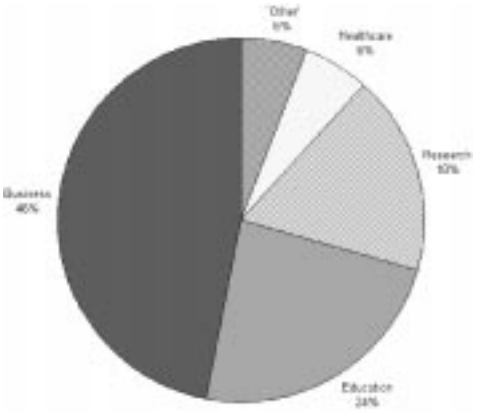



Figure 3.2: Where Our Respondents Are Employed

## 3.2 About Their Networks and Work Groups

We asked how often managers check the security of their sites. The overall results are summarized in Figure 3.3: Most (88%) do not monitor their sites continuously; about 30% check their system only after an attack has been detected(!) through other means.

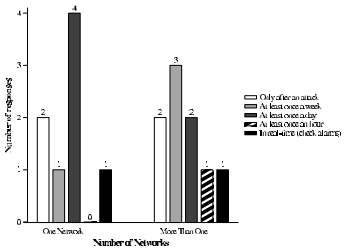
Figure 3.3(a) shows that the frequency of checking is similar across large and small networks. However Figure 3.3(b) shows that only a small proportion of system administrators (2 of 17) perform security checking in real-time. It seems that larger groups tend to check more often. Clearly frequent scheduled checks are best for maintaining network security, regardless of team or network size.

Figure 3.4 shows the team size versus the length of time administrators require to do security tasks. It seems that the time it takes network managers to deal with security checks is not affected by the size of their teams. Most respondents (10 of the 14 who answered this question) did not take more than an hour per check. Moreover, the responses presented in Figure 3.5 suggest that the size of the network does not affect the amount of time system managers use in every case. Only two administrators reported needing no more than several minutes to check the security of their networks, and those two were working in groups with other administrators.

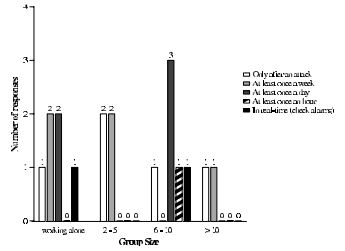
## 3.3 Tools for Security Management

Based on the guidelines given by CERT on system and network practices [1, 7], tools for system administrators to manage network security can be grouped into four categories: (1) system tools, (2) off-the-shelf tools, (3) third party outsourced tools, and (4) others. The common belief that managers rely on operating system tools most of the time is borne out by our survey results. Those of our respondents who use one type of tool more than half of the time are twice as likely to rely on system tools as any other type.

No single real-time monitoring tool catches all known attacks [4, 5]. For instance, in a recent study [4] performed using the DARPA 1999 data set [6], Snort detected only about 44% of attacks in the test dataset. Moreover, approximately 99% of Snort warnings were false alarms, and Snort did not detect attacks that other IDSs did. Of our respondents who volunteered additional information about the tools they use (or chose not to use), 75%




(a) Frequency of Checking Related By Network Topology






(b) Frequency of Checking Related By Size of Team

Figure 3.3: Frequency of Security Checks

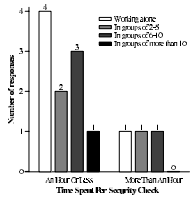



Figure 3.4: Impact of Size of Team on Duration of Security Check

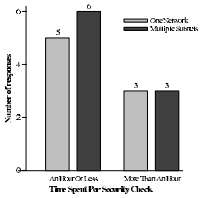



Figure 3.5: Impact of Number of Subnets on Duration of Security Check

of those with negative comments complained that false alarm rates were too high.

Figure 3.6 shows overall patterns of use of the various tools used for managing network security by our respondents. According to these results, approximately 45% prefer to use system tools (including operating system patches).

Figure 3.7 shows the reported frequency of use by the type of tool used. None of our respondents outsourced more than 25% of their security management. Also, it seems that network administrators do not use the same type of tools at all times. This may be because they are not satisfied with a single tool, or it may be that they need the different capabilities that are only available with a variety of tools.

It is apparent from the preceding data that the state of practice in network security management is far from ideal. In particular, many administrators check their networks only after an attack is detected or, at most, a few times a week. Larger groups, and those with larger networks, tend to check more frequently, but otherwise, surprisingly, we see no indication that group or network size impacts on security practice. We speculate that managing network security is not a easy job (even for trained and experience system administrators), and there is not an efficient tool available for them to do their work. That is why it takes a long time for most of our respondents to carry out these tasks.

Having identified these problems, we want to investigate the role of tools in helping (or hindering) system administrators. Since it is well known that,

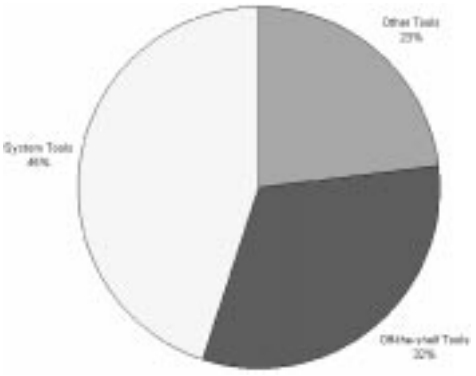


Figure 3.6: Types of Tools Used for Security Management

user interfaces have an effect on the security of computer systems [3, 10].

### 3.3.1 Current Tools

We suspect that administrators who use any type of tool less than half of the time are not happy with the performance of that tool. We investigated managers' satisfaction about their tools (see Figure 3.9).

Security management is critical and requires managers to have thorough understanding of the network configuration and potential problems. In most cases, it is a decision making based on comprehensive information aggregation.

We investigated what the managers use to diagnose potential attacks. Figure 3.10 shows the resources that administrators use to search for help. All but one of our respondents reported using some form of help document when diagnosing problems or determining the validity of alarms. Some respondents reported using more than one form of document, and one respondent did not answer the question. All of those who answered this question use the Internet to find help documents. As well, traditional documents (such as books, built-

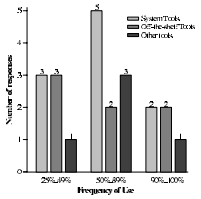



Figure 3.7: Frequency of Use by Tool Type

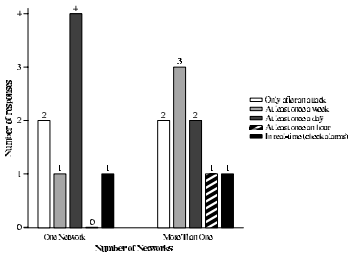


Figure 3.8: Frequency of Checking the Network/System for Any Intrusion

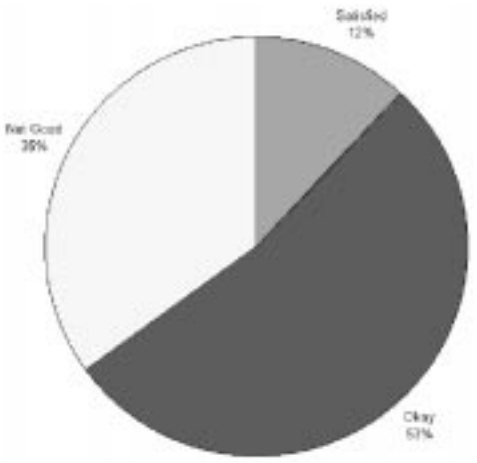


Figure 3.9: Satisfaction with Current Tools

in help files, and man pages) are also commonly used.

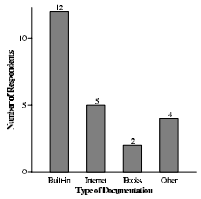



Figure 3.10: Resources Used to Help Diagnose Security Problems

### 3.3.2 Future Tools

Designing usable interfaces for complex, data-driven tools (such as IDSs) is inherently difficult, in part because the designers are not familiar with the range of users and situations the interface will be used in. Although now dated, the work by Tullis [9], is still the clearest demonstration of how non-domain experts can create highly effective interfaces. Figure 3.9 shows how the administrators we surveyed felt about current user interfaces for their security management. Few (2 of 17) respondents described themselves as 'satisfied' with the interfaces to their current software. Almost three times as many described their current software's interfaces as 'not good'. The others selected the intermediate option of 'okay, but willing to try a better one'.

As indicated in Figure 3.11, 64% of our respondents want their user interface to contain both textual and graphical components, while 30% preferred only one or the other.

Similar to the information representation in interfaces, optimized data organization (which is a convenient way for our respondents navigating collected information) is also a key factor for evaluating security tools. Figure 3.12 shows how people expect the alert information to be organized. It seems that most administrators (about 90% of our respondents) would prefer to have alerts organized in flat or hierarchical categories.

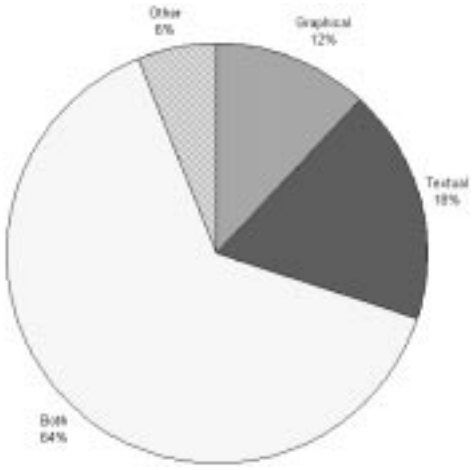



Figure 3.11: Preferred User Interface Components

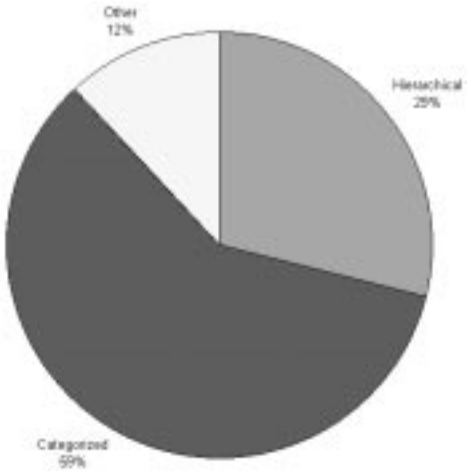



Figure 3.12: Preferences for Organization of Alert Information

# Chapter 4

# Discussion and Directions for Future Work

In this work, we have presented the results of a survey among network administrators to understand the usage of security management tools, with the aim of improving network security through better user interfaces.

The results of our survey strongly indicate that the state of network security management is poor. This situation is partly because of the lack of good tools for administrators. Only two of our administrators said it took several minutes to respond to alarms or to check the state of their network. All of the other responses indicate a serious deficiency that must be rectified for network security to improve. Current tools require so much time to use that many network administrators do not have the necessary time to use them effectively.

Moreover, it is clear that users are not happy with their tools (15 of 17 were not satisfied). Hence, to improve the state of practice, better tools are needed. Such tools would seamlessly extend users' capabilities and not be another complex system for them to learn to work around. Thus, our immediate goal is to identify the improvements that are required to develop security tools which have better interaction characteristics as a step towards improving security.

To apply the ISO's definition of usability [2] one needs to specify user characteristics and job tasks, and to consider operating environments. Through our survey, we have a sufficient understanding of working environments and user (system administrator) characteristics. CERT's guidelines to system and network security practices provide information about job tasks. Not all

administrators follow these completely, but all administrators follow at least some parts of it. We speculate that if there was a simple and accurate way to apply CERT's principles then most system administrators would be able to follow it.

Therefore, our next goals are: first, to develop measures of the usability of tools based on the results of the survey; then to design a new system, which is based on the ideas and measures learned from the survey; and finally to use those measures on existing systems as a benchmark to compare against the new system which is in development.

**Acknowledgment** This work was made possible through NSERC operating grants to the second and third authors. The assistance of the Telecom Applications Research Alliance, Inc. (TARA) and Thor Solutions, Inc. is gratefully acknowledged.

# Bibliography


[1] Julia Allen. *The CERT® Guide To System and Network Security Practices*. Addison-Wesley, 2001. ISBN 020173723X.

[2] Alan Dix, Janet Finlay, Gregory Abowd, and Russell Beale. *Human-Computer Interaction*. Prentice Hall Europe, second edition, 1998. ISBN 0-13-239864-8.

[3] U. Holmström. User-centred design of secure software. In *Proceeding of the International Symposium on Human Factors in Telecommunications*, Copenhagen, Denmark, 4 – 5 May 1999.

[4] G. Kayacik and A. N. Zincir-Heywood. Using intruder detection systems with a firewall: Evaluation on DARPA 99 data set. `http://www.cs.dal.ca/~kayacik/download/CSTR030100.pdf`, 2002. Accessed on 24 January 2003.

[5] R. A. Kemmerer and G. Vigna. Intruder detection: A brief history and overview. *IEEE Computer*, 35(4):27 – 30, April 2002.

[6] Massachusetts Institute of Technology Lincoln Laboratory. 1999 DARPA intrusion detection evaluation data. URL `http://www.ll.mit.edu/IST/ideval/data/1999/1999_data_index.html`. [dataset webpage], 1999.

[7] CERT®. CERT® website. URL `http://www.cert.org/`. Accessed on 15 December 2002, 2002.

[8] CERT®. The IDAR project [webpage]. URL `http://www.cert.org/idar/`. Accessed on 15 December 2002, 2002.

[9] Thomas S. Tullis. An evaluation of alphanumeric, graphics, and color information displays. *Human Factors*, 23(5):541 – 550, 1981.

[10] M. E. Zurko and R. T. Simon. User-centered security. In *Proceedings of the UCLA Conference on New Security Paradigms Workshops*, pages 27 – 33, Lake Arrowhead, California, USA, 1996. ACM Press.

# Appendix A

# Questionnaire

I - About You and Your Work in General

I-1)
Your job title/position: _____

Years of experience in network/system security management: _____

Years in current position: _____

Your age: __ <20 __ 20-25 __ 26-30 __ 31-35 __ 36-40
__ 41-45 __ 46-50 __ 51-55 __ >55

Sector in which you are employed:
__ Education __ Research __ Business
__ Healthcare __ Government __ Other (please specify)

I-2)
Please rate your level of knowledge of system/network management
__ Novice __ Intermediate __ Advanced

I-3)
What is the approximate server-to-workstation ratio where you work:
__ 1:1 __ 1:2 __ 1:5 __ 1:8 __ 1:10 __ >1:10

I-4)

Are all systems connected in one network?
If not, are all network blocks in the same security level?

I-5)

How often do you check intrusion activities?
___ At least once an hour
___ At least once a day
___ After the system/network being attacked
___ Other (please provide details)

I-6)

How long does it take you to review the state of your system/network?
(Choose one from each column)

| | | |
|---|---|---|
| ___ Several minutes | \ | ___ hour |
| ___ Less than an hour | \| | ___ day |
| ___ A few hours | + per | ___ week |
| ___ Several hours | \| | ___ month |
| ___ A day or longer | / | ___ other (please specify) |

I-7)

If it were possible for the work to be more automated how would you like the system/network protection work to be done?
___ Using system tools and home-grown code (e.g. tcpdump, netstat)
___ Using off-the-shelf tools (e.g. snort, NFR)
___ Outsourced to a third party
___ Other (please provide details)

II - About System/Network Protection at Your Site

II-1)
Are you solely responsible for the intrusion detection work for your network?
If there is a team, what is the team structure?

II-2)
How many people are involved in the system/network protection work?
___ Network administrators
___ System administrators
___ Other people, e.g. assistants of administrators, supervisors of administrators, etc. (please provide details)

II-3)
How many of those people's jobs are dedicated to intrusion detection?

II-4)
How is your system/network protection work currently deployed?
___% Using system tools (e.g. tcpdump, and netstat)
___% Using off-the-shelf tools (e.g. snort, and NFR)
___% Outsourced to a third party
___% Using other techniques and tools (please give some details)

II-5)
How do you prefer the system/network protection work to be done today?
___ Using system tools
___ Using an intruder detection system
___ Outsourced to a third party
___ Other (please provide details)

II-6)
Do you have defined policies for attack response?

II-7)
What types of attacks are defined in those policies?

II-8)
Some attacks are more serious than others.
Do you follow a particular routine to handle them?
If yes, what is it?

II-9)
What would you do if a new intrusion activity was reported while you are working on another one?
___ Finish the current one then start the next
___ Determine the relative risk of the attacks, and
fix the one may cause most damage
___ Other (please give details)

III - About How You Protect Your Network

III-1)
Where do you usually do the system/network protection work?
___ A specific workstation inside the network (e.g. your office)
___ Any workstation inside the network
___ A workstation outside the network (e.g. your home)
___ Other (please provide details)

III-2)
Where do you prefer to do the system/network protection work?
___ A workstation inside the network. (e.g. your office)
___ A workstation outside the network (e.g. your home)
___ Other (Please provide details)

III-3)

Do you want to have all means for protecting system/network; even if some of them are not applicable to you?
___ Yes, the more the better
___ Not all, but would like to have some as backups
___ No, one solution to fix the problem is enough

III-4)
Do you want/like to have help built-in to intruder detection tools?
___ Yes
___ No, I have the best references
___ I want help available but only when I ask for it
___ I want help available and I'd like the ID tool to make recommendations
___ Other (please give details)

III-5)
How do you investigate all of the available options when deploying network security?
___% Use help or README files provided by the system
___% Search the Internet
___% Read books
___% Other (please give details)

III-6)
Has your network ever been subject to serious attack(s)?
If so, how did you deal with the attack(s)?

III-7)
Do you want 'follow me' technology to warn you whenever an automated system detects potential threats?
___ Yes ___ No ___ It depends (please give details)

III-8)

How do you want to be informed about the intrusion?
___ Get a warning, e.g. popup messages, beeps, emails, etc.
___ An automatically generated summary report
___ Other (please give details)

III-9)
How do you want the intrusion alerts to be displayed?
___ Original data packet
___ Pre-processed readable text
___ Graphs and icons
___ Other (please give details)

III-10)
How do you want the displayed alert/log information to be organized?
___ Categorized, e.g. aggregate data in terms of IPs, signatures, time, etc.
___ Hierarchical, display the data according to the network, subnets, or machines
___ Other (please give details)

III-11)
How do you feel about your current solution to handle system/network protection work?
___ Satisfied
___ Okay, but willing to try a better one
___ Not good, looking for a new one now

III-12)
What do you want to see in the interface for doing system/network protection work?
___ Text
___ Coloured graphs and icons
___ Both

___ Other (please specify)

III-13)

Do you use someone else's intrusion detection software (e.g. that you bought or is in the public domain)?

a - If yes, how was that software chosen? How easy-to use and effective do you find it?

b - If no, what is the biggest reason that you don't use them?

Thanks for your time and help.
You may give us additional comments below.

# Appendix B

# Consent Form

Towards Improved Intruder Detection Systems

I am a graduate student studying interface design and network security. My research is about developing a user interface for a network intrusion detection system. In this project, my supervisors and I will address some usability issues network administrators face while monitoring/protecting their networks/systems. Please share your experience in network management with us.

Thanks for your time and help.

This formal consent form is required for our research. If you would prefer to have a copy on letterhead (by fax or postal mail) then please request that from Andrew Zhou <azhou@cs.dal.ca>.

Introduction

We invite you to take part in a research study at Dalhousie University which is being conducted as part of a Masters thesis of the principal researcher, Andrew Zhou. Taking part in this study is voluntary and you may withdraw from the study at any time. The study is described below. This description tells you about what you will be asked to do, and any risks, inconvenience, or discomfort which you might experience. Participating in the study might not benefit you, but we might learn things that will benefit others. You should discuss any questions you have about this study with Andrew Zhou, James Blustein, or Nur

Zincir-Heywood.

Purpose of the Study

Among various methods some network managers/administrators use network intrusion detection systems (IDSs) which help them monitoring network traffic. An IDS with good usability will increase the the quality and efficiency of their jobs. Our study is about to develop a better user interface for IDSs.

Study Design

As part of a larger study we are collecting background data to use in developing an improved interface. We are conducting a survey on network managers/administrators by sending them questionnaires. We hope the survey participants will tell us how they protect their networks and what they expect to have for monitoring network traffic. Later we will be asking volunteers to test the interface we will have made using the information gathered from the questionnaire.

Who can participate in the Study

Because the study is associated with a special domain, only people who are knowledgeable with computer system/network administration will be involved. The selected survey participants are expected to complete the form by answering questions.

Who will be conducting the research

Andrew Zhou is responsible for the background study and the interface design. James Blustein and Nur Zincir-Heywood provide guidance to Andrew Zhou's study. They also make sure the research is on the right track by reviewing Andrew Zhou's work. You can contact anyone of them for questions about this study.

What you will be asked to do

Please complete the questionnaire (or as much of it as you feel comfortable answering) and send it by e-mail to <secsurv@cs.dal.ca>. Your name and address will be removed from the questionnaire before it is used. Your answers will be treated anonymously.

Possible Risks and Discomforts

There is no risk or consequence for answering some questions but not others. There is no greater risk in answering the questions than in everyday life. All of the e-mail for this survey will be sent to and from an account setup only for this survey. Your answers will always be anonymous.

Possible Benefits

Participating in the study might not benefit you, but we might learn things that will benefit others.

Compensation/Reimbursement

Any contribution to the research is appreciated. However there is no compensation for participation.

Confidentiality

Your name and address will be removed from the questionnaire before it is used. Your answers will be treated anonymously.

Survey results will be used in a later part of the larger study. All participants will be kept anonymous in any reports or publications. Dalhousie University policy requires that data be stored securely by the University for 5 years after publication.

Problems or concerns

In the event that you have any difficulties with, or wish to voice concern about, any aspect of your participation in this study, you may contact the Human Research Ethics / Integrity Coordinator at Dalhousie University's Office of Human Research Ethics and Integrity for assistance: her telephone number is (+1)(902)494-1462; her e-mail address is <patricia.lindley@dal.ca>.

In Lieu of Signature

By e-mailing a copy of the questionnaire with your answers to Andrew Zhou at the survey account <secsurv@cs.dal.ca> you agree that:

* You have read the explanation about this study, have been given the opportunity to discuss it, have had any questions about it answered to your satisfaction;
* You consent to take part in this study;

```
   * However, you realize that your participation is voluntary and that you
     are free to withdraw from this study at any time.

Research Project Title: Towards Improved Intruder Detection Systems

Contact Information
  Principal Investigator: Andrew Zhou (Masters Candidate) <azhou@cs.dal.ca>
  Co-supervisors: Dr. James Blustein     <jamie@cs.dal.ca> and
                  Dr. Nur Zincir-Heywood <zincir@cs.dal.ca>
  Postal Address: Faculty of Computer Science, Dalhousie University
                  6050 University Ave., Halifax, Nova Scotia B3H 1W5, Canada

  Contact Person: Andrew Zhou  <azhou@cs.dal.ca>
  Survey Account: <secsurv@cs.dal.ca>
[ this is the end of the consent form ]
```