National Cyber Defense:
A Design for Securing our Future

Nathan Einwechter
April 29, 2003

Abstract

This paper represents the base design for a national cyber defense system upon which can be largely expanded to suit the needs of the many evolving requirements of law enforcement, government, research groups, and other groups of people in the context of the internet. It is largely designed around the notion of an evolving system which facilitates the need to not only shed light on the dark alleys of the internet and networks, but also to largely remove these areas. This includes everything from the malicious hacker community, to terrorist and criminal organizations operating or communication online, and child pornography producers, distributors, and viewers. Further, the system increases the intelligence capability available related to the internet significantly.

Another factor which distinguishes this system from most currently proposed or operational throughout the world is the fact that it takes civil rights into consideration. The public has a need and demand for a certain degree of privacy and freedom online which this system allows and, in some respects, promotes.

All of the work towards the concept of this system, to date, has been completed without any degree of funding. Further concepts regarding the system are also currently being developed, and papers written on these areas of interest. Further papers and design information can be expected on the topics of expansion/add-on modules, social issues, legal issues, system implementation and maintenance, system training and use, development expenses, and system reasoning.

The author is currently seeking out any level of funding , assistance, or donations to help this project and related research continue to advance.

Introduction

In a world of uncertainty and insecurity, the internet and cyber world can be a frightening and powerful place. Everything is now controlled by computers. Your bank account, stock exchanges, power grids, the military, the justice system, government, and health records are all controlled by networked computers. From a computer entire nations can be brought to their knees with a few well planned moves. A life can be destroyed in a matter of seconds using a series of simple 1's and 0's. Like a game of chess, the players move their pieces across the board. We are the defenders, they the attackers.

Now more than ever, the issue of protecting our computer networks and systems is extremely critical. As the threat of conventional terrorism increases, as does the threat of computer based terrorist attacks against the nation’s critical infrastructure and financial systems. Many experts predict that it is not a matter of if, but rather a matter of when a large scale cyber attack is launched against the nation’s infrastructure. A system to protect against these threats must be put in place if such attacks are to be thwarted preemptively, and which would allow appropriate action able to be made if attacks are carried out.

National Cyber Defense refers to the protection of a nations computer networks and systems. More specifically, a focus on government, military, and infrastructure related networks is often seen in relation to the concept. National Cyber Defense as a whole, however, requires a

much larger effort and much larger participation than just those main areas of concern. It is a process and not a single product. As such, the following National Cyber Defense system has been proposed to be one part of a series of initiatives to safeguard the nation against cyber terrorism, and organized crime online. This system will promote public and industry participation in an effort to create a safer internet for users all across the nation, while providing sufficient means in which to protect the infrastructure that is of most concern.

The system expands on the concept of distributed intrusion detection systems (dIDS), and uses innovative data collection schemes which allow for legal and security issues to be addressed. The social issues of such a system are also examined to determine any impact the system may have.

Introduction to Distributed Intrusion Detection Systems (dIDS)

The concept of Distributed Intrusion Detection Systems (dIDS) is one which any national cyber defense system will employ due to the largely distributed nature of the data to be collected and analyzed on a national level. As such, the dIDS principals will serve as the foundational concepts for such a system.

A distributed IDS (dIDS) consists of multiple Intrusion Detection Systems (IDS) over a large network, all of which communicate with each other, or with a central server that facilitates advanced network monitoring, incident analysis, and instant attack data. By having these co-operative agents distributed across a network, incident analysts, network operations, and security personnel are able to get a broader view of what is occurring on their network as a whole (Einwechter, 2001).

A dIDS also allows a company, or in this case the government, to effectively and efficiently manage its incident analysis resources by centralizing its attack records, thus giving the analyst a quick and easy way to spot new trends and patterns, as well as to identify threats to the network across multiple network segments (Einwechter, 2001).

dIDS systems consist of multiple “agents” which report either to each other in a Peer-to-Peer (P2P) intelligent network, or directly to one or a number of Central Analysis Servers (CAS). This provides the centralization of information required to complete appropriate analysis on the data, a well as to open up new research options and enforcement tools. Agents are considered to be any system which reports attack data to the dIDS system whether it be the CAS, or a P2P network.

dIDS’ have a number of advantages over tradition IDS, Firewall, and Router ACL solutions. Due to the greater view which it allows the analyst to achieve, the dIDS offers the incident analyst many advantages over other single mode IDS systems. One of these advantages is the ability to detect attack patterns across large geographic or virtual network segments, with geographic locations separating segments by time zones or even continents and virtual network segments by their respective duties. This could allow for the early detection of a well-planned and coordinated attack against the organization in question, which would allow the security people to ensure that targeted systems are secured and offending IPs are disallowed any access. Another proven advantage is to allow early detection of an Internet worm making its way

through a corporate network. This information could then be used to identify and clean systems that have been infected by the worm, and prevent further spread of the worm into the network, therefore lowering any financial losses that would otherwise have been incurred (Einwechter, 2001).

The second major advantage is that a single analysis team can now do what previously required several incident analysis teams due to physical distance. This alleviates the need to pay for distinct incident analysis teams for each separate geographic location of the organization's offices. Another issue that it addresses is attacks from within corporations network by angry, upset, or bored employees. By tying the central analysis server in with a company or ISP's DHCP or RADIUS server, the incident analysts can track down exactly who is launching attacks using the company or ISP's resources, and track what they have attempted to do, as well as provide evidence against the perpetrators (Einwechter, 2001).

dIDS' have also been shown to be effective in detecting and tracking internet worms and new attack methods or system vulnerabilities. By correlating data within the dIDS, analysts are given evidence that the perception of small attack patterns is not mere coincidence: it backs up the date to indicate that there may be something more dubious than what be concluded from a single, small set of logs. It is this ability to correlate data across numerous IDSs that allows the dIDS to be able to detect emerging and subversive worms and attacks. What may look like relatively normal activity for a given IDS can quickly turn into an obvious pattern of scans and communications to the dIDS due to its broad scope. (Einwechter, 2001)

In fact, some work has been done to mathematically model the number of agents required to detect a new worm in a minimal amount of time based on probability theory and network infection models (Xie, 2002). Xie's work on this subject becomes invaluable when one begins implementing the core agent network upon which the rest of the network is built. His mathematical equations are to be implemented and considered during the initial stages of design for the proposed National Cyber Defense system. This would also offer a method in which to verify the results of his work, or find ways of improving on the model. The equations developed by Xie also provide a function by which economic reasoning can be demonstrated for such deployments of systems, but is limited in that it only considers the events of worms.

Data Collection Schemes

Since the National Cyber Defense system is in a unique situation where it draws from many different types of sources, as well as caters to many different types of analysts, the data collection and control scheme is extremely important and very different from that of the usual dIDS setup.

To determine how the data collection system is to be designed, a number of goals must be stated upon which to work upon. The goals of the data collection and control scheme are to;

- Efficiently collect and allow analysis of large amounts of internet and incident/intrusion data for cyber threat defense and analysis
- Allow full forensic retrieval of effected data stream
- Address legal limitations
- Collect data for internet social network mapping of criminal and terrorist

organizations
- Provide a fully query able database to allow eC/cA systems as well as independent analysts to use collected data to it's fullest
- Provide built in functions for quick analysis
- Keep data secure and maintain appropriate levels of access to various levels of data

In order to achieve these goals, the system must be divided into five major areas (domains). These five domains are;

- National Cyber Defense Public Data Collection (NCD-PDC)
- National Cyber Defense Government Data Collection (NCD-GDC)
- National Cyber Defense Critical Infrastructure Data Collection (NCD-CIDC)
- National Cyber Defense Trunk Data Collection (NCD-TDC)
- National Cyber Defense Data Analysis Interface (NCD-DAI)

Each of these five major domains are then divided further into sub-domains for access control, data classification, and applied use purposes. All domains except CIDC have at least two sub-domains. These sub-domains are;

NCD-PDC
- Home/Resident Data (HOME-D)
- Business Data (BUS-D)
- Education Data (EDU-D)

NCD-GDC
- State/Provincial Government Data (STATE-D)/(PROV-D)
- Federal Government Data (FED-D)
- Classified Network Defense Data (CLASS-D)
- Unclassified Network Defense Data (UNCLASS-D)

NCD-TDC
- Regional Trunk Data (REGT-D)
- International Trunk Data (INTT-D)

NCD-DAI
- Level 1 Analyst (1A)
- Level 2 Analyst (2A)

<u>NCD-PDC</u>

Consists of regional servers which store basic incident and connection information. These regional servers would be located/created according to virtual network needs. For example, in Canada there would most likely be three or four NCD-PDC servers serving particular geographic areas (East, Central, West). Whereas, in the United States, there would most likely be one server in every or every other state depending on the virtual load of the various regions.

All data submissions in this domain are made on a voluntary basis. Home/Residential, Business, and Education facilities will submit to their respective categories.

NCD-PDC-HOME-D

Home data (HOME-D) will consist of firewall/router/ids data collected from home machines, much like the current dIDS systems myNetWatchman and Dshield. Although this data is not a vital part of the system as a whole, it can provide valuable data for correlation, incident tracking, and on-demand trending. As an advantage to these users, and to promote participation, reports can be available on demand for these users to view activity against their systems with reference information linked about each particular incident. The submission software will be available for free download to anyone wishing to participate. An account must be registered and created. Accounts are used for a number of reasons. One is to ensure that not just any random system can submit random data to the system to confuse it. The login also allows certain data to be filtered out if it is discovered that user has been submitting false data, therefore ensuring maximum data validity.

NCD-PDC-BUS-D

Businesses will submit their data (BUS-D) and pay a fee. This data will consist of much the same information as that of the HOME-D category. It will, in addition, include basic session information, listed in Appendix A. This extra session data will be put toward the virtual mapping module for virtual terrorist or criminal communications mapping which is to be explained later. This fee is increased slightly if the business agrees to store all data across the network which reaches outside of their private network, according to dynamic rules set by the federal analysts. The cost benefits of this action are explained later. This would mean the company would have to buy the monitoring equipment, but a cost saving benefit should be built into the pricing as incentive. This would allow the federal analysts to target specific computer systems or types of communications from businesses for analysis of data going out to the internet that follows certain rules or contains certain key words of interest. By leveraging the business' ability to monitor all of its own computer systems, no warrants or legal issues come about. It's currently common practice for companies to monitor employees access as it is, this is merely an extension of this to prevent and monitor terrorist or criminal communications through employer networks.

The fee paid out by the business' is offset by a number of incentives. The first of these is the reduction of internal liability for business'. The system provides the business a suitable amount of accountability and traceability of any misuse of their internal resources. As such, the company is unlikely to be held liable for any internal abuses to external sites, as the system allows those people to be quickly traced and dealt with. Another incentive is through insurance. Insurance companies, especially if approached by the government, are more likely to give lower insurance rates on specific related types of insurance to those whom are using this system. This can be expected due to the increased level of accountability for internal users as mentioned earlier. The companies participating in this also have the reporting capabilities as the HOME-D users do, where quick aggregation and automated analysis and information on events is easily accessible. These incentives should more than offset any fees paid out by the business', if not save them money. Further, it provides a certain level of funding to reduce the governmental budgeting requirements of the system.

NCD-PDC-EDU-D

Educational data will function in a very similar way as the business data. The only difference is that universities/colleges will be able to see and use non-specific data collected by the systems for research in various areas (i.e. graph theory, networking mapping/modeling). This research could also yield further advancements and developments applicable to the system as a whole.

NCD-GDC

Unlike the NCD-PDC domain, those computer systems or networks falling under the Government Data Collection (GDC) domain, would be required to store and submit specific types of data to the system. These systems include those which fall under the various categories listed earlier. The reasoning for creating the sub-domains of GDC is to enable access control to different types of data, and allow specific areas of interest to be easily isolated, yet still correlated across the entire data source. For example, only people or groups authorized to view data on classified networks would be able to use Classified Network Defense Data (CLASS-D) in their analytical/network status checking abilities. State/Provincial investigators could focus on their respective data, while federal investigators focus on theirs as well as the State/Provincial data as correlation. As such, correlation will be available across the different data sources in the different sub-domains and domains. Certain data sources will be unavailable to certain groups of people in a permission based system (according to classification).

The collection systems for this domain will be similar to that of the business data collection model, where basic session data is logged to one of several central (regional) servers for link analysis within the system. Specific conversation information is logged locally for further access at a later date. The specific logging and submission scheme for both this system and the business system, both of which are virtually the same, are found in Appendix A.

NCD-CIDC

Critical Infrastructure Data Collection (CIDC) is an important piece of the puzzle when discussing the National Cyber Defense initiative. A nation's critical infrastructure includes those systems which control or are part of a network which control energy, oil, transportation, law enforcement, defense, and economic centers (such as stock markets). Data collected from these sources important in detecting any attack against the infrastructure early. Maximum scope over these networks is absolutely critical. Session information is stored on all communications,

NCD-TDC

The collection of trunk data is a unique concept that has floated around for quite some time now. There have been several issues with data collection of trunk data in the past. The two main problems are bandwidth multiplication issues (lack of bandwidth), and legal/privacy concerns. The national cyber defense design plans to circumvent these issues using a few simple steps.

The first problem of multiplication issues occurs when you log raw data from a bit data stream and try to send it to any type of centralized server. You end up taking the original packet information and putting it into another packet to be sent out. This means that you have your original transmission (1), which is then sent out (1x2) with additional packet header information

and the need to spread it across two packets. This gives you an approximate multiplication factor of;

1.5[1x2] = 3

Based on this, you end up sending three times more data across that particular line, or two times more across a line other than the one the bit stream data was collected from. Obviously this is not a plausible situation, especially if the critical objective of placing this system upon existing infrastructure is to be met. More specific figures for bandwidth multiplication issues will be explored once research funding is granted.

The trunk data is separated into two categories largely for legal and privacy concern issues. The two separate categories are regional trunk data (REGT-D) and International Trunk Data (INTT-D).

NCD-TDC-REGT-D

Regional trunk data is data collected from major lines of networking communication (backbones etc.) from within the countries borders, which does not take any direct data from any international source. The trunk data collected from a regional source, within this design, will only log basic session information as noted in Appendix A. Payload data is not collected due to privacy laws. The system would be designed such that payload data could be collected given a warrant is issued for the collection of a specific set of data.

This design solves both the problems identified, where bandwidth multiplication does not occur when limiting the logged and sent data to just the basic session data. It also significantly decreases the privacy issues as no personal data is being logged, and, without further investigation, it is not easily determinable exactly who is using each IP address whose communications are being logged. The reduction of logged data to basic session information still allows significant analysis capabilities particularly when mapping criminal and terrorist networks using the internet as a means of communication. This mapping theory will be discussed in further detail.

NCD-TDC-INTT-D

The International Trunk Data category is similar to the regional trunk data category with a few differences. The first major difference is that international trunk data is data which is being logged from trunks (backbones) which arrive directly from international sources. This gives the software legal leeway in that the monitoring of international communications is legal and not an invasion of privacy. Due to this, the system is more able to monitor and log payload information according to keywords, packet/session characteristics, etc.

This design solves the same problems in the same ways as the REGT-D design as they are very similar in nature. A small amount of extra bandwidth should be accounted for in the INTT-D design due to the fact that it will most likely be logging more payload information than the REGT-D. The total amount of bandwidth needed can also be reduced by using advanced high compression methods.

NCD-DAI

The data analysis interface is divided into two categories. These categories could further be broken down as classification and analytical requirements change or are understood within the context of application.

Level 1 Analyst (1A)

The Level 1 Analysts are all those whom do not hold a current government clearance sufficient for the data that is being logged to the classified servers. These people will consist of private researchers, educational organizations and researchers, and some law enforcement. These people will be limited to accessing the non-classified regional servers for analytical information only.

Level 2 Analyst (2A)

The Level 2 Analysts are all those whom hold a current government clearance sufficient for the data that is being logged to the classified servers. These people will have access to both classified and regional servers as required for analytical data.

Databases

Under the current design, there are two separate categories of databases. The databases themselves are virtually the same except in regard to their content, data validity assurance, and who can access them. These two main categories are Regional Server (RS) and Classified Server (CLASERV).

The regional servers receive their data from public data collection and non-classified government (state/provincial, and federal) sources. All authorized analysts have access to the data on the regional servers. The classified server, on the other hand, receives any and all data being submitted by a node or system on a sensitive, or classified network. Only those authorized analysts maintaining proper clearance to the most sensitive data that is transmitted across a submitting network may access the data from the classified server (Level II or Level III security clearance in Canada, TS/SCI in United States).

The databases as a whole are to be designed in a distributed manner. Queries and correlations will actually be made across multiple different databases which serve as a single virtual database. Those without proper clearance will only be enabled to correlate across the regional servers, proper security precautions and safeguards must be put in place to ensure this. Proper authentication must also be made to enable any user to allow correlations to include data from the classified servers. Analyst access points are suggested to enable this, where a number of secure authentication servers are in place to determine an analysts level of rights on the various servers, and then allow or deny access accordingly.

Data Analysis Schemes

The data collection scheme solves a lot of the previous problems with large scale cyber defense by bringing the data into one small set of accessible databases. Once this data has been semi-centralized to multiple databases, and the databases linked together to create a full centralization to access the data, analysis becomes a simple issue. The data collection method and centralization allows for full forensic retrieval of many events. It also allows innumerous research opportunities for Universities and research groups interested in data collected.

Due to this centralization and the use of standard database systems, add-on modules and external systems can be quickly and inexpensively integrated into the National Cyber Defense design. This means that existing analysis systems can be easily implemented into the design. It also provides the opportunity to research groups to test analysis methods and new techniques on this great source of data. Technologies and techniques such as eventChemistry, categoricalAbstraction, and Social Network Mapping can be easily verified and demonstrated using the system data as a test bed. The design of the system also keeps these add-on modules isolated from the system, thus preventing any security concerns regarding the modification of data. As such, the system provides a large number of significant research opportunities, and helps reduce the cost of government to allow this research to occur.

The initial design and development of such a system would include a number of built in analysis functions such as event aggregation, and utilize statistical analysis techniques. A scripting system will also be provided to customize data analysis queries to suit specific investigations or research.

Terrorist/Criminal Network Mapping Theories

One module proposed to be in the initial design and development is the terrorist and criminal network mapping system. The advent of modern communications, particularly by computer and the internet, have allowed a new means of communication for terrorist and criminal groups. The internet gives these groups the perfect medium to communicate and co-ordinate. This is even more true when one considers the wide-spread use of strong cryptography today, and the relative security this gives these organizations and groups. Thus, the internet, coupled with strong cryptography, gives these groups a definite advantage over the intelligence community than has ever been seen in the past.

The following design is a theory towards the mapping of social networks within these particular groups of people. The method is just as applicable to encrypted messages as it is to plain text as the actual message itself is not important. It also uses basic link analysis and mathematical networking concepts to map out the various participants within a group or organization using the internet as a medium to communicate and co-ordinate for terrorist or criminal intentions.

Through the basic session information gathered via the data collection design as proposed in an earlier section, one can map out exactly who is connecting to where on the internet within a given monitored virtual network. In plain language, this means that we can determine things that one person or set of people (IP or set of IPs) have in common with another person or set of people (IP or set of IPs). By utilizing this knowledge, the system could be given the IP or host address of a known terrorist or organized crime member and derive, from that, a large number of IP addresses with whom the known terrorist or criminal has common links with. This can also expose methods of communication among terrorist and criminal elements, thus supporting further investigation into such groups.

Current software and tools are available which use advanced methods of social network mapping, and can be easily and efficiently implemented into this National Cyber Defense design with a minimal amount of expense.

Implementation

Implementation of the system is relatively straight forward. Once the system design is complete, implementing the design becomes relatively simple. It has been created with currently existing infrastructure in mind, and the limitations of that infrastructure. Due to the fluid nature of the network, the only part of the systems which need to be built are the database servers, analysis servers, and the agent software to be run on the various participating systems to submit data to the servers. Beyond this, the main implementation issues come in the form of creating policy requiring government at all levels to utilize the system, as well as providing training on implementing the system in various departments and organizations within the government. Due to the scale of this system, the level of marketing required to get public participation is expected to be low. A large amount of hype should drive participation of the system quite well for the initial period of operation.

Ease of use for the general user and basic law enforcement analysts is built into the system in the form of built in analysis tools and add-on modules. This reduces further the cost of training, and promotes those people to use it. A tool that people find difficult to use will not be used, and this system has been designed around that concept.

As will be discussed in the following section, no new laws should be required to allow this system to become operational. This prevents the system from being held up by the legislative process, and allows legislators to feel more comfortable with the system. Laws which they already know and have already approved are of a significantly less concern to them, as are the laws which may open up privacy concerns or issues to the general public. This design prevents these concerns from arising by staying within current laws.

Legal Implications

The use of private and voluntary data submission as the primary source of data collection for the system ensures that many legal concerns are addressed. Companies have the legal right to monitor any and all data which crosses their networks. This has been demonstrated over the years by the continued support of the legal system in cases where employees e-mails have been monitored, or data given to law enforcement without a warrant. As such, it is largely recognized that companies, and educational institutes, have this right on their networks.

The main area of concern initially was in the trunk data collection area. Due to these concerns, the trunk data is separated into two different sections, as noted earlier. Since no actual payload data is recorded in the regional trunk data category, the need for a communications interception warrants are is removed. This requirement is removed from the international trunk data by national security and telecommunications monitoring laws, under which foreign communications can be monitored.

Given the voluntary nature of most of the data collected, and the methods of collecting the different types of trunk data, the legal concerns are largely negated, and thus become of little concern to the operation and effectiveness of the system.

Social Implications

Socially, there are a number of implications with any such large scale monitoring system. General public response is expected to be relatively neutral. Some members of the public may be somewhat leery about the power held within the system, but over time will grow accustomed to its presence. This is especially true once the value of the system is demonstrated to the public. Online credit card fraud can be significantly reduced down to near zero levels, and new security measures for secure e-commerce can be put into place as modules to the system. Some degree of protest and petitioning should be expected

Response from the hacker community, as well as privacy advocates, however, is expected to be similar to the response to the Carnivore project which occurred in the United States. Attempts to design systems to circumvent and confuse the defense system are an almost certainty, although the system is designed in such a way that doing so will be extremely difficult. The fear that "big brother" is watching what everyone does online is also a concern, although this can be quelled through public awareness education about the system, and the lack of information it actually records , unless you voluntarily allow it to record more. A certain amount of attacks against the system are expected, and acts of "hacktivism" are likely to occur in response to the deployment of any such national cyber defense system.

Over time, more criminals and terrorists will realize that they can not hide their actions online and will be forced to either employ new techniques, or quit altogether. This creates a situation in which the common day "script kiddies" will become less and less frequent, and the more sophisticated attacker left as the only threat online. Once this occurs, resources can be moved away from dealing with the low threat hackers, and towards removing those high threat sophisticated attackers.

The security industry will view this system with mixed emotions. Many of the hardware vendors and managed security service providers (MSSPs) will see the system as a threat to their business and products. Other people in the security industry, particularly those doing research, will view the system as a significant advancement and a great tool for future research purposes. As such, industry coordination and awareness is required to reduce the risk of corporate action against the system.

Education about the system is the most significant factor to reducing any negative social, and political, implications involved with the system. Should the appropriate amount of information be given to the general public and industry, the system will have a minimal impact on today's social structure, excluding the hacker culture.

Conclusion

The internet has become a volatile and insecure place, and is increasingly becoming more and more so. Cyber terrorist have the capability to shut down an entire nation's power, disrupt financial transactions, and commit crimes to finance physical operations. Organized crime is also increasingly making use of the internet as a means of communication and financial gain. Peoples lives can be destroyed with a few well planned key strokes, and the entire nation brought to it's knees.

A defense mechanism must be put in place to prevent any of these actions from occurring and in order to protect the general public. The proposed National Cyber Defense system provides one significant layer of such a defense mechanism, and is a key to keeping the nation safe. Without such a system, the nation is left wide open to any people with the right knowledge to come along and take advantage of the defenseless position which the nation finds itself in. This must not be allowed to happen. As such, it is extremely critical that a system such as this be put into place without waiting until it is too late.

The safety of a nation and its way of life depends on it.

Appendix A

The following data will be collected from their respective sources;

HOME-D

- Firewall, IDS, and Router logs
- Basic attack information (source, destination, attack type, protocol, payload)

BUS-D1

- Everything in HOME-D
- Session information for out of business communications (source, destination, protocol)
- Voluntary logging of all payloads matching certain criteria (i.e. keywords, protocol types, sources, destinations, etc.)

EDU-D; STATE-D/PROV-D; FED-D; CLASS-D*; UNCLASS-D

- Same as BUS-D2

* No logging to sites containing non-classified data.
Only authorized/cleared analysts may access.

INTT-D

- Same as BUS-D with payload logging, and no intrusion/firewall data

REGT-D

- Same as INTT-D without logging of any data payloads

Bibliography

Einwechter, Nathan. (January 8, 2001). An Introduction to Distributed Intrusion Detection Systems. *SecurityFocus.Com*. Retrieved May, 2003, from; http://www.securityfocus.com/infocus/1532

Einwechter, Nathan. (October 16, 2002). Identify and Tracking Emerging and Subversive Worms Using Distributed Intrusion Detection Systems. *SecurityFocus.Com*. Retrieved May, 2003, from; http://www.securityfocus.com/infocus/1634

Xie, Bin Q. (June, 2002). The Effect of Infection Behaviors of Computer Virus on Early Detection and Detection Systems Deployment Strategies. *International Conference on Telecommunications 2002*.