Research Proposal
Intrusion Detection in Distributed Multimedia Applications

Regina Awor Komakec
(s0535273)

March 31, 2007

Contents

1 Introduction

The current trend is that it is becoming increasingly easier to attack computer systems. More people with limited computer knowledge (script kiddies) can carry out attack on poorly maintained systems, because attack tools are increasingly accessible and usable. A manifestation of this is the movement of attack tools from command-line to graphical-based tools. The Iris Network Traffic Analyzer (formally known as SpyNet) [5], for example, is a GUI (Graphical User Interface), packet sniffing tool.

Information system security is important in this computer age. It goes without saying that information management is crucial for the survival of any firm. Security breaches can have damaging consequences particularly for e-business,

which is simply Internet-aided business. Enterprises, for example, depend on information to run their businesses, which is constantly increasing. Hence, there is need to ensure its security, vis-à-vis confidentiality, integrity, and availability, to maintain a competitive edge over other businesses. Many assume that by securing entry into the network, they can secure their systems. It is not sufficient to focus only on security within networks. Other aspects of the whole system also have to be taken into consideration; for instance, operating system and application security, such as, software and database security.

It is important to note that the main threat to information systems comes from people. These threats do not only originate from outsiders, but also from insiders who misuse their privileges. Intrusion detection systems (IDS) are therefore necessary to cope with the increasing threats, both from inside and outside, which are becoming even more difficult to predict. The basic idea of intrusion detection systems is that there is a clear distinction between the behaviour of an intruder and that of a legitimate user.

The focus of research will therefore be the investigation of intrusion detection within distributed multimedia systems.

2 Background

Intrusion detection refers to the ability to detect and respond to inappropriate activity [6], [8]. Inappropriate activity, in this case, may include unauthorised or malicious use and abuse of computing and network resources. It is almost impossible to build a computer system free of vulnerabilities.

2.1 Approaches to Intrusion Detection

The primary categorisation of intrusion detection is as anomaly detection and pattern-matching detection [1]. Anomaly detection, sometimes called Statistical anomaly detection, searches for abnormalities. Activities are observed and if they deviate significantly from normal usage profiles are marked as anomalies [7]. Since it is behavioural based, it has the ability to detect novel attacks. However, it also has a high rate of false positives.

Pattern-matching or signature detection, on the other hand, depends on some previously defined pattern or signature of a known intrusion. Lee *et al.*[7] refers to this category as misuse detection, and defines it as the matching of patterns of well-known attacks to known intrusions in audit data. This raises an important question, what about new attacks? Although the rate of false positives is low, there is a high rate of false negatives.

The ideal intrusion detection system should have a high rate of detection and a low rate of false alarms [2]. Developing an efficient, updatable intrusion detection system is always going to be a difficult task. It is for this reason that more systematic approaches of developing intrusion detection systems have been proposed. Lee *et al.*[7] suggested a data mining framework for building intrusion detection models.

2.2 General Model of Intrusion Detection System (IDS)

Before modelling an intrusion detection system for a computer system, it is vital to consider how it interacts with its environment. The external environment includes the behaviour of users, including intruders, from whom input comes. The intrusion detection process starts with determining what is to be detected, and eventually results in a decision being made.

The system receives input (information), for instance a user command to the system. This information is transferred to an analysis module, which includes a data processing module and a decision-making module. The output is the action taken. For instance, in case of suspicion an alert is triggered based on certain rules; otherwise continue with usual mode of operation [1].

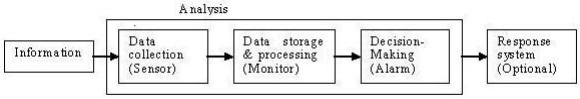

Figure 1: General Model of Intrusion Detection System

The analysis module (see figure 1) consists of the IDS components, which manage security events, usually defined by a security policy, through event generation (Sensor collecting data), monitoring, and alert generation. In event of an alert, the intrusion detection system has to respond by simply sending a notification to the administrator through, for example, e-mail or SMNP trap, or responding directly, by say, disabling a user account [4]. This direct reaction to the alarm is undertaken by a response system.

Axelsson [1] highlights several areas of concern particularly in security logging, where there is a difficulty, not only in determining what information to store in the log, but also in differentiating information from the "subject" and that from innocent (benign) usage of the system. His concern is how to address the possibility of formulating the rule that governs intrusion detection decisions.

2.3 Types of Intrusion Detection Systems

Intrusion detection systems may be network-based, host-based, or application-based, where systems in each case undertaking the anomaly or pattern-matching detection approach. This presents a kind of two-dimensional matrix-like categorisation of IDS. While network-based intrusion detection systems monitor all packets (network traffic) for intruders, host-based intrusion detection systems reside on the host and monitor log files for intrusion. There is a close relation between host-based and application-based systems. While host-based IDS monitor operating and file systems, application-based intrusion detection systems monitor only specific applications. Application-based systems are therefore sometimes classified under host-based systems [9]. All these intrusion detection system types look at attach signatures, which are specific patterns that usually indicate malicious intent.

2.3.1 Network Layer Intrusion Detection

Network-based intrusion detection checks if packets match a "signature", which could be a string, port, or a header condition [8]. A network intrusion detection system (NIDS) therefore may include a packet sniffer and a logger, which helps detect attacks, like buffer overflows, stealth port scans, Common Gateway Interface (CGI) attacks, Server Message Block (SMB) probes. Snort [10] is a popular network intrusion system.

Naturally, attackers want to hide their identity. A common practice is to use technique called Stepping-stones, where previously compromised, intermediary hosts are used to initiate attacks, rather than the attacker's own computer. Stepping-stone detection attempts to detect traffic involved in stepping-stone attacks at the routers.

Notions such as round-trip time (RTT), thumbprints ("signatures"), and traceback are common notions applied in several network intrusion detection and response systems. In the networking context, round-trip time can be defined as the time a packet takes to travel back and forth between hosts. The TCP transport protocol keeps an estimate of RTT. Huang [3] highlights the difficulty with the TCP protocol in matching the packets, as they are not one-to-one mapping.

A thumbprint is basically a signature of a session; it characterises a session. It is both content-based and time-based; it calculates time gaps between packets and includes round-trip time (RTT). According to Huang [3], the advantages with this approach include: use of small storage space, hides transmitted content, and computes efficiently. However, since it is content-based, it is unsuitable for encrypted sessions.

Traceback is a technique used to trace back an attack to its source. It is therefore not a detection feature, but rather it constitutes the response activity of the network intrusion detection system, particularly for anonymous attacks.

2.3.2 Application Layer Intrusion Detection

As already mentioned, it is important to ensure the security of the applications, particularly in the case of critical, real-time systems. Application IDS are systems designed for a specific application, such as a Web server. There are several systems where intrusion detection can be applied, for example, financial systems (fraud detection systems), information management systems (databases), identity management systems, and so on.

2.4 Network Layer and/or Application Layer Intrusion Detection

It has been widely suggested that a combination of network and application-based intrusion detection is more efficient than each one separately. According to Lee [6],

'Intrusion detection at application can potentially offer accurate and precise detection for the targeted application.'

This implies that intrusion detection is not only necessary at network and host level, but also at application level.

3 Research Question

How well can intrusion detection systems deal with the dynamic nature of the computer environment?

The research question will be addressed in a distributed multimedia application setting. The teleconferencing application will therefore be used as a case study.

3.1 Sub-Questions

The following sub-questions will be applied to the case to help answer the main research question:

- What is the dynamic nature of the computer environment?
- How will effectiveness be measured?
- What is the benchmark for attacks?
- Given the two approaches to intrusion detection, which is more (cost) effective; statistical anomaly detection or pattern-matching detection with regard to network and/or application-based intrusion detection?
- What are the possibilities of combining network- and application-based intrusion detection?

4 Relevance of Research

The extensive use of computer systems for business purposes has made them even more vulnerable to attacks. It has become costly to keep up with the number of security breaches that are on the rise. Intrusion detection systems cannot work alone. Intrusion detection by no means solves all security problems; rather it supplements other security measures.

The motivation behind this research is to describe/build an effective intrusion detection system. Given the increasingly dynamic nature of today's computing environment, there is always the trade-off between accuracy and adaptability, as well as being all-embracing.

5 Research Methods

Apart from studying literature, I intend to use the aforementioned case study to investigate the issues raised in the research. I also propose using scientific tools, such as data mining techniques, particularly Bayesian networks as an analysis tool.

5.1 Proposed Case Study: Distributed Multimedia Applications

Distributed systems in general consist of three components: the server, the clients, and the communication (information flow) channel linking the server to the client.

With distributed multimedia arises the notion of video-on-demand, audio-on-demand, and Quality of Service (QoS), which includes, among others, latency, jitter, and loss rates. The applications might be classified as interactive or non-interactive. Multimedia information not only constitutes continuous data, but also discrete data, like text and images. Distributed multimedia systems can also be classified as either real-time or non-real time applications. Real-time applications may have, what is commonly referred to as, soft deadlines, where a short time delay can be tolerated. Hard deadlines are mostly associated with safety critical applications.

5.1.1 Teleconferencing

Teleconferencing is a distributed multimedia application, which deals with the real-time information sharing among people and/or machines in remote sites (see figure 2 below).

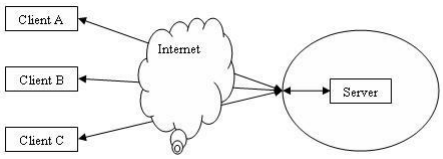

Figure 2: General Teleconferencing Model

Teleconferencing might be either phone-based or Internet-based. Phone-based teleconferencing refers to interactive communication sessions over telephone lines, while Internet-based teleconferencing refers to communication sessions conducted over the Internet. Phone-based teleconferencing has existed for years. But, the Internet is currently a popular choice for the delivery of information to the intended recipients. Not only do more people have access to the Internet than ever before, it is easier to install and use Internet-based services such as Voice over IP (VoIP) applications.

However, the Internet is certainly not the safest 'environment'. Packets can travel all over the world before arriving at the final destination. There is therefore less control over the communication channel with Internet-based teleconferencing as compared to teleconferencing by phone, hence it is more susceptible to attacks.

Security Issues in Teleconferencing

Security simply means regulating access to assets, that is data (information). Access regulation involves ensuring the confidentiality, integrity, and availability of data. Attacks to data, particularly in transit, include: interruption, interception, modification, and fabrication, which are threats to availability, confidentiality, integrity, and authenticity, respectively. The security challenge of the teleconferencing application is to find the right balance between these notions.

Referring to Figure 5-1, the goal is to ensure that only Clients A, B, and C have access to the conference (confidentiality), the information transmitted during the conference is delivered to the intended audience, within a specific time frame (availability), the data transmitted amongst invited conference members is not tampered with (integrity), and the sender cannot deny making a transmission (non-repudiation).

5.1.2 Intrusion Detection and Teleconferencing

The natural approach to intrusion detection is to determine what normal or abnormal behaviour is. But, how is abnormal behaviour recognised within a system? One approach is to use attack patterns.

With real-time systems, there is an extra requirement, namely the ability to detect attacks in real-time. This is the motivation behind studying intrusion detection in teleconferencing applications. The complication here is that data is fast changing, and therefore must be continuously monitored and managed by, say a backend real-time database. In this case, apart from a real-time network IDS, like Snort, an application IDS that monitors the activity of the database server might be required.

6 Work Plan

The target for finishing is the first week of July, which is week 27. In order to achieve this goal, there will be weekly meetings with the supervisor to present the deliverables.

For work plan see table 1

References

[1] S. Axelsson. Intrusion detection: A survey and taxonomy. PDF document, 2000. `http://www.cs.plu.edu/courses/CompSec/arts/taxonomy.pdf`.

Week	Task	Deliverables
Week 12	Writing proposal	Draft proposal completed
Week 13	Editing draft proposal	Final proposal
Week 14	Research on sub-question 1	Deliverable 1
Week 15	Answering sub-question 1	Sub-question 1 answered
Week 16	Research on sub-question 2	Deliverable 2
Week 17	Answering sub-question 2	Sub-question 2 answered
Week 18	Research on sub-question 3	Deliverable 3
Week 19	Answering sub-question 3	Sub-question 3 answered
Week 20	Research on sub-question 4	Deliverable 4
Week 21	Answering sub-question 4	Sub-question 4 answered
Week 22	Research on sub-question 5	Deliverable 5
Week 23	Answering sub-question 5	Sub-question 5 answered
Week 24	Answering research question	Deliverable 6
Week 25	Writing draft report	Draft completed
Week 26	Reviewing draft report	Final report written
Week 27	Editing final report	Report handed in

Table 1: Work Plan

[2] D.E. Denning. An intrusion-detection model. In *IEEE Symposium on Security and Privacy*, pages 222–232, Oakland, California, USA, April 1986. IEEE Computer Society Press. Available at: `http://csdl.computer.org/dl/proceedings/sp/1986/0716/00/07160118.pdf`.

[3] S. Huang. Intrusion detection design and analysis of algorithms. Powerpoint presentation, September 2005. `http://www.cs.uh.edu/events/2005_09_minitalks/Huang.ppt`.

[4] P. Innella and O. McMillan. An introduction to intrusion detection systems. Article on the SecurityFocus portal, December 2001. Available at `http://www.securityfocus.com/infocus/1520`.

[5] Network security packet sniffer iris network traffic analyzer. Available at `http://www.eeye.com/html/Products/Iris/index.html`. Accessed Mar-16.

[6] S.Y. Lee, W.L.Low, and P.Y.Wong. Learning fingerprints for a database intrusion detection system. In *7th European Symposium on Research in Computer Security*, volume 2502/2002, pages 264–279, Zurich, Switzerland, 2002. Springer Berlin / Heidelberg. Available at: `http://www.springerlink.com/content/ntk16qdvfjhrbdja/fulltext.pdf`.

[7] W. Lee, S.J. Stolfo, and K.W. Mok. A data mining framework for building intrusion detection models. In *IEEE Symposium on Security and Pri-*

vacy, page 0120, 1999. Available at: http://csdl.computer.org/dl/proceedings/sp/1999/0176/00/01760120.pdf.

[8] D. Lehmann. What is id? SANS Institute: Intrusion Detection FAQ. Available at http://www.sans.org/resources/idfaq/what_is_id.php?portal=7a7d026c64983858261f04abc00ec026. Accessed Jan-07.

[9] K. Scarfone and P. Mell. Guide to intrusion detection and prevention systems. Special Publication 800-94, National Institute of Standards and Technology, February 2007. Available at http://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[10] Available at http://www.snort.org/. Accessed Mar-16.

[11] IBM Web Services Architecture team. Web services architecture overview. *IBM Journal*, September 2000. Available at: http://www-128.ibm.com/developerworks/webservices/library/w-ovr/.

Appendices

A Intrusion Detection (ID) Models

Several intrusion detection models have been suggested. Denning's (1986) IDES model forms the basis for several intrusion detection systems. Other approaches involve the use of agents for intrusion detection (Asaka, et al., 1999).

A.1 Denning's (1986) Intrusion Detection IDES Model

Denning's IDES model checks mainly for abnormal behaviour.

Subjects Initiators of actions; users/processes

Objects Resources managed by system; recipients of actions

Audit records Logs of system activities

Profiles Representations of subject behaviour with respect to objects

Anomaly records Log of abnormal behaviour

Activity rules Define what actions are taken when some condition is met

B Ideas for Applications To Study

B.1 Information Management

It goes without saying that information management is crucial for the survival of any enterprise. Databases are usually used to manage this information, which includes sensitive information. While the number of e-commerce sites using databases at their back-ends is increasing, the number of security breaches to these databases is also increasing. Threats to databases include, among others, illegitimate access to the system (passive attack) and/or modification of database contents (active attack). A common active attack on databases is the SQL injection attack, where the SQL code is manipulated.

Today, e-business has evolved such that it involves Web Services technology, which allows back-end interactions between computer systems, business applications, and software components. This has complicated the issue of ensuring computer resources.

B.2 Web Services

As mentioned above, e-business nowadays involves back-end interactions between computer systems, business applications, and software components, hence web services technology has become today's business's enabling technology.

> "Web services are self-contained modular applications that can be described, published, located and invoked over a network, generally, the Web." ([11])

Web services support interoperability between software components, in machine-to-machine interactions over a network.

B.3 Identity Management

Today, several identity management systems use biometric identification technology, for example finger-imaging technology. It goes without saying that ensuring security of people's identity is an important issue. Security involves ensuring privacy, integrity, as well as protection from identity theft, which is a growing concern.