Technical Aspects of Intrusion Detection Techniques

Final Year Project 2003-04

Project Plan

Version 0.2

28th, November 2003

By

Cheung Lee Man

2001572141

Computer Science and Information Systems

Supervisor

Dr. H.W. Chan

Document Revisions

Revision	Date	Author	Description
0.1	22/10/2003	Cheung Lee Man	Initial draft
0.2	28/11/2003	Cheung Lee Man	Outline of contents revised

Table of Contents

Introduction

Plan overview

Plan statement

The project plan briefly describes the project with title “Evaluation of Intrusion Detection Techniques: State-transition Analysis and Statistical Analysis”.

It states the background of intrusion detection and why we need intrusion detection. Then, we briefly introduce two approaches of intrusion detection systems: misuse detection and anomaly detection. After that, we will describe the state-transition analysis and statistical analysis shortly. The project plan also states the outline of contents and what will be achieved in the project and how they can be done. Overall schedule and milestone will be provided in the project plan.

Scope

The scope of the project includes the evaluation of the two techniques. It studies the underlying assumption, principle and characteristics of each technique. After the analysis of the basic principles, statistical component of Next-Generation Intrusion Detection Expert System (NIDES) and UNIX state transition analysis tool (USTAT) will be presented in order to show the design and implementation of the techniques. Survey and technical reports will be used to evaluate the performance of the techniques and analyze the pros and cons of the techniques. After all, suggestions of improvement will be studied.

Revision Process

The project plan will be reviewed at the end of the semester to evaluate the achievement in the first semester and how the actual work deviated from the project plan. It checks whether the schedule is followed. Hence, estimation should be done in order to ensure the project will be finished on time in the second semester.

Project

Project Title

"Evaluation of Intrusion Detection Techniques: State-transition Analysis and Statistical Analysis".

Background

As computer systems increasingly perform critical operations and deal with important data, the lack of computer security can lead to loss of money, loss of manpower, reputation destructed, etc. The goal of computer security is to protect the resources of the computer systems. The requirements include confidentiality, integrity and availability. Confidentiality ensures authorized access, integrity ensures the consistency of data and availability ensures the information would not under the denial of service. Before using intrusion detection system, three areas are used to deal the first line of defense of the computer systems. They are 1. Access control to control the access between subjects, objects and subsystems, 2. Identification and authentication (I&A) to identify subjects and objects, 3. Network security includes packet-filtering firewall, cryptography, etc. However, there are still vulnerable attacks such as bugs in I&A, wrong configuration of access control, weak key in cryptography.

The general goal of intrusion detection systems is to analyze the activities in the system to see if there is any violation of the computer security. It is a security approach that enables to detect the attacks (by monitoring the system's activities) after it occurred, so that it is capable to deal with the security problems mentioned above (as if the first line of defense was bypassed, there is no defense for the computer system). Basically, there are generally two approaches of intrusion detection. They are misuse detection and

anomaly detection. Misuse detection is the detection of suspicious activities that directly violates security policy. The goal is to identify these suspicious actions and check for the occurrences of the actions in audit trail. Anomaly detection establishes normal behavior of subjects by observing audit trail over duration of time. An audit trail that deviates from the normal behavior is an indicator of intrusion occurs.

Basic concept

State transition analysis

State transition analysis models penetrations as a series of state transitions that lead from an initial secure state to a target compromised state in terms of signature actions and state assertions. State transition diagram is a graphical representation of penetrations. It identifies precisely the requirements for the compromise of penetrations and presents only the critical events that must occur for the successful completion of the penetrations. It is written to represent to the states of the actual computer system. The diagrams form the basis of rule-based expert system for detecting penetrations, called STAT. State transition analysis differs to common rule-based system that it focuses on the effects that the individual steps of a penetration has on the state of the computer system so that audit records can be independent of rule-base. The design and implementation of a UNIX-specific prototype of this expert system, called USTAT is also presented.

Statistics analysis

It observes the audit trail in order to draw conclusion about the normal behavior of subjects (which can be users, groups, remote hosts, entire system). Multivariate method (frequency tables, means, and covariance) is used for profiling normal behavior and identifying deviations. It maintains statistical knowledge base of subjects and audited activity which are used to compare the incoming audit trail with the profiles. When audit record comes, the relevant profiles are retrieved from the knowledge base. Then, a comparison will be made between the vector of intrusion detecting variables and the vectors in profiles. If the vector of intrusion detecting variables are sufficiently far from the vectors in profiles, then the activity is identifies anomalous.

Aims

The aim of the project is to evaluate the 2 techniques by studying the principles, assumptions and characteristics of them. For each technique, we will also study their design and implementation (The statistical component of NIDES for statistical analysis and USTAT for state-transition analysis) in order to have a deeper understanding and get the performance results from their technical reports and surveys. Through the study of the techniques and applications, pros and cons will be analyzed, and limitations of the corresponding technique and approach will be revealed. Lastly, it will study suggestions of improvement towards the tools and techniques.

Outlines of contents

Summary

Introduction [16, 19, 20]

- What is intrusion detection?
- Why do we need intrusion detection?

Taxonomy of intrusion detection approaches

- Misuse detection
    - Expert system [1]
    - Signature analysis [2, 3]
    - Pattern matching [4]
    - Model-based reasoning [5]
    - Petri-nets [6]
    - State-transition analysis [7, 8]
        - STAT
            - Host-based: USTAT
            - Network-based: NSTAT

- Anomaly detection
    - Statistics [9, 10, 11]
        - Simple model
        - Complex model

          Haystack, DIDS, Emerald, NSM, Secure Net, IDES, NIDES
    - Expert system [12]
    - Neural networks [13]
    - User intention identification [14]
    - Computer immunology [15]

Introduction to state transition analysis

- Limitations of the existing approaches
- Premise of the technique
- State transition diagram
- How the representations applied to the state of an actual computer

USTAT – design of STAT [17]

STAT – applying the state transition analysis to intrusion detection [21]

- STAT design
  - STAT audit record preprocessor
  - STAT knowledge base
  - STAT inference engine
  - STAT decision engine

USTAT

- The audit record preprocessor
- The knowledge base
- Inference engine
- Decision engine
- Functional and performance evaluation

STATL – extensible state-based attack description language [18]
(Developed to support STAT)

Weakness/limitations

- Functional
- Performance

Suggestions of improvement

- A STAT knowledge acquisition subsystem
- STAT Decision engine
- Network audit support

Introduction to statistical analysis

- Simple Model
  - Detection objectives
  - Limitations of the simple model
    - Effectiveness
      - Imperfect information
      - Incomplete information
- Introduction of complex model

NIDES – Next-generation Intrusion Detection System [22]

- Overview of NIDES
- Overview of statistical component

NIDES: statistical component [24, 25]

- The NIDES score value
- Algorithm for computing S from Q
- Frequency distribution for Q
- Computing Q

Performance evaluation

- Concept experiment
- Verification experiment
- Refinement Experiment
  - False-positive result
  - True-positive result
- Cross-profiling
- Group-profiling

Discussion

Weakness/limitations of state-transition analysis and statistical analysis

Suggestions of improvement

Conclusion

Project milestone and schedule

Overall schedule

Schedule	Progress
2003	
Oct	Project homepage
Nov	Finalized project plan
Dec – Jan	Principles and characteristics of statistical analysis and the statistical component of NIDES
	Evaluation of statistical component of NIDES and the statistical analysis
12th – 16th Jan	First presentation
19th Jan	Detailed intermediate project report
2004	
Jan -Feb	Principles and characteristics of state-transition analysis and USTAT
	Evaluation of USTAT and state-transition analysis
Mar - Apr	Suggestions for improvement
13th Apr	Detailed project report
15th Apr	Project exhibition
19-24th Apr	Final presentation

References

[1] T.Lunt, R. Jagannathan, A prototype real-time intrusion detection expert system, Proc. Symp. On Security and Privacy, Oakland, CA, April 1988, pp. 59-66

[2] Giovanni Vigna, Fredrik Valeur, Richard A. Kemmerer, Designing and implementing a family of intrusion detection systems, Proceedings of the 9th European software engineering conference held jointly with 10th ACM SIGSOFT international symposium on Foundations of software engineering**,** Vol. 28, 5, 2003

[3] M.Roesch.Snort – Lightweight Intrusion Detection for Networks. In Proceedings of the USENIS LISA '99 Conference, Nov. 99

[4] Sandeep Kumar. Classification and Detection of Computer Intrusions. Ph.D. Dissertation, August 1995

[5] T D Garvey and Teresa Lunt. Model based intrusion detection. In Proceedings of the 14th National Computer Security Conference, pages 372-385, October 1991

[6] S. Kumar, E.Spafford, A pattern matching model for misuse intrusion detection, Proc. 17th National Computer Security Conf. October 1994, pp. 11-21

[7] P. Porras, R. Kemmerer, Penetration state transition analysis – a rule-based intrusion detection approach, Proc. 8th Annual Computer Security Applications Conf., November 1992, pp. 220-229

[8] Koral Ilgun, Richard A. Kemmerer, Fellow, IEEE, and Phillip A. Porras, "State Transition Analysis: A Rule-Based Intrusion Detection Approach", *IEEE Transactions of software engineering, Vol. 21, no. 3, march 1995*

[9] Paul Helman and Gunar Liepins, "Statistical Foundations of Audit Trail Analysis for the Detection of Computer Misuse", *IEEE transaction of software engineering, vol. 19, no. 9, September 1993*

[10] P.Helman, G.Lipins, W. Richards, Foundations of intrusion detection, Proc. 5th Computer Security Foundations Workshop Franconic, NH, June 1992, pp. 114-120

[11] *Detecting Unusual Program behavior using the statistical component of the Next-generation Intrusion Detection Expert System (NIDES),* D. Anderson, Teresa F. Lunt, Harold Javitz, Ann Tamaru, Alfonso Valdes, Computer Science Laboratory, SRI-CSL-95-06, May 1995

[12] H.S. Vaccaro, G.E. Leipins, Detection of anomalous computer session activity, Proc. IEEE Symp. On Research in Security and Privacy, 1989, pp.280-289

[13] H. Debar, M. Becker, D.Siboni, A neural network component for an intrusion detection system, Proc. 1992 IEEE Computer Society Symp. On Research in Security and Privacy Oakland, CA, May 1992, pp.240-250

[14] T.Spyrou, J.Darzentas, Intention modeling: approximating computer user intentions for detection and prediction of intrusions, in: S.K. Katsikas, D. Gritzalis (Eds.), Information Systems Security, Samos, Greece, May 1996, pp.319-335

[15] S. Forrest, S.A. Hofmeyr, A. Somayaji, Computer immunology, Communications of the ACM 40 (10) (October 1997) 88-96

[16] N.J. McAuliffe et al., "Is your computer being misused? A survey of current intrusion detection system technology," in *Proc. Sixth Comput. Security Applicat. Conf.,* Dec 1990, pp. 260-272

[17] *USTAT: A Real-Time Intrusion Detection System for UNIX*. SRI Technical report, 1993

[18] *STATL definition*: Technical report, 2000-19. University of California, Santa Barbara (UCSB)

[19] *Research in intrusion detection systems: A Survey*. Department of computer engineering, Chalmers University of Technology, Aug 19, 1999

[20] Herve Debar, Marc Dacier, Andreas Wespi: Towards a taxonomy of intrusion-detection systems, Computer Networks 31 (1999) 805-822

[21] Phillip Andrew Porras, STAT: A State Transition Analysis Tool for Intrusion Detection, master thesis, University of California, Santa Barbara

[22] Software Design, Product Specification, and Version Description Document, Next Generation Intrusion Detection Expert System (NIDES), SRI Technical report 1992

[23] Safeguard Final Report: Detecting Unusual Program Behavior Using the NIDES statistical Component, SRI Final Report, Dec 2, 1993

[24] The NIDES Statistical Component: Description and Justification, SRI report, March, 1993

[25] Detecting Unusual Program behavior using the statistical component of the Next-generation Intrusion Detection Expert System (NIDES), SRI technical report 1995

Web site

The SANS institute: intrusion detection FAQ**.** Version 1.80 - Updated June 12, 2003
www.san.org/resource/idfaq

ACM Digital Library
http://portal.acm.org/dl.cfm

IEEE journals, transactions, magazines and conference proceedings
http://ieeexplore.ieee.org/Xplore/DynWel.jsp

Book

Terry Escamilla. Intrusion detection: network security beyond the firewall

Paul E. Proctor; forword by Dorothy Denning; technical editor, Ira Winkler. Practical intrusion detection handbook

Edward G. Amoroso. Intrusion detection: an introduction to Internet surveillance, correlation, traps, trace back, and response