The New York Public Library

Interlibrary & Document Services
476 Fifth Avenue, New York, NY 10018
212.592.7200 • copies@nypl.org
http://www.nypl.org/help/research-services/interlibrary-loan

Reference: TN : 497207

To: Christine Wierzba
Bryan Cave LLP

Date: September 2, 2016

As requested, enclosed is a copy of the requested 1 document(s):

IEEE Transactions on Software Engineering, Vol. SE-13, No. 2, February 1987 "Cover (w/ date stamp), publisher information page, and pages 222-232 inclusive of the article " An intrusion - detection model," by D.E. Denning." (Inclusive w/ certification)

Symantec 1032

The New York Public Library

Interlibrary & Document Services
476 Fifth Avenue, South Court Mezzanine, New York, New York 10018
212.592.7200 •fax 212.391.2502• copies@nypl.org
https://www.nypl.org/help/research-services/interlibrary-loan

September 1, 2016

AFFIDAVIT

STATE OF NEW YORK}
ss:
COUNTY OF NEW YORK}

I, Maurice Klapwald, Librarian/Interlibrary & Document Services, The New York Public Library, being duly sworn, depose and say:

That the attached reproductions, as described below, are true copies made from the original in the collection of this library.

IEEE Transactions on Software Engineering, February 1987, Volume SE–13, Number 2. Cover (w/date stamp), publisher information page & pages 222 – 232, inclusive of the article "An intrusion-detection model," by D.E. Denning.

Maurice B. Klapwald
Maurice B. Klapwald
Assistant Manager / Librarian
Interlibrary & Document Services

Subscribed and sworn to before me
This 1st day of September 2016

Alexandra Griffiths
Notary

ALEXANDRA MARIE GRIFFITHS
NOTARY PUBLIC-STATE OF NEW YORK
No. 01GR6169796
Qualified in Kings County
My Commission Expires July 02, 2019

IEEE TRANSACTIONS ON

SOFTWARE ENGINEERING

FEBRUARY 1987 VOLUME SE-13 NUMBER 2 (ISSN 0098-5589)

A PUBLICATION OF THE IEEE COMPUTER SOCIETY

SPECIAL ISSUE ON COMPUTER SECURITY AND PRIVACY

IEEE TRANSACTIONS ON SOFTWARE ENGINEERING is published monthly by The Institute of Electrical and Electronics Engineers, Inc. Responsibility for the contents rests upon the authors and not upon the IEEE, the Society/Council, or its members. **IEEE Headquarters:** 345 East 47 Street, New York, NY 10017-2394. **NY Telephone:** 212-705 + extension: Information -7900; General Manager -7910; Controller -7748; Public Information -7867; Publishing Services -7560; Spectrum -7556; Standards -7960; Technical Activities -7890. **NY Telecopier:** 212-752-4929. **NY Telex:** 236-411 (international messages only). **IEEE Service Center** (for orders, subscriptions, address changes, Educational Activities, Region/Section/Student Services): 445 Hoes Lane, Piscataway, NJ 08854-4150. **NJ Telephone:** 201-981-0060. **IEEE Washington Office** (for U.S. professional activities): 1111 19th Street, NW, Suite 608, Washington, DC 20036. **Washington Telephone:** 202-785-0017. **Price/Publication Information:** Individual copies: IEEE members $10.00 (first copy only), nonmembers $20.00 per copy. (Note: Add $4.00 postage and handling charge to any order from $1.00 to $50.00, including prepaid orders.) Member and nonmember subscription prices available on request. Available in microfiche and microfilm. **Copyright and Reprint Permissions:** Abstracting is permitted with credit to the source. Libraries are permitted to

An Intrusion-Detection Model

DOROTHY E. DENNING

Abstract—**A model of a real-time intrusion-detection expert system capable of detecting break-ins, penetrations, and other forms of computer abuse is described. The model is based on the hypothesis that security violations can be detected by monitoring a system's audit records for abnormal patterns of system usage. The model includes profiles for representing the behavior of subjects with respect to objects in terms of metrics and statistical models, and rules for acquiring knowledge about this behavior from audit records and for detecting anomalous behavior. The model is independent of any particular system, application environment, system vulnerability, or type of intrusion, thereby providing a framework for a general-purpose intrusion-detection expert system.**

Index Terms—**Abnormal behavior, auditing, intrusions, monitoring, profiles, security, statistical measures.**

I. Introduction

THIS paper describes a model for a real-time intrusion-detection expert system that aims to detect a wide range of security violations ranging from attempted break-ins by outsiders to system penetrations and abuses by insiders. The development of a real-time intrusion-detection system is motivated by four factors: 1) most existing systems have security flaws that render them susceptible to intrusions, penetrations, and other forms of abuse; finding and fixing all these deficiencies is not feasible for technical and economic reasons; 2) existing systems with known flaws are not easily replaced by systems that are more secure—mainly because the systems have attractive features that are missing in the more-secure systems, or else they cannot be replaced for economic reasons; 3) developing systems that are absolutely secure is extremely difficult, if not generally impossible; and 4) even the most secure systems are vulnerable to abuses by insiders who misuse their privileges.

The model is based on the hypothesis that exploitation of a system's vulnerabilities involves abnormal use of the system; therefore, security violations could be detected from abnormal patterns of system usage. The following examples illustrate:

- *Attempted break-in:* Someone attempting to break into a system might generate an abnormally high rate of password failures with respect to a single account or the system as a whole.
- *Masquerading or successful break-in:* Someone logging into a system through an unauthorized account and password might have a different login time, location, or connection type from that of the account's legitimate user. In addition, the penetrator's behavior may differ considerably from that of the legitimate user; in particular, he might spend most of his time browsing through directories and executing system status commands, whereas the legitimate user might concentrate on editing or compiling and linking programs. Many break-ins have been discovered by security officers or other users on the system who have noticed the alleged user behaving strangely.
- *Penetration by legitimate user:* A user attempting to penetrate the security mechanisms in the operating system might execute different programs or trigger more protection violations from attempts to access unauthorized files or programs. If his attempt succeeds, he will have access to commands and files not normally permitted to him.
- *Leakage by legitimate user:* A user trying to leak sensitive documents might log into the system at unusual times or route data to remote printers not normally used.
- *Inference by legitimate user:* A user attempting to obtain unauthorized data from a database through aggregation and inference might retrieve more records than usual.
- *Trojan horse:* The behavior of a Trojan horse planted in or substituted for a program may differ from the legitimate program in terms of its CPU time or I/O activity.
- *Virus:* A virus planted in a system might cause an increase in the frequency of executable files rewritten, storage used by executable files, or a particular program being executed as the virus spreads.
- *Denial-of-Service:* An intruder able to monopolize a resource (e.g., network) might have abnormally high activity with respect to the resource, while activity for all other users is abnormally low.

Of course, the above forms of aberrant usage can also be linked with actions unrelated to security. They could be a sign of a user changing work tasks, acquiring new skills, or making typing mistakes; software updates; or changing workload on the system. An important objective of our current research is to determine what activities and statistical measures provide the best discriminating power; that is, have a high rate of detection and a low rate of false alarms.

II. Overview of Model

The model is independent of any particular system, application environment, system vulnerability, or type of intrusion, thereby providing a framework for a general-pur-

Manuscript received December 20, 1985; revised August 1, 1986. This work was supported by the Space and Naval Warfare Command (SPAWAR) under Contract 83F830100 and by the National Science Foundation under Grant MCS-8313650.

The author is with SRI International, Menlo Park, CA 94025.

IEEE Log Number 8611562.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.