

Distributed Intrusion Detection

Konstantine Koukouchkine

Motivation

- Increasing use of distributed computer resources creates difficulties for intrusion detection
 - Reduced control over network components.
 - Attacks now concentrating on networks, attacks on individual computers barely detectable.
 - Too much data for a single IDS to analyze.

Paper overview

Snapp et al "DIDS (Distributed Intrusion Detection System) -- Motivation, Architecture, and an Early Prototype"

DIDS - Distributed Intrusion Detection System

- Components running at a central location and on hosts and networks that are monitored
- Operates in a heterogeneous environment composed of C2 (Controlled Access Protection) [2] or higher rated computers

Attack scenarios

- Doorknob attack
 - Attempt to find and gain access to insufficiently protected hosts in the system.
 - Very few attack attempts on any individual host, thus not detectable by host-based IDS.
- Network browsing
 - Network user looking through files on several computers within a short period of time

Purpose of DIDS

- Detecting attacks on network that would not be detectable by host-based IDS or NSM.
- Determining the source of attacks detected by host-based IDS.
- Should be at least as effective as host-based IDS and at least as effective as a standalone NSM.

DIDS Architecture

- DIDS director
- A single host monitor for each host.
- A single LAN monitor for each broadcast LAN segment.
- Reports sent independently and asynchronously to the DIDS director

Host monitor

- Host event generator (HEG)
 - Collects and analyzes audit records from the operating system.
 - Scans for *notable events*.
 - Sends notable events to the director.
- Host agent
 - Handles all communications between the host monitor and the DIDS director

Host monitor

- Runs on SunOS 4.0.x with the Sun C2 security package.
- Notable events always passed to the director
- Other events analyzed locally and only summary reports sent to the director.
- Converts audit records into set of abstract *events*, most parts of HEG are thus OS-independent.

Events

- Data from audit records.
- Action
 - session_start, session_end, read, write, execute, terminate, create, delete, move, change_rights, change_user_id
- Domain
 - tagged, authentication, audit, network, system, sys_info, user_info, utility, owned, not_owned

Events

- Each event may succeed or fail.
- All possible transactions fall into a finite number of possible events.
- Abstraction allows to analyze events with an expert system.

LAN monitor

- LAN event generator (LEG)
 - Observes all traffic on it's LAN segment.
 - Monitors host-to-host connections, services used and the volume of traffic.
 - Reports on interesting network activity and change of network traffic patterns.
 - Currently a subset of UC Davis' NSM [4].
- LAN agent, handles communications.

DIDS director

- Located on a dedicated workstation.
- Communications manager
 - Handles all communications and sends notable events to the expert system.
- Expert system
 - Evaluates and reports on the security state of the system. Rule-based with learning capability.
- User interface

Expert system

- Rule-based expert system (in Prolog).
- Uses a hierarchical Intrusion Detection Model
- Uses a fixed set of rules, with a dynamic *Rule Value* (RV) assigned to each rule.
- Receives feedback from SSO on every alert.
- Adjusts RVs based on feedback.

Intrusion Detection Model

6. Security State Overall network security level.
5. Threat Categories of abuse.
4. Context Event placed in context.
3. Subject Definition of network user.
2. Event OS independent representation.
1. Data Audit or OS provided data.

Network-user identification (NID)

- Ability to track users and objects as they move across the network.
- In DIDS, a login from an external device causes a creation of a new, unique NID.
- The NID is applied to every subsequent action by that user, including remote logins.
- The NID is also applied to every new login using the affected user account.

Results

- Demonstrated the viability of the DIDS distributed architecture.
- Success in identification of network users.

Future plans for DIDS

- Further refinement of existing and development of new rules.
- Porting of the expert system from Prolog to CLIPS
- Specialized host monitors for file servers, Gateways etc.
- Extension of the model to a hierarchical Wide Area Network environment

Other related works

- IDES: a real-time intrusion-detection expert system developed by SRI Intl. [3]
 - Target system domain
 - Realm interface
 - IDES processor
 - IDES user interface
 - Modular, distributed system

Other related works

- CIDEF - Common Intrusion Detection Framework [6] - an effort to develop industry standards that allow:
 - different IDS to inter-operate and share information as richly as possible
 - components of IDS to be easily reused in different contexts

CIDF data objects

- Generalized Intrusion Detection Objects (gidos) encode
 - facts about events
 - conclusions about events
 - instructions to carry out actions

CIDF components

- Event generators (E-boxes)
 - Observe their domains and produce gidos
- Event analyzers (A-boxes)
 - Analyze gidos to their significance, produce further gidos.
- Event databases (D-boxes)
 - Store gidos for later retrieval
- Response units (R-boxes)

CIDF communication layers

- gido layer
 - Ensures compatible data format and semantics between different IDS
- Message layer
 - Ensures reliable communications (encryption, ability to pass firewalls etc)
- Transport layer
 - Transport mechanism, not specific to CIDF

Conclusions

- Distributed intrusion detection has many advantages over host- and LAN-based IDS.
- The need for DID will grow as the complexity and thus vulnerability of computer networks increase.
- An open industry standard will facilitate the development and acceptance of distributed intrusion detection systems.

References

- [1] Snapp, S. et al.: DIDS – Motivation, Architecture and an Early Prototype, Proc. 14th National Conference on Computer Security, 1991
- [2] Department of Defense, Trusted Computer System Evaluation Criteria, National Computer Security Center, DOD 5200.28-STD, Dec. 1985.
- [3] T.F. Lunt, A. Tamaru, F. Gilham et al, „A REAL-TIME INTRUSION-DETECTION EXPERT SYSTEM (IDES), Final Technical Report, Project 6784, SRI International 1990
- [4] L.T. Heberlein, G. Dias, K. Levitt, B. Mukherjee, J. Wood, and D. Wolber, „A Network Security Monitor“, Proc. 1990 Symposium on Research in Security and Privacy, pp. 296-304, Oakland, CA, May 1990.
- [5] M. Huang, T. Wicks: „A Large-scale Distributed Intrusion Detection framework Based on Attack Strategy Analysis“, RAID'98 proceedings <http://www.zurich.ibm.com/pub/Other/RAID/RAID98.html>
- [6] CIDF WWW page:<http://www.isi.edu/gost/brian/cidf/>: