Intrusion Detection

Adam Ashenfelter
Nicholas J. Tyrrell

What Is Intrusion Detection

- A network burglar alarm
- Passively monitors the system for suspect behavior
- Sources for monitored data
  - Audit trails (logs of user commands)
  - System calls
  - Network traffic

Examples of Suspect Behavior

- System use outside of normal time
- Abnormal frequency of use
- Abnormal volume of data referenced
- Abnormal patterns of reference to programs or data

Some Possible Intrusions

- External Penetrator
  - An attacker who has gained access to a computer of which he is not a legitimate user
- Masquerader
  - An attacker who has gained the gained access to a valid user’s account
- Misfeasor
  - A legitimate user who abuses his privileges to violate system security policies

Types of Intrusion Detection

- Policy based detection
  - Detects using a predefined rule base
- Anomaly detection
  - Collects statistics, generating profiles for normal/abnormal behavior

Policy Based Detection

- Pros
  - Good against known attacks
  - “False alarms” can be kept low
  - Normally less computationally expensive

- Cons
  - Very susceptible to novel or unusual attacks
  - Writing the rules can be very tedious
  - If the rules become known to an attacker, they can be avoided

Anomaly Detection

- Pros
  - Robust against new types of attacks
  - Can learn by example, no need to write rules by hand
- Cons
  - Might give “false alarms” for unusual but valid behavior
  - Computationally expensive; sometimes requiring off-line algorithms
  - Might learn to accept dangerous behavior as normal over time

Some Current and Previous Intrusion Detection Systems

- NIDES
- NADIR
- NSM

NIDES

- Evolved from IDES over the early 1990’s
- Uses both rule based and anomaly detection

NIDES

- Pros
  - Highly Modularized
  - Real or non-real time detection
  - Low false positive rate (false alarms)

- Cons
  - Susceptible to Tampering
    - Direct attack on Nides
  - Reverse Engineering
    - Attacker could avoid rules used by Nides' policy detection

NADIR

- Automated system for detecting network intrusion and misuse
- Developed at Los Alamos National Laboratory
- Served 9000 computers including 6 Cray-class computers
- Uses rules at system wide level and also creates statistical profiles for each user

NADIR Continued

- Pros
  - Highly Interactive
  - Error Detection
  - System Management
  - User Education

- Cons
  - High number of false positives
  - Needs better anomaly detection
  - Not real time detection

NSM

- Prototype deployed at UC Davis during 1980’s
- First System to use Network data directly
- Layered approach to data collection
- Uses both policy and anomaly detection

NSM Continued

- Pros
  - Audit data instantly available
  - Impervious to direct attack
  - Low impact on system resources
- Cons
  - Attacks made on hosts without accessing the network are undetectable
  - Cryptography could be the death of NSM

Some Current Research Areas

- Data Mining
  - Using data mining techniques to better find consistent and useful patterns from logged data to use as rules
- Machine Learning
  - Using machine learning methods, such as neural networks, to try and build better anomaly detection (fewer false alarms)

Biliography

Axelsson, S. (1999) **Research in Intrusion-Detection Systems: A Survey**

Ghosh, A. Schwartzbard, A., Schatz, M. **Learning Program Behavior Profiles for Intrusion Dection**

Ryan, J., Lin, M., Miikkulainen, R. (1998) **Intrusion Detection with Neural Networks** In *Advances in Neural Information Processing Systems 10*

Lane, T., Brodley, C (1997). **An Application of Machine Learning to Anomaly Detection**

Lee, W., Stolfo, S. **Data Mining Approaches for Intrusion Detection**