ArgusNet: An Architecture for Collecting Attack Data

Susmit Panjwani (ENTS), Michel Cukier (ME, ISR, CS)

Objective

To develop a solution to analyze attacks
- Design an architecture to collect attacks transparent to attackers
- Restrict attackers to exploit only the target machines
- Analyze the collected data in order to understand the threat of attacks

Functional Components

- Access Control: Restricts attackers to IsoNet
  - Reverse firewall: limits number of outgoing connections
  - Network Intrusion Prevention System: drops outgoing connections based on attack signature
- Data Collection: Collects real time data at network, host and application level
- Event Logging: Collects and stores system, application and security logs
- Event Alerting: Alerts the administrator about any attacker activity and system failure
- Network Management: Monitors the state of all the machines in network
  - Collects network statistics

Architecture

- ArgusEyes: Monitoring Network:
  - Reverse firewall
  - Intrusion detection system
  - Syslog server
  - Data collection server
  - Network management system
- IsoNet: Isolated Target Network:
  - Modified OS kernel
  - Data collection tools
  - Monitored applications
  - Simulated users
  - Simulated application traffic
- Router: Separates ArgusEyes from IsoNet

Validation

Phase 1:
- Develop profile of user and application traffic
- Simulate network traffic without launching attacks

Phase 2:
- Build a database of attacks
- Launch attacks without simulated background traffic

Phase 3:
- Launch attacks with simulated background traffic
  - Analyze the results to tune parameters of access control and data collection modules