Hydra: Agents for Information Security

A Systems Approach to Security

Jim Ross
Morris Brill
Introduction

- Hydra integrates intrusion detection system (IDS), scanning, and vulnerability assessment tools within an agent framework
- Intelligent agent and AI techniques used to collect, detect, evaluate, and respond to events
- All tools are open source
- New tools can be integrated into the agent framework
Hydra Architecture is Distributed and Extensible

- Agents act as wrappers for IDS tools
- Agents collect, format and forward data to host agent
- IDS data is evaluated for significant events using AI methods
- Agents respond intelligently by starting defensive or offensive agents
- ZEUS provides the infrastructure
- Each agent makes decisions about its environment and tasks
Hydra Integrates Publicly Available Tools

- **ZEUS**: Infrastructure to build intelligent agent systems
- **CLIPS (C Language Integrated Production System)**: A productive development and delivery expert system shell
- **FIPA (Foundation for Intelligent Physical Agents)**: Communication protocol that binds Hydra agents
  - FIPA is a group of standards specifying the communications and other protocols for intelligent agents
- Open source scanners and other tools: portsentry, clog, nmap, logcheck, snort, etc.
Hydra Evaluates Data
Fused from Independent Agents

- Each agent contributes its piece of the total picture
- The information is evaluated by host agents
- The follow information is evaluated:
  - The age of the data
  - The type of agent
  - The dependability of the data
  - Criticality (or importance) of the data
  - The number of other agents reporting similar data
  - The number of other agents reporting conflicting data
Example Scenario: IDS

- Host with Agent
- Host
- Router
- Firewall
- Bad Guy
- Data Collection and Decision Agent
- Data
- Control and Coordination
- Offensive Actions
- Defensive Actions
- Scan or Attack
- Host with Agent
Distributed Intrusion Detection Increases Probability of Detection

- Different computer architectures (e.g., operating systems) detect different attacks
- Distributed IDS uses open source and existing tools (e.g. snort, portsentry, ISS)
- Agents intelligently coordinate intrusion reports
  - Improves performance during coordinated attacks
  - Evaluates data using attack signatures from multiple systems
Hydra: Benefits of the System Approach

- Integrates standalone capabilities into a coordinated end-to-end security system
  - Collect, detect, evaluate, respond
- Uses all open source tools to reduce life cycle costs
- Incorporates IDS, scanning, and evaluation tools used on a daily basis by typical security operations centers
  - Not a prototype or superficial construct
  - Not reinventing the wheel
- Java cross platform capability integrates tools running on their native platform
- True intelligent agents
Further Information

- Jim Ross: Jim.Ross@trw.com
- Morris Brill: morris.brill@trw.com