Autonomous Anti-DDOS Network V2.0 (A2D2-2)
IDIP enhanced DDOS

Sarah Jelinek
University Of Colorado, Colorado Springs
sarah.jelinek@sun.com
This project will deliver the following components:

- Partial implementation of the Intrusion Detection and Isolation Protocol Message Layer Protocol Definition [NB02-2]:
  - IDIP Neighborhood Management
  - Reliable Delivery of IDIP Messages
  - All Message formatting
  - Hello Protocol
  - Protocol Initialization
  - Message Forwarding
  - Socket communication
Partial implementation of the Intrusion Detection and Isolation Protocol Application Layer Protocol Definition[NB02-1]:

- Modify Snort to become an IDIP Application:
- Add IDIP Trace capability to Snort IDIP Application
- Add IDIP Notify capability to Snort IDIP Application
- Add IDIP Requested Action capability to the Snort IDIP Application (this feature lets other IDIP nodes in the neighborhood know what the suggested response is)
- Add new Snort Alert to accept and handle IDIP Requested Action messages
A project write-up that will detail the following:

- A2D2-2 system architecture
- Results comparing an A2D2 enabled and an A2D2-2 enabled DDoS attack response
- Comparison of IDIP and other intrusion detection/tracking and response protocols
- Future work that can be done with A2D2-2
Status of project deliverables

- Code is complete
  - Will put code in public directory
- Preliminary testing done using Solaris
  - Using testbed setup in office to flush out major bugs in code
  - No real data available yet
  - Hope to have substantial data within two weeks
- Started project report
- Completed research except for a few new things
  Dr. Chow has asked me to look at :-)
What I Have Learned

- Key IDIP Principles:
  - An IDIP system must be able to respond to detected intrusions in real-time
    - This can be difficult depending on amount of trace messages
    - Need reasonably sophisticated knowledge engine to determine best responses based on trace data
    - Possible to use JESS, (Java Rule Engine)
    - Possible AI application
  - An IDIP system must support environments that span multiple administrative domains
  - An IDIP system must have minimal impact on system performance
  - An IDIP system must be capable of operating while the system is under attack
  - The IDIP system components should be capable of responding autonomously to the attack based on the IDIP message
IDIP vs. IDMEF

- Intrusion Detection Message Exchange Format (IDMEF)
  - Defines data formats and exchange procedures for sharing data from IDS systems, to other IDS systems and to the management systems interacting with them.
  - Two open source libraries available today, libidmef and a Java IDMEF set of classes.
- Both IDMEF and IDIP enable interoperability among open source, commercial and research IDS systems.
- IDMEF is XML based schema, makes it highly interoperable, IDIP uses a message protocol.
- IDIP requires additional software infrastructure to IDS nodes. IDMEF only requires use of a library/java class to generate appropriate message.
Both IDIP and IDMEF require a knowledgeable party to help correlate data.
IDMEF has some correlation protocol definitions.
IDIP relies on trace message data to determine appropriate responses.
IDMEF is an open, fully available protocol.
IDIP documentation is not fully available, and is currently implemented by proprietary companies. The IDIP Key distribution and Cryptographic extension protocols are not available at this time.
IDIP and CISL
- CISL is IDIP information specification language
- It is used in IDIP to communicate trace and report information
- CISL uses an S-expression syntax to form sentences describing events and responses

Using IDIP and IDMEF together
- CISL seems a bit cumbersome
- Using IDMEF(XML) to transfer data in a compatible way may be better and more lightweight
What I Have Learned, cont.

- **IDIP and CIDF**
  - Common Intrusion Detection Framework (CIDF)
  - Effort to develop protocols and application programming interfaces so that IDS research projects can share information and resources to enable sharing of IDS components
  - Utilizes CISL for data format
  - CIDF's primary goal is to represent intrusion detection data in a Global Intrusion Detection Object (GIDO) format
  - Last substantial work done for CIDF in 1999
  - CIDF is intended for use in conjunction with IDIP
What I Have Learned, cont.

- IDIP vs. IDXP
  - Intrusion Detection Exchange Protocol (IDXP)
  - Protocol for exchanging data between IDS entities
  - Supports mutual authentication, integrity and confidentiality over a connection-oriented protocol
  - Specified as a Blocks Extensible Exchange Protocol (BEEP)
  - Provides for the exchange of IDMEF messages, unstructured text and binary data between IDS systems
  - IDXP is an open, published standard
  - IDIP protocol spec is only partially available
  - Both allow for proxy or intermediate nodes to pass along data
  - Both provide for a security protocol, however the IDIP spec is not available at this time
Intrusion Detection Exchange Architecture

- Open source project, sourceforge.net
- Allows interpretation of data from many disparate types of IDS systems
- Provides a unified view of this data translated into network activity
- Uses XML as data transfer/correlation protocol
- Not standards based
- Java implementation

Might be interesting to look more closely at this for possible enhancements
Future Work Suggested

- IDIP Redundant/Cooperative Discovery Coordinators
- Discovery Coordinator and Application layer response enhancements
- More updates to SNORT for DDoS pushback
- Security protocol implementation
- More Application protocol implementation
- OpenSLP proxy server work
- Look at IDMEF and IDXP for possible inclusion with IDIP
References

  http://zen.ece.ohiou.edu/~inbounds/DOCS/reldocs/IDIP_Architecture.doc
  http://zen.ece.ohiou.edu/~inbounds/DOCS/reldocs/IDIP_Application_Layer.doc
  http://zen.ece.ohiou.edu/~inbounds/DOCS/reldocs/IDIP_Message_Layer.doc
- [T02] Tanase, Matt. 2002. Barbarians at the Gate: An Introduction to Distributed Denial of Service Attacks
  http://www.securityfocus.com/infocus/1647
  http://www.isi.edu/gost/cidf/
  http://www.openslp.org/
  http://www.sans.org/rr/firewall/prevention.php
References

- [CIDF] Common Intrusion Detection Framework and Specification Language
- [IDMEF] Intrusion Detection Message Exchange Format
- [IDXP] Intrusion Detection Exchange Protocol