

Analyzing Rule Based, and Adaptive Case Based Reasoning Architectures for Intruder Detection Systems

Timothy Crofton

REU 2004



Table of contents

- Initial problems
- Snort Overview and results
- Adaptive CBR software from FSU
- Future work

Life After Microsoft



The MIT/LL Database

- Large database with a wide variety of attacks such as U2R, DoS, R2L, Probes.
- Attacks were clearly marked in the training data.
- Large knowledge base of research to reference as needed.
- Often criticized for not mirroring actual traffic closely enough (e.g. lack of 'crud') [1].



Snort 2.2

- Robust open source IDS software that has many helpful plugins available.
- Rule based, with each rule expressing some action to be performed.
- Fairly easy to modify or write new rules.
- Easily the most researched IDS in existence.
- Large support group of users online with several dedicated forums.

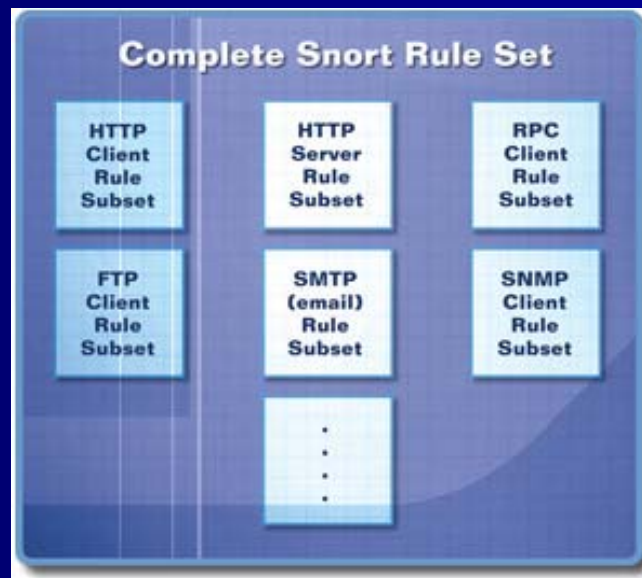
Typical Snort Rule

```
alert tcp any any -> 192.168.1.0/24!111:  
  (content: |"000186a5"|; msg "mountd  
  access")
```

Destination IP range 192.168.1.0 through
192.168.1.255 on a port not greater than 111.

Snort Detection Engine Architecture

The detection engine uses a setwise methodology for analyzing snort rules [2]. There are 4 rule groups, TCP, UDP, ICMP, and IP.



Results so far

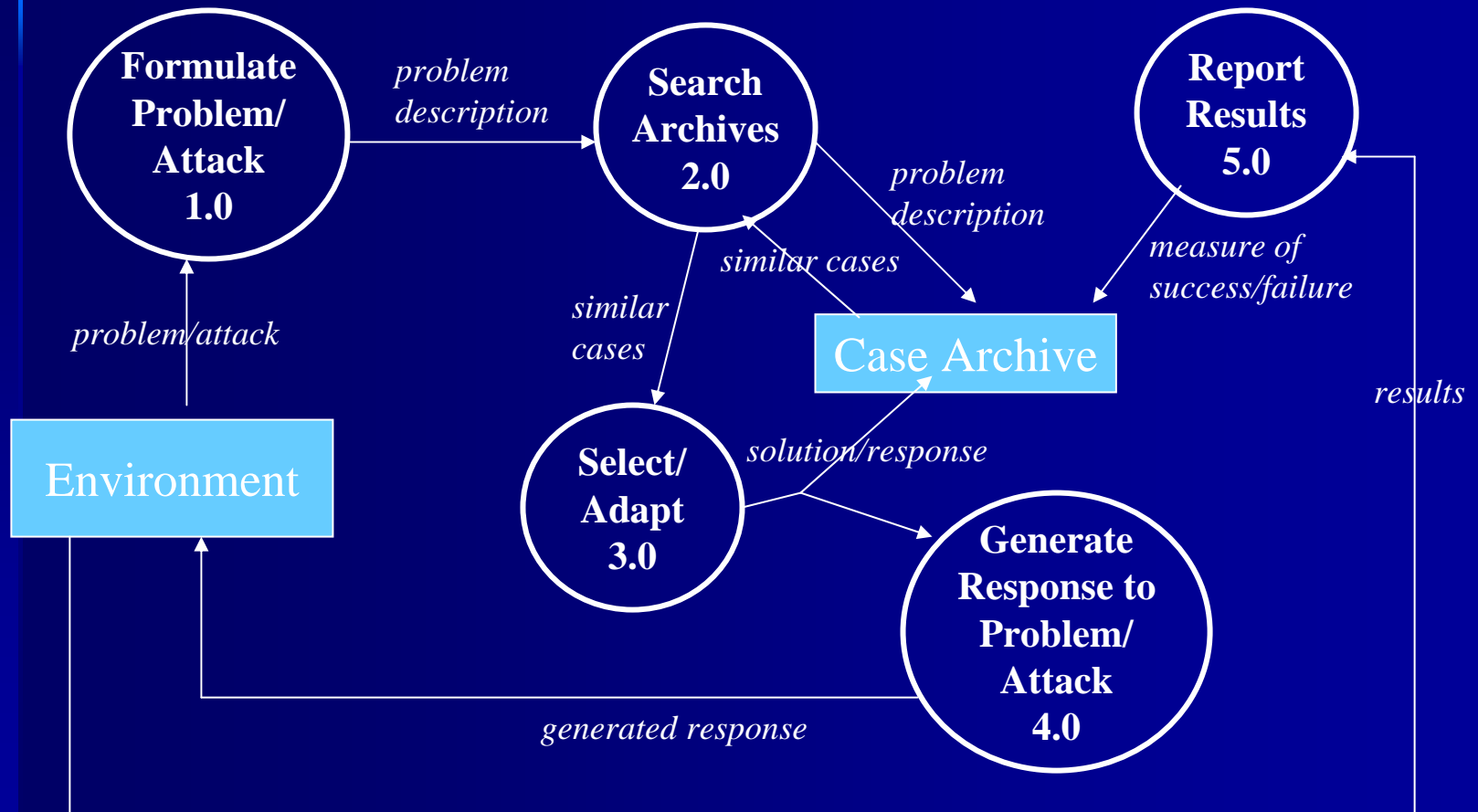
- With the full rule sets, almost 100% of the attacks were detected. However the false positives were almost immeasurable.
- Adjusting the rule sets has helped, but detection dropped below 80% and the false positives are still too high.

Case Based Reasoner

Java based software developed by D.G. Schwartz, S. Stoecklin, and E. Yilmaz at Florida State University.

Seeks to abstract away program specifics thus lending itself to greater portability between implementations[3].

CBR cont.



Snort As A CBR

```
alert tcp any any -> 192.168.1.0/24!111: (content:  
|"000186a5"|; msg "mountd access")
```

- *Protocol:* tcp
 - Source IP address:* any
 - Source port:* any
 - Destination IP address:* 192.168.1.0 to 255
 - Destination port:* not > 111
 - Packet contents:* 000186a5 (hex code)
- Case action: Output alert "mountd access"

Future work...

- Continue tuning Snort's rules until the false positive/alert ratio is acceptable.
- Run the CBR software over the same data sets and compare results.

References

1. M. Mahoney and P. Chan "An analysis of the 1999 DARPA/LL evaluation data for network anomaly detection" 2003
2. J. Beale "Snort 2.1 Intruder Detection" 2nd edition 2004
3. D. Schwartz, S. Stoecklin, E. Yilmaz "A case based approach to network intrusion detection" 2002