

Packet Space Analysis of Intrusion Detection Signatures

Frédéric Massicotte

Communications Research Centre Canada, Ottawa, Ontario K2H 8S2 • E-mail: frederic.massicotte@crc.gc.ca, Tel: 1-613-998-2843

Motivation

- A single packet can trigger more than one IDS signature
 - Different signatures may include/intersect each other
- These problems can be used to design evasion/denial of service attacks
 - IDSs can raise a limited number of events on a single packet (some signatures are not triggered)
 - Dangerous overlap in the signature sets (a specific packet can be used to trigger many signatures at the same time)
- We need to be able to compare two different signatures designed for the same attack
- We need to be able to analyze the IDS signatures for inclusions and intersections

Example in Snort

```

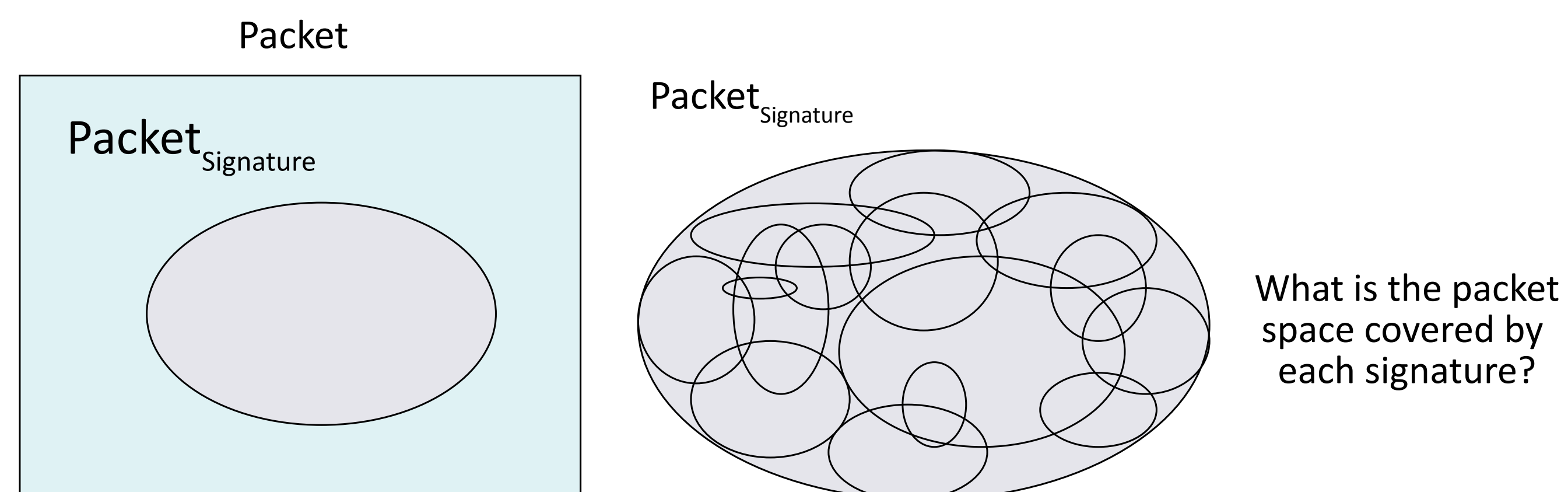
alert tcp $EXTERNAL NET any -> $HOME NET 21 (msg:"FTP CWD ~attempt";
flow:to_server,established;
content:"CWD"; nocase;
pcre:"/^CWD\s+~/smi";
sid:1672; rev:11;)
  
```

```

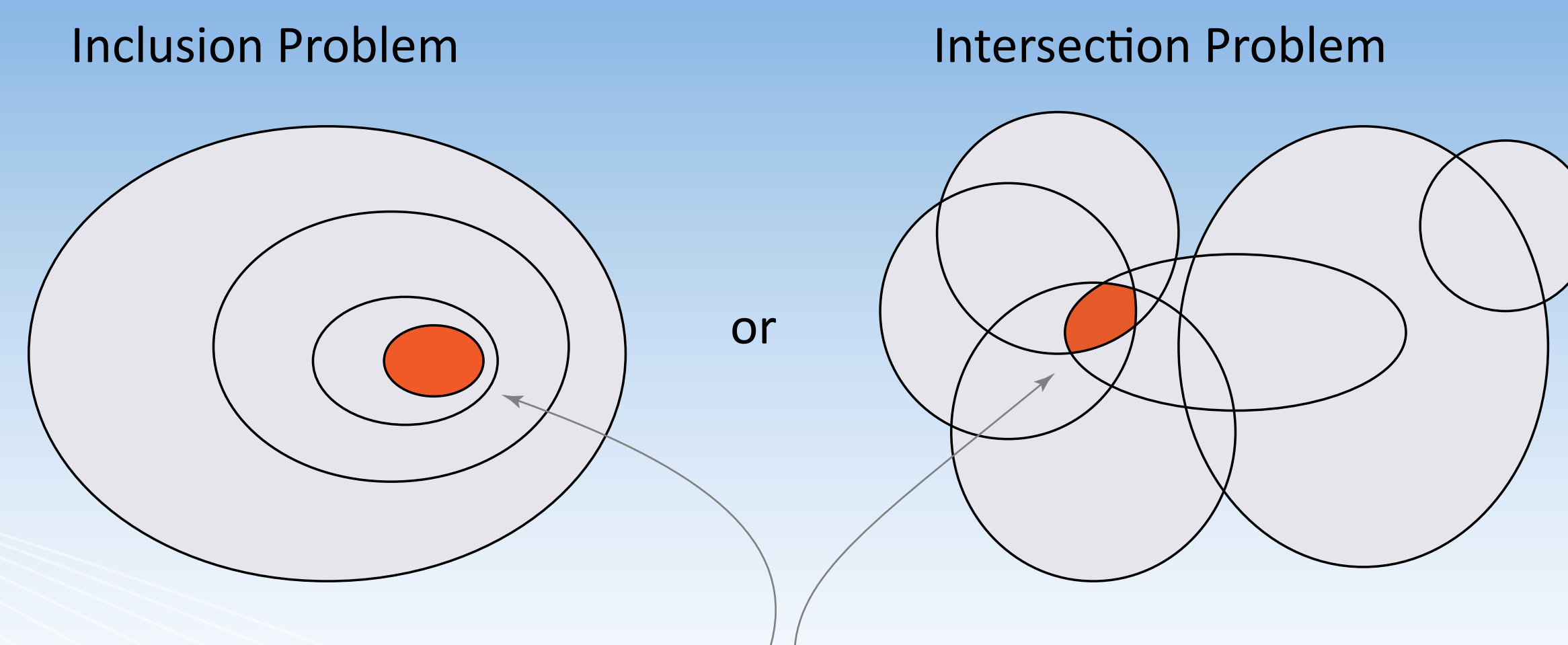
alert tcp $EXTERNAL NET any -> $HOME NET 21 (msg:"FTP CWD ~root attempt";
flow:to_server,established;
content:"CWD"; nocase;
content:"~root"; distance:1; nocase;
pcre:"/^CWD\s+~/smi";
sid:336; rev:10;)
  
```

$S_{336} \subset S_{1672}$?

Packet Space Model



How do we identify these situations?



What about the packets in these packet spaces?
Are we missing IDS events?

Proposed Approach

- Transform each signature into a set of packets (e.g., $S_1 \dots S_i \dots S_n$)
 - Set of ranges
 - Set of finite state automata
- Our Signature Space Analysis approach allows the identification of:
 - Equal signatures (i.e., $S_i = S_j$)
 - Signature inclusions (i.e., $S_i \subset S_j$)
 - Inclusion sequences (i.e., $S_i \cap S_j \dots \subset S_n$)
 - Signature intersections (i.e., $S_i \cap S_j \neq \emptyset$)
 - Intersection sequences (i.e., $S_i \cap S_j \dots \cap S_n \neq \emptyset$)

Current Results

- We analyzed various versions of Snort signature databases (i.e., 12 signature database versions from Snort 1.8.6 to 2.4.5)
 - So far, we only analyzed the inclusion problem
 - We observed similar results across Snort signature database versions.
- Results for Snort 2.4.5
 - Number of equal signature pairs: 3
 - Number of inclusion pairs: 266
 - Number of inclusion sequences of three: 2