Northwestern Lab for Internet and Security Technology

NetShield: Towards High Performance Network-based Vulnerability Signature Matching

Zhichun Li, Gao Xia, Yi Tang, Yan Chen, and Bin Liu
Northwestern University and Tsinghua University (China)

Problems

Currently, the regular expressions used by NIDS for signature matching have low accuracy because fundamentally regex cannot capture the vulnerability condition well. On the other hand, vulnerability signatures are much more accurate, but may have performance problems.

	Regular Expression	Vulnerability
Accuracy	Relative Poor	Much Better
Speed	Good	??
Memory	OK	??
Coverage	Good	??

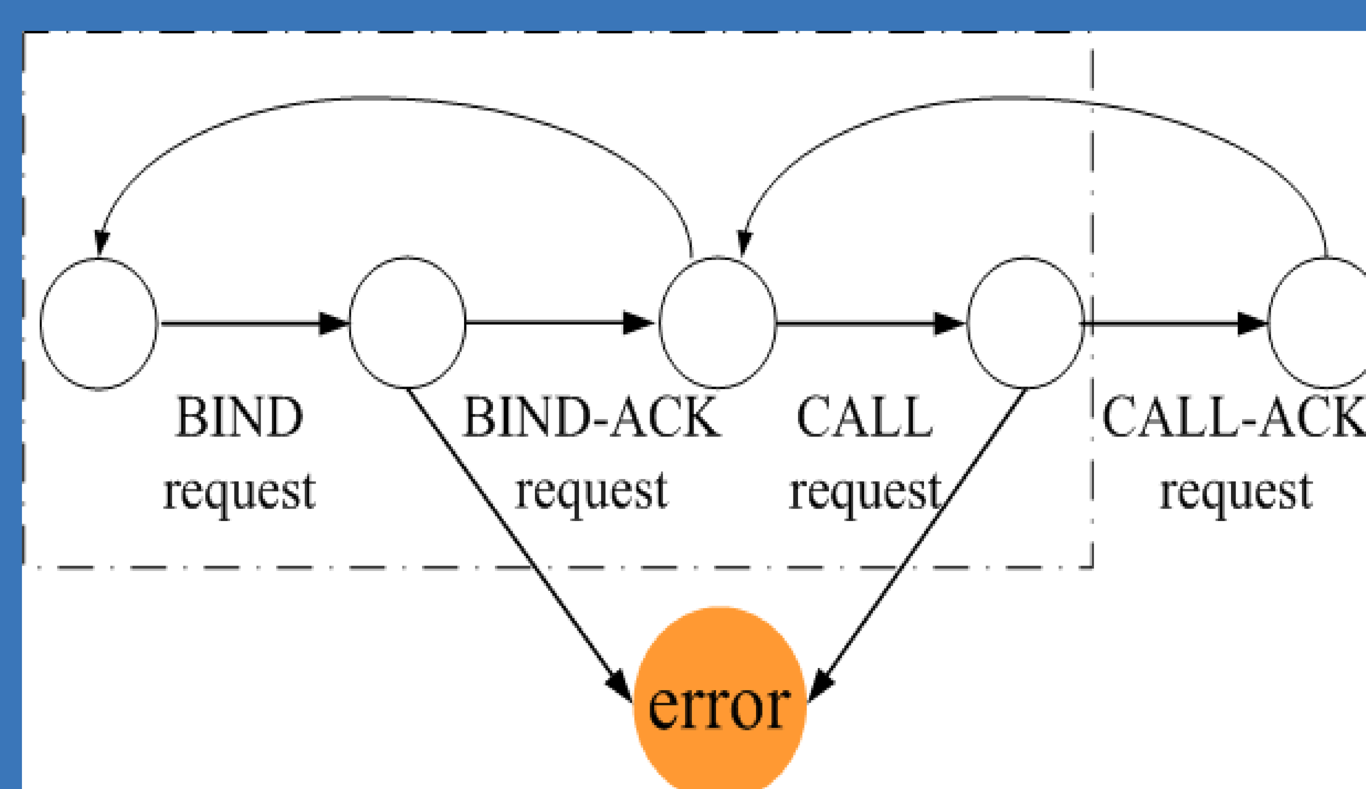
Shield [sigcomm'04]

Focus of this work

Goal: Build a high speed vulnerability signature matching engine!

Our approach

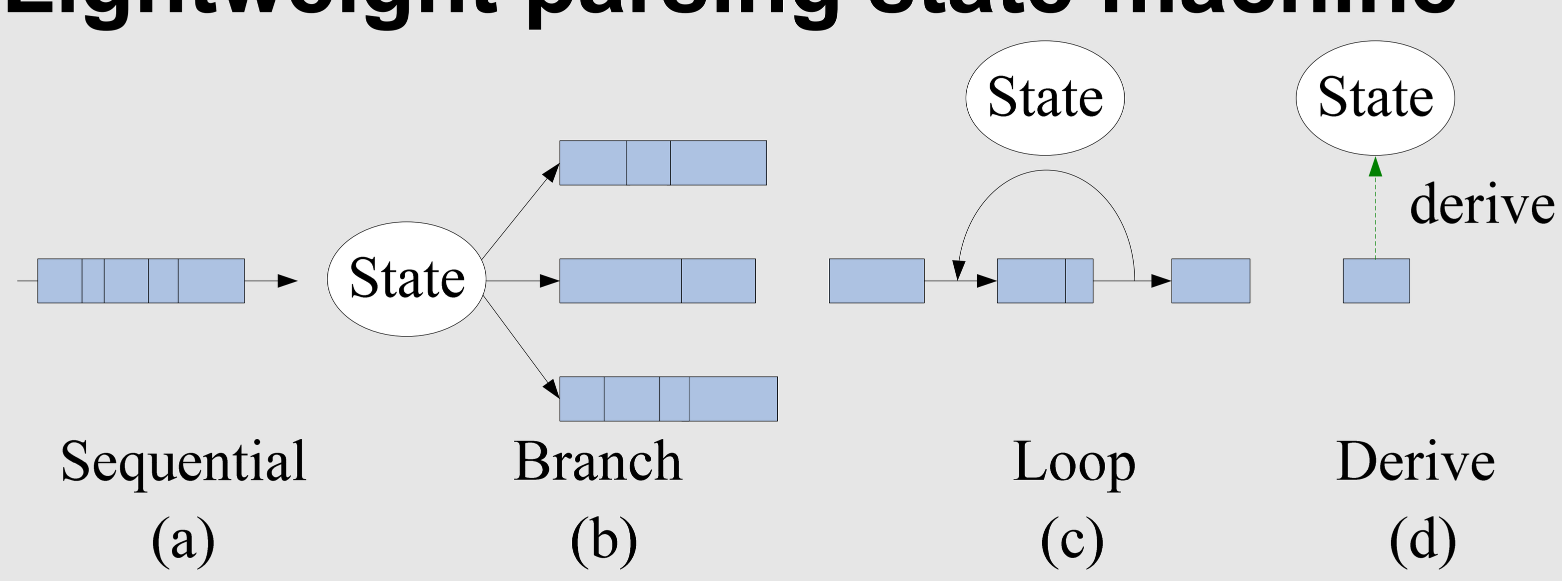
```
BIND:
  rpc_vers==5 && rpc_vers_minor==1
  && packed_drep==\x10\x00\x00\x00
  && context[0].abstract_syntax.uuid
  ==UUID_RemoteActivation
BIND-ACK:
  rpc_vers==5 && rpc_vers_minor==1
CALL:
  rpc_vers==5 && rpc_vers_minor==1
  && packed_drep==\x10\x00\x00\x00
  && stub.RemoteActivationBody.actual_length
  >=40 && matchRE(stub.buffer,/^\x5c\x00\x5c\x00/)
```



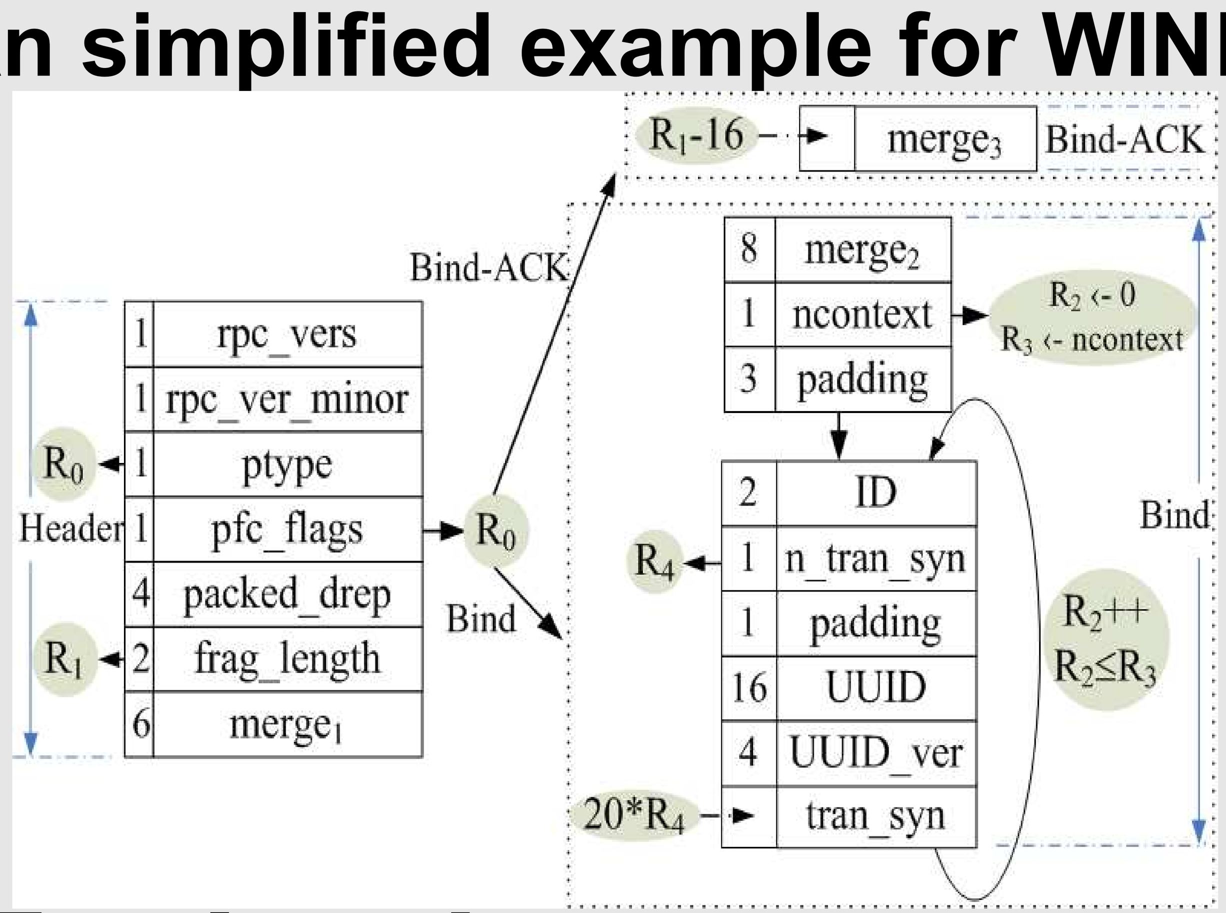
Signature Example

High speed parsing

Lightweight parsing state machine



An simplified example for WINRPC



High speed matching

Problem formulation

- Using a n x k table to keep track of whether signature *i* depend on matching dimension (matcher) *j*
- Matching dimension is a two tuple (field, operator), *e.g.*, (rpc_vers, ==)

Candidate Selection Idea

- Pre-computation decides the rule order and matcher order. Given that usually most matchers are good rule filters, we only keep track of a few matching candidates for one connection. Group
- For each matcher, match rules in parallel.
- Iteratively combine the candidate sets for multiple matchers.

Evaluation

- High speed parsing: 2.9~15 Gbps for different protocols (HTTP, WINRPC, DNS)
- High speed matching: HTTP, 791 vulnerability signatures at ~1Gbps
- Applicability: in Snort ruleset (6,735 signatures) 86.7% can be improved to vulnerability signatures
- Prototype has been deployed on live-network environment and ***faster*** than Snort.