Semantics-Preserving Simplification of Real-World Firewall Rule Sets

Formal Methods 2015

Cornelius Diekmann[*] Lars Hupel[‡] Georg Carle[*]

[*]Chair for Network Architectures and Services [‡]Chair for Logic and Verification
Technische Universität München
Munich, Germany

With contributions by Lars Noschinski[‡], Julius Michaelis[*], Andreas Korsten[*], Manuel Eberl[‡], Lukas Schwaighofer[*], and Fabian Immler[‡].

Introduction to Firewalls

```
Chain INPUT (policy ACCEPT)
target      prot source          destination
DOS_PROTECT all  0.0.0.0/0       0.0.0.0/0
ACCEPT      all  0.0.0.0/0       0.0.0.0/0   state RELATED,ESTABLISHED
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp dpt:22
DROP        tcp  0.0.0.0/0       0.0.0.0/0   multiport dports 21,873,5005,...
DROP        udp  0.0.0.0/0       0.0.0.0/0   multiport dports 123,111,2049,...
ACCEPT      all  192.168.0.0/16  0.0.0.0/0
DROP        all  0.0.0.0/0       0.0.0.0/0

Chain DOS_PROTECT (1 references)
target      prot source          destination
RETURN      icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8 limit: avg 1/sec ...
DROP        icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8
RETURN      tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04 limit: ...
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04
...
```

Introduction to Firewalls

```
Chain INPUT (policy ACCEPT)
target      prot source          destination
DOS_PROTECT all  0.0.0.0/0       0.0.0.0/0
ACCEPT      all  0.0.0.0/0       0.0.0.0/0   state RELATED,ESTABLISHED
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp dpt:22
DROP        tcp  0.0.0.0/0       0.0.0.0/0   multiport dports 21,873,5005,...
DROP        udp  0.0.0.0/0       0.0.0.0/0   multiport dports 123,111,2049,...
ACCEPT      all  192.168.0.0/16  0.0.0.0/0
DROP        all  0.0.0.0/0       0.0.0.0/0

Chain DOS_PROTECT (1 references)
target      prot source          destination
RETURN      icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8 limit: avg 1/sec ...
DROP        icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8
RETURN      tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04 limit: ...
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04
...
```

Introduction to Firewalls

```
Chain INPUT (policy ACCEPT)
target      prot source          destination
DOS_PROTECT all  0.0.0.0/0       0.0.0.0/0
ACCEPT      all  0.0.0.0/0       0.0.0.0/0   state RELATED,ESTABLISHED
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp dpt:22
DROP        tcp  0.0.0.0/0       0.0.0.0/0   multiport dports 21,873,5005,...
DROP        udp  0.0.0.0/0       0.0.0.0/0   multiport dports 123,111,2049,...
ACCEPT      all  192.168.0.0/16  0.0.0.0/0
DROP        all  0.0.0.0/0       0.0.0.0/0

Chain DOS_PROTECT (1 references)
target      prot source          destination
RETURN      icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8 limit: avg 1/sec ...
DROP        icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8
RETURN      tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04 limit: ...
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04
...
```

Introduction to Firewalls

```
Chain INPUT (policy ACCEPT)
target      prot source          destination
DOS_PROTECT all  0.0.0.0/0       0.0.0.0/0
ACCEPT      all  0.0.0.0/0       0.0.0.0/0   state RELATED,ESTABLISHED
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp dpt:22
DROP        tcp  0.0.0.0/0       0.0.0.0/0   multiport dports 21,873,5005,...
DROP        udp  0.0.0.0/0       0.0.0.0/0   multiport dports 123,111,2049,...
ACCEPT      all  192.168.0.0/16  0.0.0.0/0
DROP        all  0.0.0.0/0       0.0.0.0/0

Chain DOS_PROTECT (1 references)
target      prot source          destination
RETURN      icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8 limit: avg 1/sec ...
DROP        icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8
RETURN      tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04 limit: ...
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04
...
```

Introduction to Firewalls

```
Chain INPUT (policy ACCEPT)
target      prot source          destination
DOS_PROTECT all  0.0.0.0/0       0.0.0.0/0
ACCEPT      all  0.0.0.0/0       0.0.0.0/0   state RELATED,ESTABLISHED
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp dpt:22
DROP        tcp  0.0.0.0/0       0.0.0.0/0   multiport dports 21,873,5005,...
DROP        udp  0.0.0.0/0       0.0.0.0/0   multiport dports 123,111,2049,...
ACCEPT      all  192.168.0.0/16  0.0.0.0/0
DROP        all  0.0.0.0/0       0.0.0.0/0

Chain DOS_PROTECT (1 references)
target      prot source          destination
RETURN      icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8 limit: avg 1/sec ...
DROP        icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8
RETURN      tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04 limit: ...
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04
...
```

Introduction to Firewalls

```
Chain INPUT (policy ACCEPT)
target      prot source          destination
DOS_PROTECT all  0.0.0.0/0       0.0.0.0/0
ACCEPT      all  0.0.0.0/0       0.0.0.0/0   state RELATED,ESTABLISHED
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp dpt:22
DROP        tcp  0.0.0.0/0       0.0.0.0/0   multiport dports 21,873,5005,...
DROP        udp  0.0.0.0/0       0.0.0.0/0   multiport dports 123,111,2049,...
ACCEPT      all  192.168.0.0/16  0.0.0.0/0
DROP        all  0.0.0.0/0       0.0.0.0/0

Chain DOS_PROTECT (1 references)
target      prot source          destination
RETURN      icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8 limit: avg 1/sec ...
DROP        icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8
RETURN      tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04 limit: ...
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04
...
```

Introduction to Firewalls

```
Chain INPUT (policy ACCEPT)
target      prot source          destination
DOS_PROTECT all  0.0.0.0/0       0.0.0.0/0
ACCEPT      all  0.0.0.0/0       0.0.0.0/0   state RELATED,ESTABLISHED
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp dpt:22
DROP        tcp  0.0.0.0/0       0.0.0.0/0   multiport dports 21,873,5005,...
DROP        udp  0.0.0.0/0       0.0.0.0/0   multiport dports 123,111,2049,...
ACCEPT      all  192.168.0.0/16  0.0.0.0/0
DROP        all  0.0.0.0/0       0.0.0.0/0

Chain DOS_PROTECT (1 references)
target      prot source          destination
RETURN      icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8 limit: avg 1/sec ...
DROP        icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8
RETURN      tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04 limit: ...
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04
...
```

Introduction to Firewalls

```
Chain INPUT (policy ACCEPT)
target      prot source          destination
DOS_PROTECT all  0.0.0.0/0       0.0.0.0/0
ACCEPT      all  0.0.0.0/0       0.0.0.0/0   state RELATED,ESTABLISHED
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp dpt:22
DROP        tcp  0.0.0.0/0       0.0.0.0/0   multiport dports 21,873,5005,...
DROP        udp  0.0.0.0/0       0.0.0.0/0   multiport dports 123,111,2049,...
ACCEPT      all  192.168.0.0/16  0.0.0.0/0
DROP        all  0.0.0.0/0       0.0.0.0/0

Chain DOS_PROTECT (1 references)
target      prot source          destination
RETURN      icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8 limit: avg 1/sec ...
DROP        icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8
RETURN      tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04 limit: ...
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04
...
```

Introduction to Firewalls

```
Chain INPUT (policy ACCEPT)
target      prot source          destination
DOS_PROTECT all  0.0.0.0/0       0.0.0.0/0
ACCEPT      all  0.0.0.0/0       0.0.0.0/0   state RELATED,ESTABLISHED
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp dpt:22
DROP        tcp  0.0.0.0/0       0.0.0.0/0   multiport dports 21,873,5005,...
DROP        udp  0.0.0.0/0       0.0.0.0/0   multiport dports 123,111,2049,...
ACCEPT      all  192.168.0.0/16  0.0.0.0/0
DROP        all  0.0.0.0/0       0.0.0.0/0

Chain DOS_PROTECT (1 references)
target      prot source          destination
RETURN      icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8 limit: avg 1/sec ...
DROP        icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8
RETURN      tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04 limit: ...
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04
...
```

Introduction to Firewalls

```
Chain INPUT (policy ACCEPT)
target      prot source          destination
DOS_PROTECT all  0.0.0.0/0       0.0.0.0/0
ACCEPT      all  0.0.0.0/0       0.0.0.0/0    state RELATED,ESTABLISHED
DROP        tcp  0.0.0.0/0       0.0.0.0/0    tcp dpt:22
DROP        tcp  0.0.0.0/0       0.0.0.0/0    multiport dports 21,873,5005,...
DROP        udp  0.0.0.0/0       0.0.0.0/0    multiport dports 123,111,2049,...
ACCEPT      all  192.168.0.0/16  0.0.0.0/0
DROP        all  0.0.0.0/0       0.0.0.0/0

Chain DOS_PROTECT (1 references)
target      prot source          destination
RETURN      icmp 0.0.0.0/0       0.0.0.0/0    icmptype 8 limit: avg 1/sec ...
DROP        icmp 0.0.0.0/0       0.0.0.0/0    icmptype 8
RETURN      tcp  0.0.0.0/0       0.0.0.0/0    tcp flags:0x17/0x04 limit: ...
DROP        tcp  0.0.0.0/0       0.0.0.0/0    tcp flags:0x17/0x04
...
```

Introduction to Firewalls

```
Chain INPUT (policy ACCEPT)
target      prot source          destination
DOS_PROTECT all  0.0.0.0/0       0.0.0.0/0
ACCEPT      all  0.0.0.0/0       0.0.0.0/0   state RELATED,ESTABLISHED
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp dpt:22
DROP        tcp  0.0.0.0/0       0.0.0.0/0   multiport dports 21,873,5005,...
DROP        udp  0.0.0.0/0       0.0.0.0/0   multiport dports 123,111,2049,...
ACCEPT      all  192.168.0.0/16  0.0.0.0/0
DROP        all  0.0.0.0/0       0.0.0.0/0

Chain DOS_PROTECT (1 references)
target      prot source          destination
RETURN      icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8 limit: avg 1/sec ...
DROP        icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8
RETURN      tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04 limit: ...
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04
...
```

Introduction to Firewalls

```
Chain INPUT (policy ACCEPT)
target      prot source          destination
DOS_PROTECT all  0.0.0.0/0       0.0.0.0/0
ACCEPT      all  0.0.0.0/0       0.0.0.0/0   state RELATED,ESTABLISHED
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp dpt:22
DROP        tcp  0.0.0.0/0       0.0.0.0/0   multiport dports 21,873,5005,...
DROP        udp  0.0.0.0/0       0.0.0.0/0   multiport dports 123,111,2049,...
ACCEPT      all  192.168.0.0/16  0.0.0.0/0
DROP        all  0.0.0.0/0       0.0.0.0/0

Chain DOS_PROTECT (1 references)
target      prot source          destination
RETURN      icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8 limit: avg 1/sec ...
DROP        icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8
RETURN      tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04 limit: ...
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04
...
```

Introduction to Firewalls

```
Chain INPUT (policy ACCEPT)
target      prot source          destination
DOS_PROTECT all  0.0.0.0/0       0.0.0.0/0
ACCEPT      all  0.0.0.0/0       0.0.0.0/0   state RELATED,ESTABLISHED
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp dpt:22
DROP        tcp  0.0.0.0/0       0.0.0.0/0   multiport dports 21,873,5005,...
DROP        udp  0.0.0.0/0       0.0.0.0/0   multiport dports 123,111,2049,...
ACCEPT      all  192.168.0.0/16  0.0.0.0/0
DROP        all  0.0.0.0/0       0.0.0.0/0

Chain DOS_PROTECT (1 references)
target      prot source          destination
RETURN      icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8 limit: avg 1/sec ...
DROP        icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8
RETURN      tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04 limit: ...
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04
...
```

Introduction to Firewalls

```
Chain INPUT (policy ACCEPT)
target      prot source          destination
DOS_PROTECT all  0.0.0.0/0       0.0.0.0/0
ACCEPT      all  0.0.0.0/0       0.0.0.0/0   state RELATED,ESTABLISHED
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp dpt:22
DROP        tcp  0.0.0.0/0       0.0.0.0/0   multiport dports 21,873,5005,...
DROP        udp  0.0.0.0/0       0.0.0.0/0   multiport dports 123,111,2049,...
ACCEPT      all  192.168.0.0/16  0.0.0.0/0
DROP        all  0.0.0.0/0       0.0.0.0/0

Chain DOS_PROTECT (1 references)
target      prot source          destination
RETURN      icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8 limit: avg 1/sec ...
DROP        icmp 0.0.0.0/0       0.0.0.0/0   icmptype 8
RETURN      tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04 limit: ...
DROP        tcp  0.0.0.0/0       0.0.0.0/0   tcp flags:0x17/0x04
...
```

Introduction to Firewalls

- Firewalls are usually managed manually

Introduction to Firewalls

- Firewalls are usually managed manually
- ... which is extremely error-prone

Introduction to Firewalls

- Firewalls are usually managed manually
- ... which is extremely error-prone
- There are tools to analyze rulesets and discover errors
  - Margrave
  - ITVal
  - FIREMAN
  - Firewall Builder
  - Firewall Policy Advisor
  - ConfigChecker
  - ...

Example: IPSpace Partition

Ruleset from the introduction

- ... treats all packets equally
- ... except for the last two rules

Example: IPSpace Partition

Ruleset from the introduction

- ... treats all packets equally
- ... except for the last two rules

Expected output

- `192.168.0.0/16` is accepted
- Everything else is dropped

ITVal output

```
There is 1 class:  The Universe
```

Problems in Firewall Analysis Tools

- This talk is not about *ITVal*
- Many tools have similar problems

1. Complex Chain model
   - Calling to and returning from user-defined chains
   - May lead to errors in tools

Problems in Firewall Analysis Tools

- This talk is not about *ITVal*
- Many tools have similar problems

2. Vast amount of primitive matches
   - Check `man iptables`
   - Now check `man iptables-extensions`
   - Now check if you have custom extensions running
   - Now think about future features
   - Supporting everything is infeasible
   - Certain features cannot be supported by some tool's algorithm

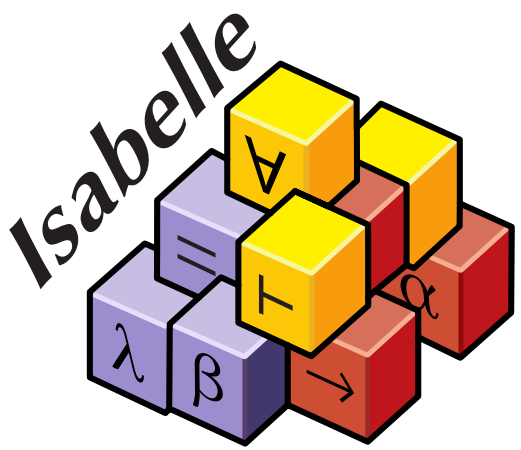
Summary

Problem

Tools cannot “understand” complex real-word rulesets

Our Solution

Semantics-preserving simplification



Agenda

1 Semantics

2 Simplification

3 Evaluation

Agenda

1 Semantics

2 Simplification

3 Evaluation

Syntax

- Rule: $(\mathit{mexpr},\ \mathit{action})$
- Example: $(\texttt{icmp} \wedge \texttt{icmptype}\ 8 \wedge \texttt{limit} : \texttt{avg1/sec} \ldots,\ \texttt{Return})$
- Ruleset: *rule list*
- Firewall state: ✓, ✗, ?
- Primitive matcher: γ
  - Primitive $\rightarrow$ Packet $\rightarrow$ Bool

Syntax

- Rule: $(\mathit{mexpr},\ \mathit{action})$
- Example: $(\texttt{icmp} \wedge \texttt{icmptype}\ 8 \wedge \texttt{limit} : \texttt{avg1/sec} \ldots,\ \texttt{Return})$
- Ruleset: *rule list*
- Firewall state: ✓, ✗, ?
- Primitive matcher: γ
  - Primitive $\rightarrow$ Packet $\rightarrow$ Bool
- Semantics:

$$\gamma, p \vdash \langle rs,\ s \rangle \Rightarrow t$$

Syntax

- Rule: $(\mathit{mexpr},\ \mathit{action})$
- Example: $(\texttt{icmp} \wedge \texttt{icmptype}\ 8 \wedge \texttt{limit} : \texttt{avg1/sec} \ldots,\ \texttt{Return})$
- Ruleset: *rule list*
- Firewall state: ✓, ✗, ?
- Primitive matcher: γ
  - Primitive $\rightarrow$ Packet $\rightarrow$ Bool
- Semantics:

$$\underbrace{\gamma}_{\text{primitive matcher}},\ \underbrace{p}_{\text{packet}} \vdash \langle\ \underbrace{rs}_{\text{ruleset}},\ \underbrace{s}_{\text{start state}}\ \rangle \Rightarrow \underbrace{t}_{\text{final state}}$$

Determinism

$$\text{If} \quad \gamma, p \vdash \langle rs,\ s \rangle \Rightarrow t \quad \text{and} \quad \gamma, p \vdash \langle rs,\ s \rangle \Rightarrow t' \quad \text{then} \quad t = t'$$

Agenda

1 Semantics

2 Simplification

3 Evaluation

Rewriting simple actions

- Remove `Log` actions
- Unfolding custom chains
  - Eliminates `Call`/`Return`
  - Linux kernel only accepts acyclic call graphs
  - $\rightsquigarrow$ unfolding terminates

Rewriting simple actions – Unfolding custom chains

Example

```
Chain INPUT
X  a

Chain X
Return  b
Accept  c
```

Result

$$\left[\left(a \wedge (\neg b) \wedge c,\ \texttt{Accept}\right)\right]$$

Simplification – Summary

- Actions left: `Accept`, `Drop`
- Semantics are preserved

$$\gamma, p \vdash \langle \text{simplify } rs,\ t \rangle \Rightarrow t' \quad \textit{iff} \quad \gamma, p \vdash \langle rs,\ t \rangle \Rightarrow t'$$

Simplification – Summary

- Actions left: `Accept`, `Drop`
- Semantics are preserved

$$\gamma, p \vdash \langle \text{simplify } rs,\ t \rangle \Rightarrow t' \quad \textit{iff} \quad \gamma, p \vdash \langle rs,\ t \rangle \Rightarrow t'$$

- Remaining problems
  1. Unknown primitives matches
  2. Complex nested match-expressions after unfolding unsupported by iptables

Unknown primitives

- Lifting to ternary logic
  - Kleene's 3-valued logic
- Primitive matcher may now return *unknown*
- Default decision strategy: *in-doubt-allow* or *in-doubt-deny*

$$\gamma, p \vdash \langle rs,\ s \rangle \Rightarrow_{\text{allow}} t$$

$$\gamma, p \vdash \langle rs,\ s \rangle \Rightarrow_{\text{deny}} t$$

Unknown primitives

Let m_u be an unknown match.

in-doubt-allow

$$(m_u, \texttt{Accept}) \rightarrow (\text{True}, \texttt{Accept})$$
$$(m_u, \texttt{Drop}) \rightarrow (\text{False}, \texttt{Drop})$$

$\rightsquigarrow$ more permissive ruleset

Example

$\big(\texttt{icmp} \wedge \texttt{icmptype 8} \wedge \texttt{limit} : \texttt{avg1/sec} \ldots, \texttt{Drop}\big) \rightarrow$
$\big(\texttt{icmp} \wedge \texttt{icmptype 8} \wedge \text{False}, \texttt{Drop}\big)$

Closure Property

$$\{p \mid \gamma, p \vdash \langle rs, ? \rangle \Rightarrow_{\text{deny}} ✓\}$$
$$\subseteq$$
$$\{p \mid \gamma, p \vdash \langle rs, ? \rangle \Rightarrow ✓\}$$
$$\subseteq$$
$$\{p \mid \gamma, p \vdash \langle rs, ? \rangle \Rightarrow_{\text{allow}} ✓\}$$

- We continue with one of the approximations

Normalization

- Impossible: `# iptables (tcp ∨ udp) -j ACCEPT`
- Impossible: `# iptables ¬ (src` *ip* `∧ tcp) -j ACCEPT`

Normalization

Problem

iptables supports only negation-normal form with the $\wedge$ connective

Solution

- `normalize`: rule $\rightarrow$ rule list
  where all rules share the same action
- Example (exclude *ip* from accessing an HTTP server)

$$\big[\big(\texttt{src}\ \mathit{ip} \wedge \neg\ (\texttt{tcp} \wedge \texttt{port}\ 80),\ \texttt{Accept}\big)\big] \equiv$$
$$\big[\big(\texttt{src}\ \mathit{ip} \wedge (\neg\ \texttt{tcp} \vee \neg\ \texttt{port}\ 80),\ \texttt{Accept}\big)\big] \equiv$$
$$\big[\big(\texttt{src}\ \mathit{ip} \wedge \neg\ \texttt{tcp},\ \texttt{Accept}\big),\ \ \big(\texttt{src}\ \mathit{ip} \wedge \neg\ \texttt{port}\ 80,\ \texttt{Accept}\big)\big]$$

Agenda

1 Semantics

2 Simplification

3 Evaluation

Evaluation

- Ruleset 1
  - Shorewall firewall on a home router; $\sim$ 500 rules.
  - Unfolding: firewall does not unconditionally drop packets from private IP ranges

Evaluation

- Ruleset 1
  - Shorewall firewall on a home router; $\sim$ 500 rules.
  - Unfolding: firewall does not unconditionally drop packets from private IP ranges
- Ruleset 2
  - Small firewall script found online (`networking.ringofsaturn.com`)
  - Most rules are dead; contrary to documented behavior
  - Author probably confused: `-I` (insert at top) and `-A` (append at tail)

Evaluation

- Ruleset 1
  - Shorewall firewall on a home router; $\sim$ 500 rules.
  - Unfolding: firewall does not unconditionally drop packets from private IP ranges
- Ruleset 2
  - Small firewall script found online (`networking.ringofsaturn.com`)
  - Most rules are dead; contrary to documented behavior
  - Author probably confused: `-I` (insert at top) and `-A` (append at tail)
- Ruleset 3 & 4 & 5
  - Main firewall of our lab
  - Snapshot 2013: $\sim$ 2800 rules
    - Firewall Builder: import errors
    - ITVal: erroneous results
    - After simplification: success
      Upper closure: $\sim$ 1000 rules
      Lower closure: $\sim$ 500 rules
  - Snapshot 2014: $\sim$ 4000 rules
  - Snapshot 2015: almost 5000 rules

Future Work


Our Firewall features
Isabelle
certified
spoofing protection
Here is the sha256 hash of the git sha1 commit that proves it:
658eda77f97f0d36bb56af7ec2132805f40b341595eba1a46df6d7131976e22b
Only sha256 is genuine!
works on my machine
GET YOUR FREE VIRUS NOW!
GitHub Gist
iangreenleaf / yaml.vim
Dumb-smart indentation for Yaml

Q & A

Backup Slides

Specifying Primitive Matchers in Ternary Logic

Very easy: Specify what you know/want, the rest in unknown

```
8  fun common_matcher :: "(common_primitive, simple_packet) exact_match_tac" where
9    "common_matcher (IIface i) p = bool_to_ternary (match_iface i (p_iiface p))" |
10   "common_matcher (OIface i) p = bool_to_ternary (match_iface i (p_oiface p))" |
11
12   "common_matcher (Src ip) p = bool_to_ternary (p_src p ∈ ipv4s_to_set ip)" |
13   "common_matcher (Dst ip) p = bool_to_ternary (p_dst p ∈ ipv4s_to_set ip)" |
14
15   "common_matcher (Prot proto) p = bool_to_ternary (match_proto proto (p_proto p))" |
16
17   "common_matcher (Src_Ports ps) p = bool_to_ternary (p_sport p ∈ ports_to_set ps)" |
18   "common_matcher (Dst_Ports ps) p = bool_to_ternary (p_dport p ∈ ports_to_set ps)" |
19
20   "common_matcher (Extra _) p = TernaryUnknown"
```

Semantics (1)

$$\textsc{Skip}\quad \frac{}{\gamma, p \vdash \langle [],\ t \rangle \Rightarrow t}$$

$$\textsc{Accept}\quad \frac{\text{match } m\ p}{\gamma, p \vdash \langle [(m,\ \texttt{Accept})],\ ? \rangle \Rightarrow \checkmark}$$

$$\textsc{Drop}\quad \frac{\text{match } m\ p}{\gamma, p \vdash \langle [(m,\ \texttt{Drop})],\ ? \rangle \Rightarrow \times}$$

$$\textsc{Reject}\quad \frac{\text{match } m\ p}{\gamma, p \vdash \langle [(m,\ \texttt{Reject})],\ ? \rangle \Rightarrow \times}$$

$$\textsc{NoMatch}\quad \frac{\neg\ \text{match } m\ p}{\gamma, p \vdash \langle [(m,\ a)],\ ? \rangle \Rightarrow ?}$$

Semantics (2)

$$\textsc{Seq}\quad \frac{\gamma, p \vdash \langle rs_1,\ ?\rangle \Rightarrow t \qquad \gamma, p \vdash \langle rs_2,\ t\rangle \Rightarrow t'}{\gamma, p \vdash \langle rs_1 ::: rs_2,\ ?\rangle \Rightarrow t'}$$

$$\textsc{Log}\quad \frac{\text{match } m\ p}{\gamma, p \vdash \langle [(m,\ \texttt{Log})],\ ?\rangle \Rightarrow ?}$$

$$\textsc{Empty}\quad \frac{\text{match } m\ p}{\gamma, p \vdash \langle [(m,\ \texttt{Empty})],\ ?\rangle \Rightarrow ?}$$

Semantics (3)

Background ruleset Γ : *chain name* $\rightarrow$ *rule list*

$$\textsc{CallResult}\quad \frac{\text{match } m\ p \qquad \gamma, p \vdash \langle \Gamma\ c,\ ? \rangle \Rightarrow t}{\gamma, p \vdash \langle [(m,\ \texttt{Call}\ c)],\ ? \rangle \Rightarrow t}$$

$$\textsc{CallReturn}\quad \frac{\begin{array}{c}\text{match } m\ p \qquad \Gamma\ c = rs_1 ::: (m',\ \texttt{Return}) :: rs_2 \\ \text{match } m'\ p \qquad \gamma, p \vdash \langle rs_1,\ ? \rangle \Rightarrow ?\end{array}}{\gamma, p \vdash \langle [(m,\ \texttt{Call}\ c)],\ ? \rangle \Rightarrow ?}$$

Ruleset 3 (excerpt, 22 of 2800 rules displayed)

```
 1  Chain FORWARD (policy ACCEPT)
 2  target     prot opt source               destination
 3  LOG_DROP   all  --  127.0.0.0/8          0.0.0.0/0
 4  ACCEPT     tcp  --  131.159.14.206       0.0.0.0/0           multiport sports 389,636
 5  ACCEPT     tcp  --  131.159.14.208       0.0.0.0/0           multiport sports 389,636
 6  ACCEPT     udp  --  131.159.14.206       0.0.0.0/0           udp spt:88
 7  ACCEPT     udp  --  131.159.14.208       0.0.0.0/0           udp spt:88
 8  ACCEPT     tcp  --  131.159.14.192/27    0.0.0.0/0           tcp spt:3260
 9  ACCEPT     tcp  --  131.159.14.0/23      131.159.14.192/27   tcp dpt:3260
10  ACCEPT     tcp  --  131.159.20.0/24      131.159.14.192/27   tcp dpt:3260
11  ACCEPT     udp  --  131.159.15.252       0.0.0.0/0
12  ACCEPT     udp  --  0.0.0.0/0            131.159.15.252      multiport dports 4569,5000:65535
13  ACCEPT     all  --  131.159.15.247       0.0.0.0/0
14  ACCEPT     all  --  0.0.0.0/0            131.159.15.247
15  ACCEPT     all  --  131.159.15.248       0.0.0.0/0
16  ACCEPT     all  --  0.0.0.0/0            131.159.15.248
17             tcp  --  0.0.0.0/0            131.159.14.0/23     state NEW tcp dpt:22flags: 0x17/0x02
                    recent: SET name: ratessh side: source
18             tcp  --  0.0.0.0/0            131.159.20.0/23     state NEW tcp dpt:22flags: 0x17/0x02
                    recent: SET name: ratessh side: source
19  mac_96     all  --  131.159.14.0/25      0.0.0.0/0
20  LOG_DROP   all  -- !131.159.14.0/25      0.0.0.0/0
21
22  Chain LOG_DROP (21 references)
23  target     prot opt source               destination
24  LOG        all  --  0.0.0.0/0            0.0.0.0/0           limit: avg 100/min burst 5 LOG flags 0
          level 4 prefix "[IPT_DROP]:"
25  DROP       all  --  0.0.0.0/0            0.0.0.0/0
26
27  Chain mac_96 (1 references)
28  target     prot opt source               destination
29  RETURN     all  --  131.159.14.92        0.0.0.0/0           MAC XX:XX:XX:XX:XX:XX
30  DROP       all  --  131.159.14.92        0.0.0.0/0
```

Ruleset 3 – Upper Closure (excerpt)

```
1   Chain FORWARD (policy ACCEPT)
2   target  prot source               destination
3   DROP    all  127.0.0.0/8          0.0.0.0/0
4   ACCEPT  tcp  131.159.14.206/32    0.0.0.0/0
5   ACCEPT  tcp  131.159.14.208/32    0.0.0.0/0
6   ACCEPT  udp  131.159.14.206/32    0.0.0.0/0
7   ACCEPT  udp  131.159.14.208/32    0.0.0.0/0
8   ACCEPT  tcp  131.159.14.192/27    0.0.0.0/0
9   ACCEPT  tcp  131.159.14.0/23      131.159.14.192/27
10  ACCEPT  tcp  131.159.20.0/24      131.159.14.192/27
11  ACCEPT  udp  131.159.15.252/32    0.0.0.0/0
12  ACCEPT  udp  0.0.0.0/0            131.159.15.252/32
13  ACCEPT  all  131.159.15.247/32    0.0.0.0/0
14  ACCEPT  all  0.0.0.0/0            131.159.15.247/32
15  ACCEPT  all  131.159.15.248/32    0.0.0.0/0
16  ACCEPT  all  0.0.0.0/0            131.159.15.248/32
17  DROP    all  !131.159.14.0/25     0.0.0.0/0
```

Ruleset 3 – Lower Closure (excerpt)

```
1   Chain FORWARD (policy ACCEPT)
2   target  prot source               destination
3   DROP    all  127.0.0.0/8          0.0.0.0/0
4   ACCEPT  udp  131.159.15.252/32    0.0.0.0/0
5   ACCEPT  all  131.159.15.247/32    0.0.0.0/0
6   ACCEPT  all  0.0.0.0/0            131.159.15.247/32
7   ACCEPT  all  131.159.15.248/32    0.0.0.0/0
8   ACCEPT  all  0.0.0.0/0            131.159.15.248/32
9   DROP    all  131.159.14.92/32     0.0.0.0/0
10  DROP    all  131.159.14.65/32     0.0.0.0/0
11  ... (unfolded DROPs from chain mac_96)
12  DROP    all  !131.159.14.0/25     0.0.0.0/0
```