Verified iptables Ruleset Verification

Cornelius Diekmann  diekmann@net.in.tum.de

---

Packet Filtering In Simple Terms

Matching a packet

- match \( \gamma \) (Match \( \beta \)) \( p \) \( \quad \Rightarrow \quad \gamma \beta p \)
- match, MatchAny \( \gamma \) \( p \) \( \quad \Rightarrow \quad \) True
- match \( \gamma \) (MatchNot \( m \)) \( p \) \( \quad \Rightarrow \quad \sim \) match \( \gamma \) \( m \) \( p \)
- match \( \gamma \) (MatchAnd \( m_1 \), \( m_2 \)) \( p \) \( \quad \Rightarrow \quad \gamma m_1 p \land \gamma m_2 p \)

Processing a ruleset

```
<table>
<thead>
<tr>
<th>Step</th>
<th>Accept</th>
<th>Reject</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>( \gamma, p \vdash [\langle \langle m, \text{Accept} \rangle \rangle, \phi] \Rightarrow \phi )</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>( \gamma, p \vdash [\langle \langle m, \text{Reject} \rangle \rangle, \phi] \Rightarrow \phi )</td>
<td></td>
</tr>
</tbody>
</table>
```

- For any primitive matcher \( \gamma \) (primitive \( \Rightarrow \) packet \( \Rightarrow \) \( \beta \))
- For any well-formed ruleset \( \Gamma \)
- Specification not executable but deterministic

---

Formal Verification

All the algorithms and translations are machine-verifiably proven sound with the Isabelle proof assistant.

Using Isabelle's code generation feature, a stand-alone Haskell tool is derived from the theory.

---

Easy to Use

adm@fw# iptables-save | ./check ipassmt.txt
preprocessing ruleset
sanity checking ipassmt
checking spoofing protection:
eth1.96 True
eth1.109 False
...  
```
[timen] real 0m38.439s
```

---

Service Matrix: SSH Connectivity

```
<table>
<thead>
<tr>
<th>Service Matrix</th>
<th>SSH Connectivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>{224.0.0.0..239.255.255.255}</td>
<td>{0.0.0.0..126.255.255.255} ∪ {128.0.0.0..131.159.13.255} ∪ {131.159.16.0..131.159.19.255} ∪ ... 88.95.232.64..188.95.232.191} ∪ {138.246.253.6..138.246.253.10} ∪ 138.246.253.5 ∪ 131.159.15.50 ∪ {127.0.0.0..127.255.255.255}</td>
</tr>
</tbody>
</table>
```

"Which machines are accessible via ssh?"

Table filter: 4911 rules, 94 user-defined chains.

---

Sound, Permissive Ruleset Simplification

For arbitrary iptables matching rules:

- \( \{ p. \text{ new } p \land \gamma, p \vdash (r_1, \phi) \Rightarrow \phi \} \)

where simple-fw can only match on

- in/out interface, including support for the "*" wildcard
- src/dst IP address range in CIDR notation, e.g. 192.168.0.0/24
- protocol (*, or any numeric protocol identifier)
- src/dst interval of ports, e.g. 0:65535

---

YO DAWG I HEAR YOU LIKE VERIFICATION

Free & Open Source

http://iptables.isabelle.systems/