Design and Implementation of DNSSEC Simulator using Unmodified Real Implementations

Hajime Tazaki, Tomohiro Ishihara, Yuji Sekiya
*University of Tokyo, Japan

Motivation
DNSSEC, why not?
• Solutions for DNS spoofing problem
Obstacles
• Needs update, increase operational/computational load
• Exploited by attacker (amplifier attack)

Challenges
• Study possible operational costs without actual deployment
• But hard to investigate/not realistic output

Simulation vs Emulation vs Testbed?

<table>
<thead>
<tr>
<th>Simulation</th>
<th>Emulators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Realism</td>
<td>??</td>
</tr>
<tr>
<td>Timing Realism</td>
<td></td>
</tr>
<tr>
<td>Topology Flexibility</td>
<td>(limited)</td>
</tr>
<tr>
<td>Easy Replication</td>
<td></td>
</tr>
<tr>
<td>Experimental Scalability</td>
<td></td>
</tr>
</tbody>
</table>

Fig. 1 Attacks of spoofing DNS packets.

Architectures
Implemented by Direct Code Execution (DCE) [2] (ns-3 extension)
Highlights
• Using useful simulator’s features
  • Reproducible timing, control, deep inspection
  • Various Zone/Topology/Traffic configurations
  • Flexible control of experiment
  • Input parameters, Output result analysis

Scenarios
• Process overhead at validators
• Reproducible any experiment
  • Network incidents, (possibly mitigations)

Fig. 3 Overview of DNSSEC simulator.

Simulations
• Reproducible, Scalable
  • but not realistic (pitfall)
Emulations
• Real(istic)
  • but hard to control, not scalable
Real environments
• Real
  • but limited flexibility

References

Fig. 2 Experimental DNS tree

Executable Software
• Bind9 (Root, Auth DNS Server)
• Unbound (Cache resolver)
• dig command (querier)
• Linux kernel (for forwarding plane)

Future Plans/Ideas
Reproduce network incidents from measurement data
• DDoS (DNS/ntp reflection attack)
• Input traffic source from Hadoop
• Apply mitigation ideas (C-plane, D-plane)

Further Information
• Project Web page:
  http://dnssec.sekiya-lab.info/