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)

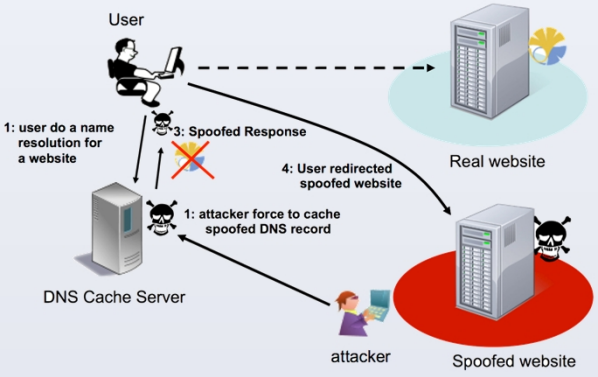

Fig. 1 Attacks of spoofing DNS packets.

Challenges

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

Simulation vs Emulation vs Testbed ?

	Simulators	Testbeds	Emulators
Functional Realism	???	p	p
Timing Realism	p	p	p
Topology Flexibility	p	(limited)	p
Easy Replication	p	p	p
Experimental Scalability	p		

Simulations

- Reproducible, Scalable
- but not realistic (pitfall)

Emulations

- Real(istic)
- but hard to control, not scalable

Real environments

- Real
- but limited flexibility

Architecture

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
- With improving simulator's weakness (Functional realism)
  - Runnable real binaries (bind9, unbound)

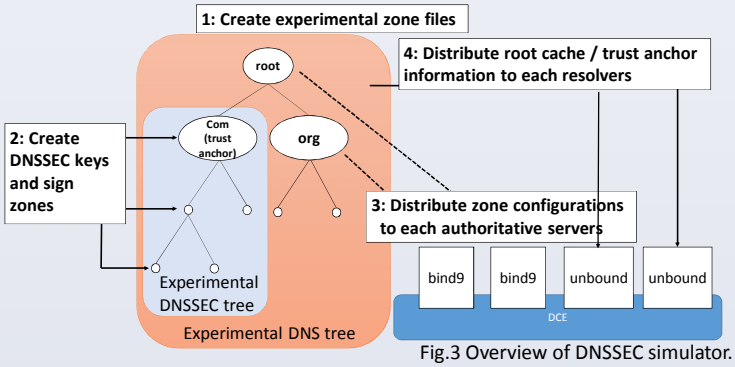

Fig.3 Overview of DNSSEC simulator.

Use-Cases

Scenarios

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

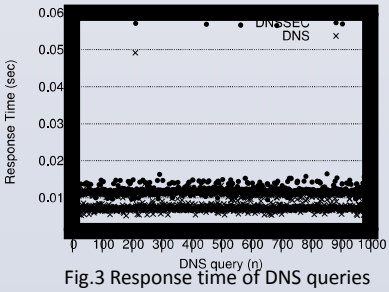

Fig.3 Response time of DNS queries w,w/o key validations.

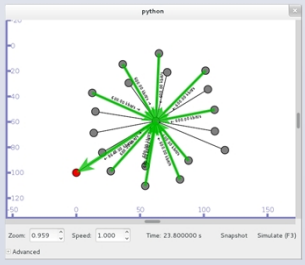

Fig.4 DNS reflection attack with bind9 over ns-3 DCE.

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/

References

[1] Tomohiro Ishihara, Hajime Tazaki, Yuji Sekiya, **Design and Implementation of DNSSEC Simulator using Unmodified Real Implementations**, IEICE Tech. Report., vol. 133, no 240, IA2013-27, pp. 7-12, October 2013.

[2] Hajime Tazaki, Fréderic Urbani, Emilio Mancini, Mathieu Lacage, Daniel Câmara, Thierry Turletti, and Walid Dabbous, **Direct Code Execution: Revisiting Library OS Architecture for Reproducible Network Experiments**, ACM CoNEXT 2013, December 2013.

[3] Daniel Camara, Hajime Tazaki, Emilio Mancini, Mathieu Lacage, Thierry Turletti, and Walid Dabbous. **DCE: Test the real code of your protocols and applications over simulated networks**. IEEE Communications Magazine, (to appear), March 2014.