Subverting BIND’s SRTT Algorithm  
**Derandomizing NS Selection**

Roee Hay  
roeeh@il.ibm.com  
Jonathan Kalechstain  
kalechstain@gmail.com  
Dr. Gabi Nakibly  
gabin@rafael.co.il  

---

**DNS 101**

The DNS protocol maps domain names into IP addresses and vice versa. It is usually carried over UDP port 53. BIND is the most popular DNS server.

---

**Off-Path DNS Cache Poisoning Attacks**

The attacker’s goal is to inject a forged entry into the target resolver’s cache, in order to subvert the confidentiality and/or integrity of the resolver’s clients. The attacker does not see the information between the resolver and the server.

---

**The New Attack**

Our attack lowers the SRTT value of an arbitrary NS to a very low value. In contrast to previous work, we present a deterministic attack against BIND which abuses non-open NSs that can be easily found across the Internet.

---

**BIND’s SRTT Algorithm**

**Goal.** Choose the most responsive (by Round-Trip Time) authoritative nameserver (NS).

**Problem.** RTT changes frequently.

**Data structure.** A moving average for each NS IP.

**Operations.**

- **Initialize**  
  \[ SRTT \in [1,32] \mu s \]

- **Update**  
  \[ SRTT = 0.7 \cdot SRTT_{old} + 0.3 \cdot RTT \]

- **Decay**  
  \[ SRTT = 0.98 \cdot SRTT_{old} \]

- **Error**  
  \[ SRTT = \min (SRTT_{old} + 200\text{ms}, 1s) \]

**Cache.** A map indexed only by NS IPs is maintained.

**Selection.** Authoritative NS with lowest SRTT value is queried first.