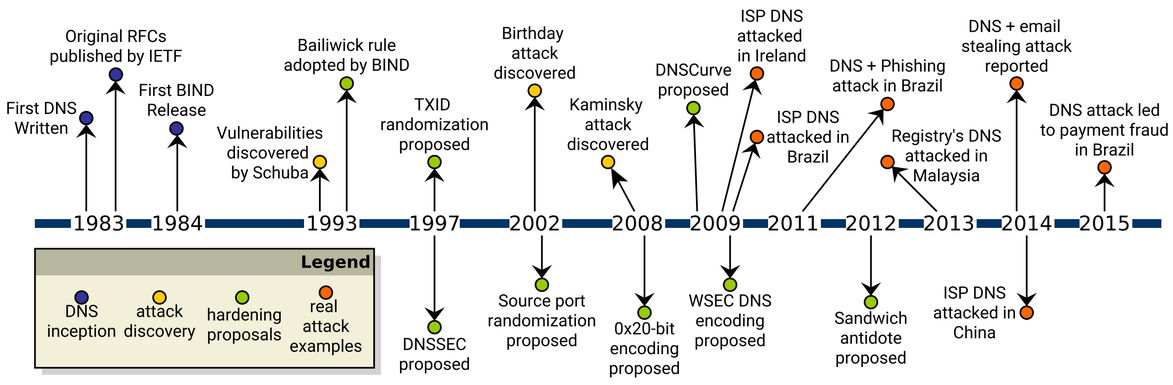
CERIAS
The Center for Education and Research in Information Assurance and Security

*CG*uard: Adaptive Defense Against DNS Cache Poisoning Attacks By Off-path Adversaries

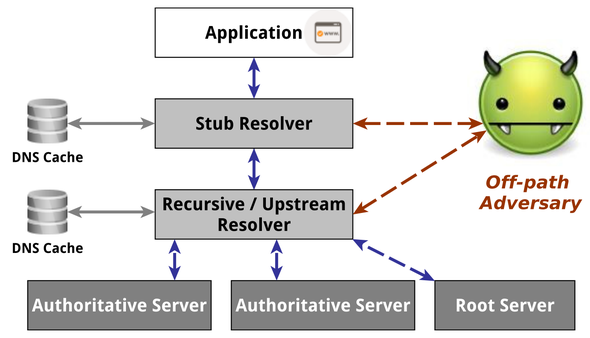
Omar Chowdhury, Sze Yiu Chau, Victor Gonsalves, Weining Yang, Huangyi Ge, Sonia Fahmy, Ninghui Li
Computer Science, Purdue University

(1) History of DNS Cache Poisoning



(2) Why do we care?

- Cache poisoning is a **real threat**
- Can be used to
  - → Track users and serve Ads
  - → Conduct MITM attacks
  - → Trigger drive-by downloads
- **Serious** potential **damages**
  - → Compromise confidentiality
  - → Mount fraudulent transactions

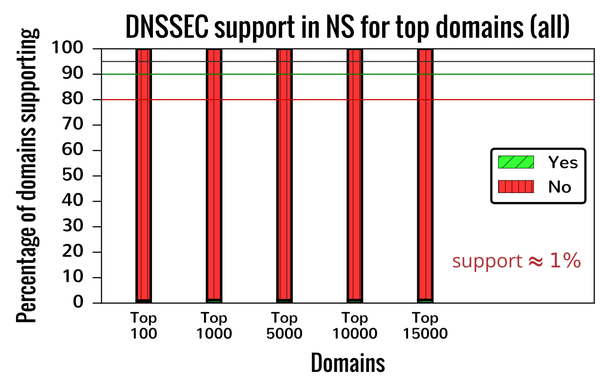


(3) Existing Solutions – Short Term

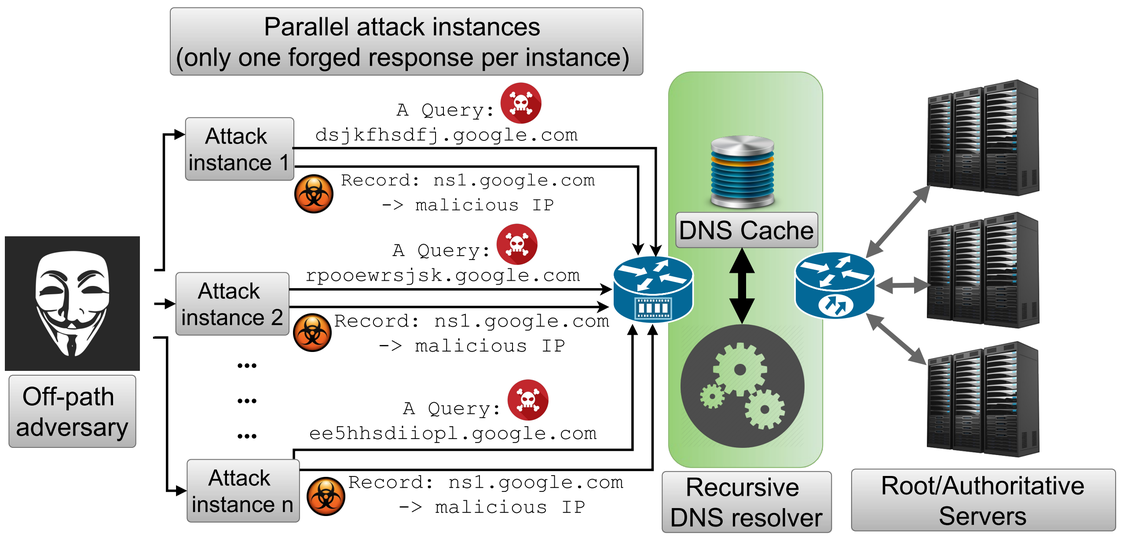
- Entropy increasing mechanisms
  - → Source **port** randomization
  - → IP **address** (destination, source) randomization
  - → **0x20**-bit encoding - rAnDOm caPitALiZaTiOn
  - → **WSEC** DNS - prepend random nounce to queries
- Other mechanisms
  - → Hold-on - wait and use RTT to pick among multiple matching responses
  - → Sandwich Antidote - sends 3 queries, expects 3 in-order valid responses

(4) Existing Solutions – Long Term

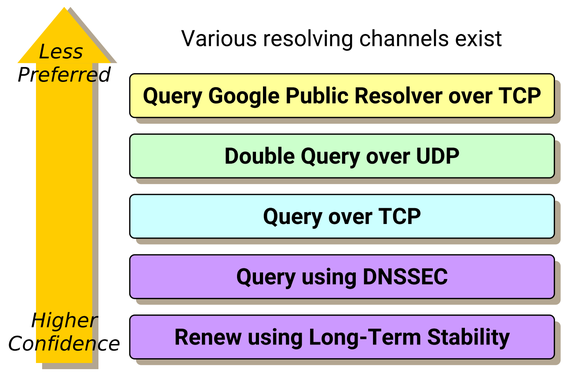
- Using cryptographic means
  - → **DNSCurve** - breaks caching; key distribution problem
  - → **DNSSEC** - adoption is low
- Using P2P cooperative network
  - → **CoDNS** (OSDI '04)
  - → **DoX** (ICC '06)
  - → **CofiDNS** (WORLDS '06)

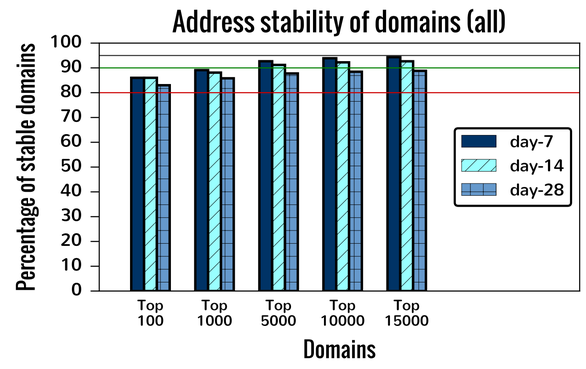


(5) New attack – Parallel Kaminsky



(6) Intuition Behind Our Adaptive Approach





(7) Experiment Results

- We evaluate our defense by implementing in Unbound 1.5.4, and then run instances of Parallel Kaminsky attack against it

	Turn #	1	2	3	4	5	6
Original	Instances	2266	1331	**3072**	1884	2519	1674
	Result	Poisoned	Poisoned	Failed	Poisoned	Poisoned	Poisoned
Modified	Instances	**3072**	**3072**	**3072**	**3072**	**3072**	**3072**
	Result	Failed	Failed	Failed	Failed	Failed	Failed

(8) Take-aways

- DNS cache poisoning is still an **unsolved problem**
  - → Internet was not designed with inbuilt authentication
  - → Long term fixes like DNSSEC are not incentive compatible and hence are not deployed wide enough
- An **adaptive defense mechanism** is desirable
  - → Compatible with the existing **infrastructure**
  - → Compatible with service providers' **incentive**
  - → Deterrence comes almost for free in terms of **performance**
  - → Can benefit from a wide adoption of long term solutions

CERIAS®

PURDUE UNIVERSITY