Agenda

- Remote DNS Cache Poisoning Attack - The Kaminsky Attack

Kaminsky Attack

- aka., Kaminsky Vulnerability.
- DNS cache poisoning vulnerability.
- Discovered by Dan Kaminsky in 2008.
- Root cause: DNS transaction ID: only 2^{16} (65,536) possibilities.
- Key idea: target non-existing sibling subdomains - bypass cache effect or TTL defense.

Two Defense Approaches

- Source Port Randomization: makes the attack up to 65,536 times harder - implemented in most major DNS servers.
- DNSSEC: Domain Name System Security Extensions (Digital signatures introduced into DNS responses - checks the digital signature to verify if it's a valid or fake response.)

References

A large portion of the material is adapted from:

- Computer Security - A Hands-on Approach by Wenliang Du