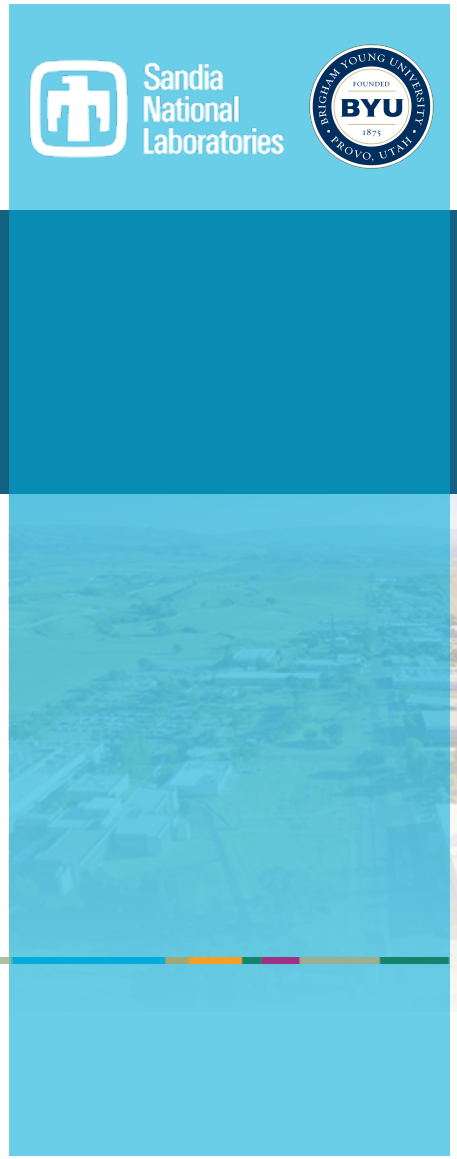


A Peek Into the DNS Cookie Jar:

An Analysis of DNS Cookie Use

BY

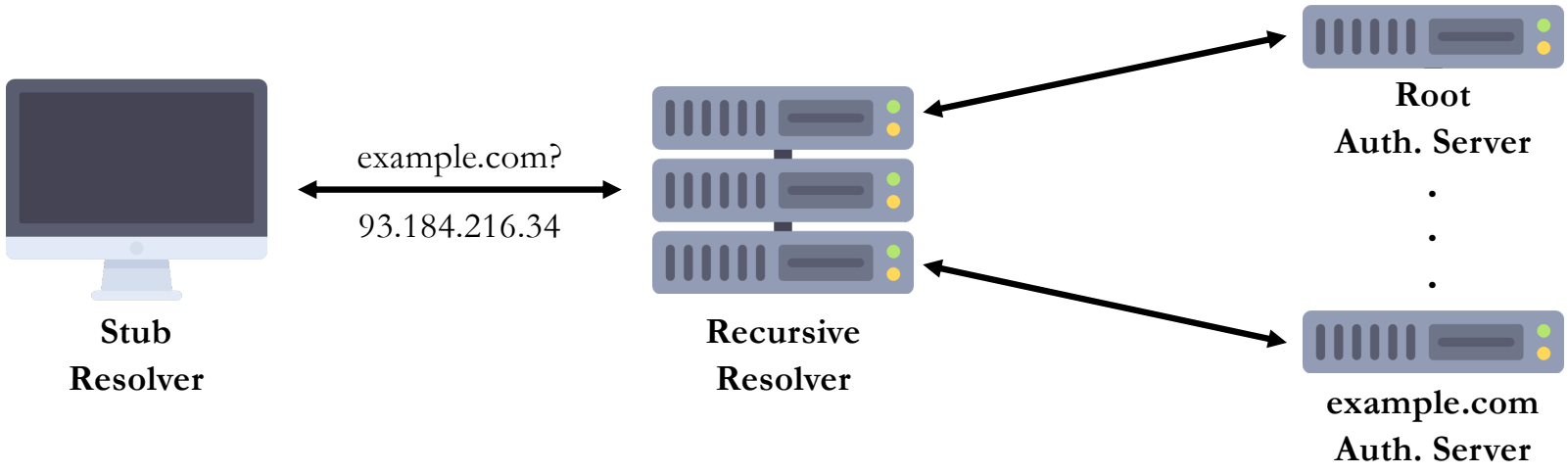
Jacob Davis and **Casey Deccio**

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Unless otherwise noted, images by Freepik from flaticon.com

Domain Name System (DNS) Overview

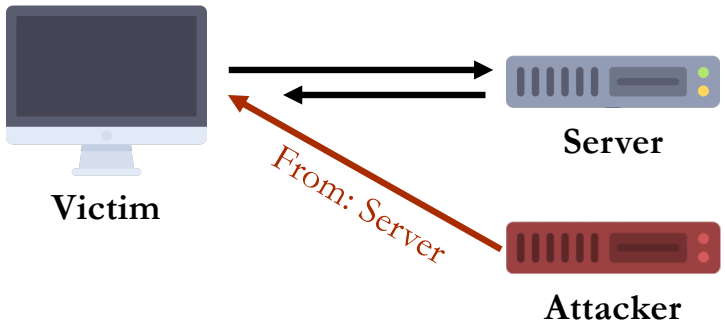
- 2 client-server pairs
  - Stub resolver ↔ recursive resolver
  - Recursive resolver ↔ authoritative server
- Typically runs over UDP (original standard)



Attacks On Identity Management

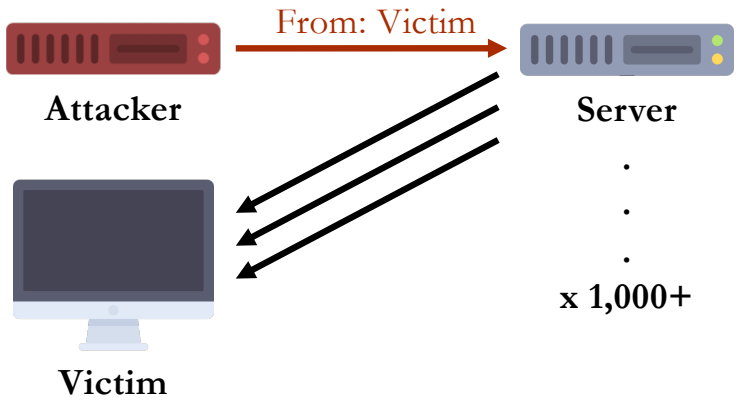
Cache Poisoning

Spoof server response maliciously



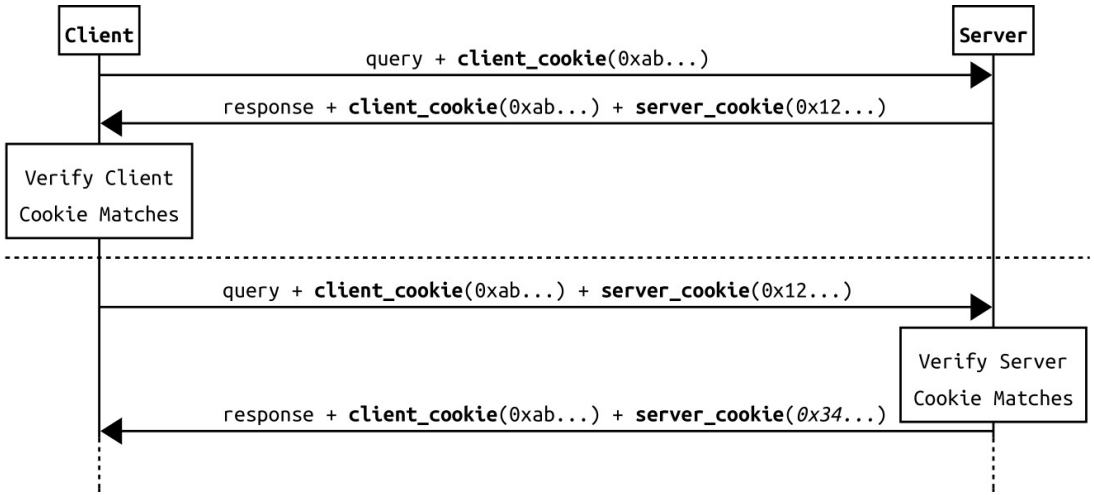
Denial of Service via Reflection

Flood victim with responses to spoofed queries



DNS Cookies

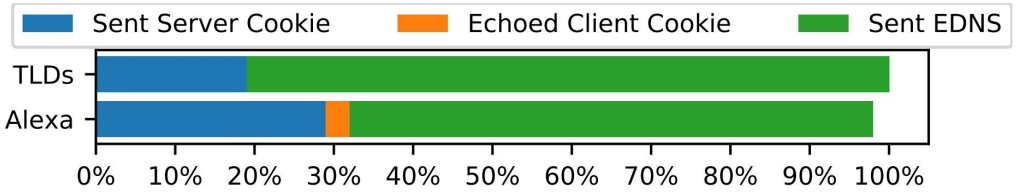
- Extension to DNS messages that provides identity management
- Standardized in 2016
- Clients and servers exchange cookie values
  - Can then verify in future transactions
  - Off-path attacker can't see value

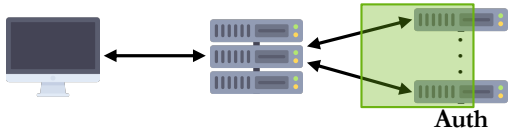


Authoritative Server Support

- Analyzed servers for top-level domains (TLDs) and Alexa top 1 million sites
  - For each: query for nameserver then IPs of nameserver
- 157,679 Alexa IPs and 6,615 TLD IPs

- >98% support EDNS
- <30% fully support cookies

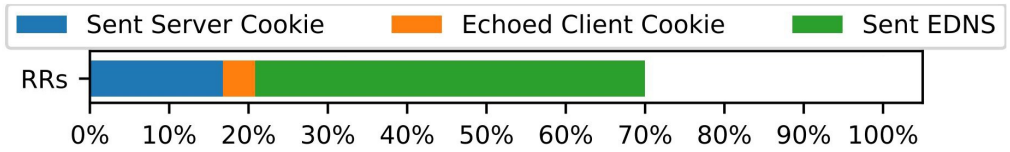


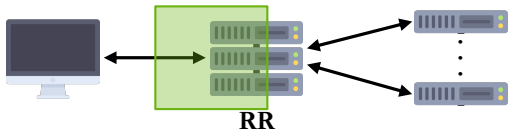


Recursive Resolver Support — Server-Side

- Queried every IPv4 address. Check if queried our server, flags, error codes
- 1,908,397 open resolvers discovered

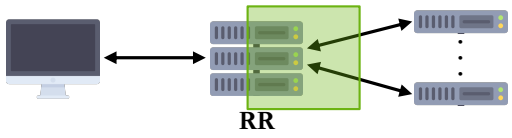
- 70% support EDNS
- 17% fully support cookies





Recursive Resolver Support — Client-Side

- For each resolver, query for a domain we control
  - See if their query to us includes cookie
- 93,395 IPs (representing 1.55 million resolvers)
  - Implies large amount of forwarding
- 9.1% sent at least one query with a cookie

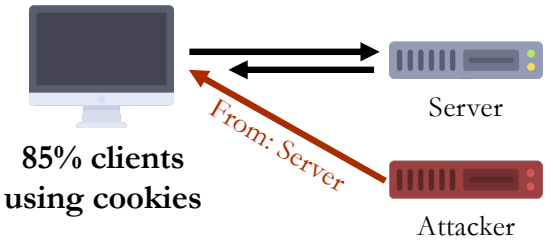


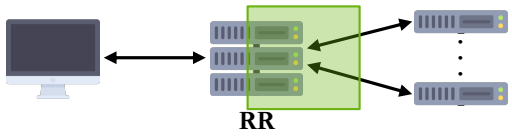
Cookie Enforcement — Clients

- Alter our server responses for 1.5 million resolver clients
  - First respond with full cookie support. Then vary future response
- 28,605 clients considered

- ~85% clients behave normally when no cookie/EDNS present
  - Only 20% when presented with incorrect cookie
- Susceptible to cache poisoning (barring other measures)
- Unsafe and direct violation of specification

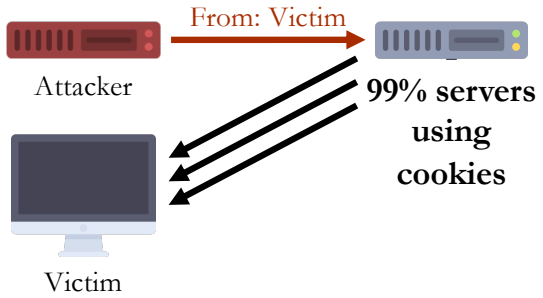
> RFC: "If the client is expecting the response to contain a COOKIE option and it is missing, the response MUST be discarded."



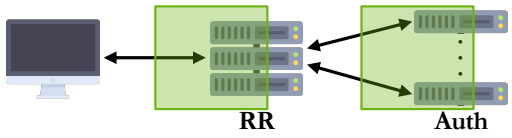


Cookie Enforcement — Servers

- Query servers with real server cookie, no cookie, then fake cookie
- Per specification, server may:
  1. Silently discard query
  2. Respond with `BADCOOKIE` error code
  3. Respond normally
- 41,083 Alexa IPs; 1,246 TLD IPs; 137,896 resolver IPs

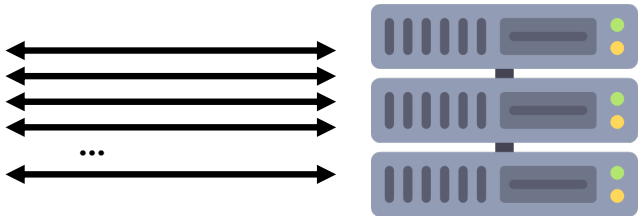


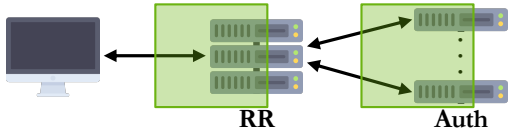
- >99% respond normally with missing or fake cookie
- Nearly all servers can still be utilized for reflection attacks



Dynamic Server Cookies – Experiment

- Dynamic cookies include nonce, timestamp (clear text), and hash
- Experiment:
  - Send 60 queries to each server
  - Collect cookies returned by each server
  - Identify dynamic cookies and other interesting behaviors

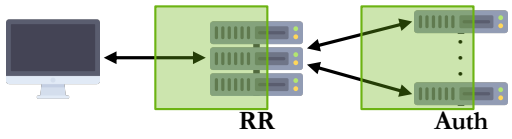




Dynamic Server Cookies – Timestamp Observations

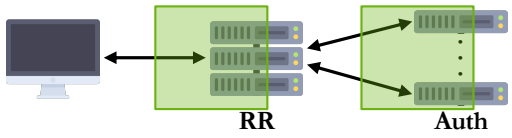
- Dynamic cookies:
  - Embedded timestamp between 1 hour in the past and 30 minutes in the future
  - Auth servers:
    - 99% returned at least one dynamic cookie
  - Recursive servers:
    - 83% returned at least one dynamic cookie
- ts_{diff}: absolute difference between query time and timestamp field:
  - 1, 1, 1, 1, 1, 2, 1, 1, 1, 1 … => All Cookies accurate ($|ts_{diff}| <= 5s$)
  - 75, 75, 75, 75, 75, 75, 75, 75 … => All Cookies Out-of-Sync($|ts_{diff}| > 60s$)
  - 1, 1, 1, 1, 75, 1, 2, 1, 75, 1 … => Mixed Accurate & Out-of-Sync
    - Indicative of 5 backend servers: four with an accurate clock and one that is out of sync

	Alexa	TLDs	RRs
All Cookies Accurate ($\|ts_{diff}\| \leq 5s$)	41,639 (96%)	1,225 (98%)	131,520 (95%)
All Cookies Out-of-Sync ($\|ts_{diff}\| > 60s$)	1,615 (3.7%)	17 (1.4%)	3,544 (2.6%)
Mixed Accurate & Out-of-Sync	66 (0.15%)	0 (0.0%)	2,980 (2.2%)



Dynamic Server Cookies – Interoperability

- Interoperable Cookies:
  - begin with 0x01000000; AND
  - are dynamic (i.e., have embedded timestamp between 1 hour in the past and 30 minutes in the future)
- Results:
  - Auth servers:
    - 4.2% used interoperable cookies
  - Recursive servers:
    - 18% used at least one interoperable cookie
    - 6.5% used a mixture of interoperable and non-interoperable cookie
      - Inconsistent with the spirit of interoperable cookies!



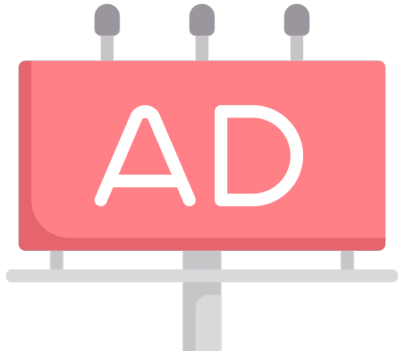
Possible Enforcement Methods

Clients

- Should begin enforcing cookies when expected
- Or rely on other methods

Servers

- More difficult to determine client support
  - A client using cookies once may not always use them
- One solution may be for clients to "advertise" support in reverse DNS
  - Servers could then check and enforce advertisements



Conclusion

- DNS Cookies are a recent standard that add identity management
- ~30% of servers and 10% of recursive clients are using cookies

- Only ~15% of clients enforce cookies properly
- Less than 1% of servers enforce cookies

- Possible solution: clients "advertise" intended use of cookies