November 12’ 2017
IEPG Open Meeting-IETF100

Impact of security vulnerabilities in timing protocols on Domain Name System (DNS)

Aanchal Malhotra[1], Willem Toorop[2], Benno Overeinder[2], Sharon Goldberg[1]
Boston University[1], NLnet Labs[2]

Recommendations based on : draft-aanchal-time-implementation-guidance-00 - On Implementing Time

Previous Work on NTP [RFC5905]

[1] **Attacking the Network Time Protocol.**

A. Malhotra, I. Cohen, E. Brakke, S. Goldberg. In the proceedings of The Network & Distributed System Security Symposium (NDSS), CA, 2016.

[2] **Attacking NTP's Authenticated Broadcast Mode**.

A. Malhotra, S. Goldberg. ACM SIGCOMM, Computer Communication Review, 2016.

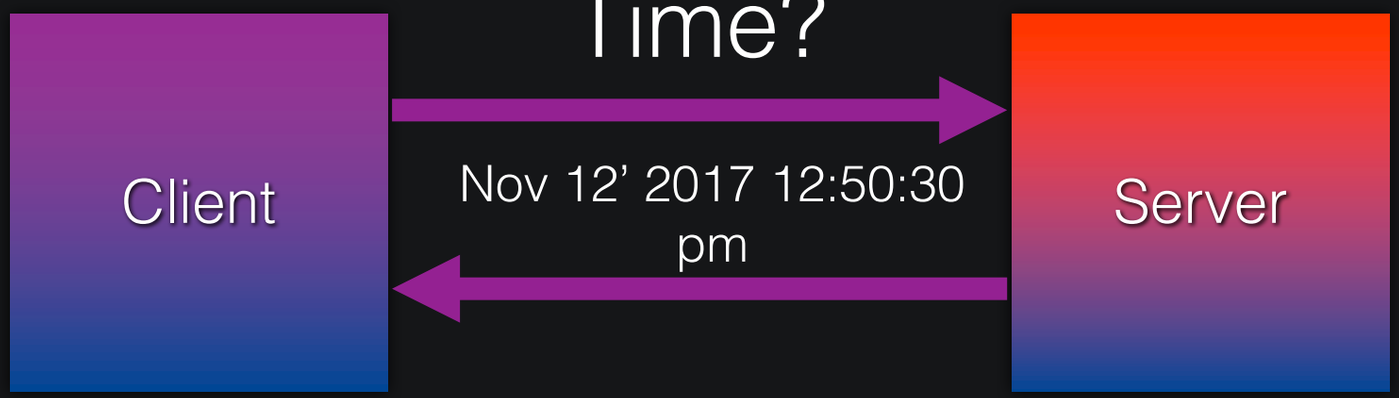
[3**] The Security of NTP's Datagram Protocol.**

A. Malhotra, M.V. Gundy, M. Varia, H. Kennedy, J. Gardner, S. Goldberg. In the proceedings of 21st International Conference on Financial Cryptography and Data Security (FC), 2017.

Outline of the Talk

- Background - Network Time Protocol (NTP)
- DNS - dependence on time, current implementation-problems & recommendations
- DNSSEC – dependence on time, current implementation-problems & recommendations
- Measuring the attack surface – challenges & results

Background: Network Time Protocol (NTP)



Client/Server model

Client may update its time to Nov 12’ 2017 12:50:30 pm

How does DNS depend on time?

Caching of Resource Records (RRs)

- Time to Live indicates the duration (Time spans)

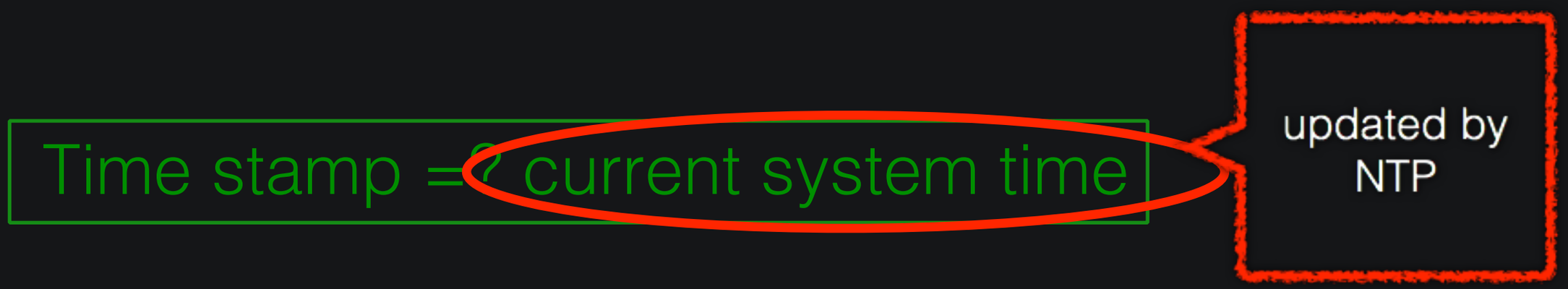
```
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         228     IN      A       172.217.9.68
```

How do software implementations deal with time spans?

- In a typical software implementation (Unbound, Bind, PowerDNS, DNSMasq, etc)

Time spans - translated to time stamps.



Why is this a problem?

- Timing protocols are subvertible.
  - off-path time shifting and Denial of Service (DoS) attacks on NTP clients [1, 2, 3]
- In this work we show that :
  - these vulnerabilities can be leveraged to perform off-path attacks on DNS cache
    - Cache-sticking attack (Time shifted forward)
    - Cache-expiration attack (Time shifted backwards)

Recommendation

- Not a protocol problem ☺
- Deal with implementations ONLY!
- Since we do not need absolute time, use “**RAW TIME**” (on POSIX systems)
  - Can’t be set or changed manually
  - Not adjusted by network time protocols.

draft-aanchal-time-implementation-guidance-00 - On Implementing Time

How does DNSSEC depend on time?

Validation of crypto DNSSEC RRs

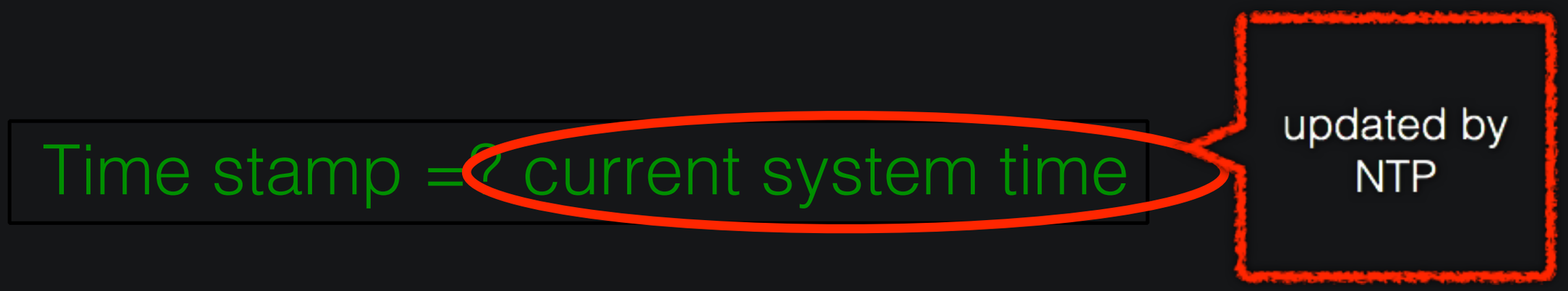
- Signature inception and expiration times (Time stamps)

```
d0.dig.afilias-nst.info. 83797  IN      AAAA    2a01:8840:9::1
ns-ext.nlnetlabs.nl.    7598    IN      RRSIG   A 8 3 10200 20171129015003 20171101015003 42
393 nlnetlabs.nl. zOcSBB8C06IpUZ+8OGxdafqMv9gCYGHkCG9WDayetXwh/b/kxhec6uNU unYrsMDuVZUPYo6Gr
lo3AHM17HnuDPYoFuPXIuAQNGCej8hXm2DB/NbR QotCaaXUuoQ4hqiiifwK4qbW8W9QT79Jc251CKBsCL28TOmcVYFq
h02H kGQ=
```

How do implementations deal with time stamps?

Again,

In a typical software implementation (Unbound, Bind, PowerDNS, DNSMasq, etc)



Recommendations

- Fundamental problem with the protocol ☹
- Have to use SYSTEM TIME

The only solution

Fix Network Time Protocols ☺

Measure the attack surface
RIPE ATLAS

- RIPE Atlas probes get resolvers list from DHCP
- Total 10,320 probes. Allows DNS queries to its resolvers BUT .....

Challenge1: Only to public IP addresses.

Solution: *o-o.myaddr.l.google.com. TXT*

whois.akamai.net. A

We got 8,244 DNS resolvers with public IP addresses (from 4,594 probes)

Measure the attack surface RIPE ATLAS

- To identify NTP servers from these resolvers:
  - 2,021 (24.5%) answered NTP time queries.
  - How many are vulnerable to NTP attacks?

Challenge 2: CAN NOT send NTP control queries from ATLAS probes

Solution 1: From outside, 75 (0.9%) answered control queries

Solution 2: Form inside using NLnog ring nodes in the same ASN,1.23% answered control queries

Measure the attack surface
Open resolvers

Open Resolver Project - 16.5M IPs identified (Aug'17)

Out of 6.5M of those:

2.3M still answered DNS queries (Nov'17), BUT

1.7M (72.5%) answered REFUSED (authoritatives?)

600K (27.5%) did a lookup (open resolvers)

- 3.72% answered NTP time queries
  (recall 24.5% in Atlas)
- 0.93% answered NTP control queries
  (0.91% from Internet, 1.23% from inside at least)

Conclusion

- Time to think about time!
- Refer to the draft :

draft-aanchal-time-implementation-guidance-00 - On Implementing Time

- More attack vectors based on time?
- More ways of measuring the attack surface?