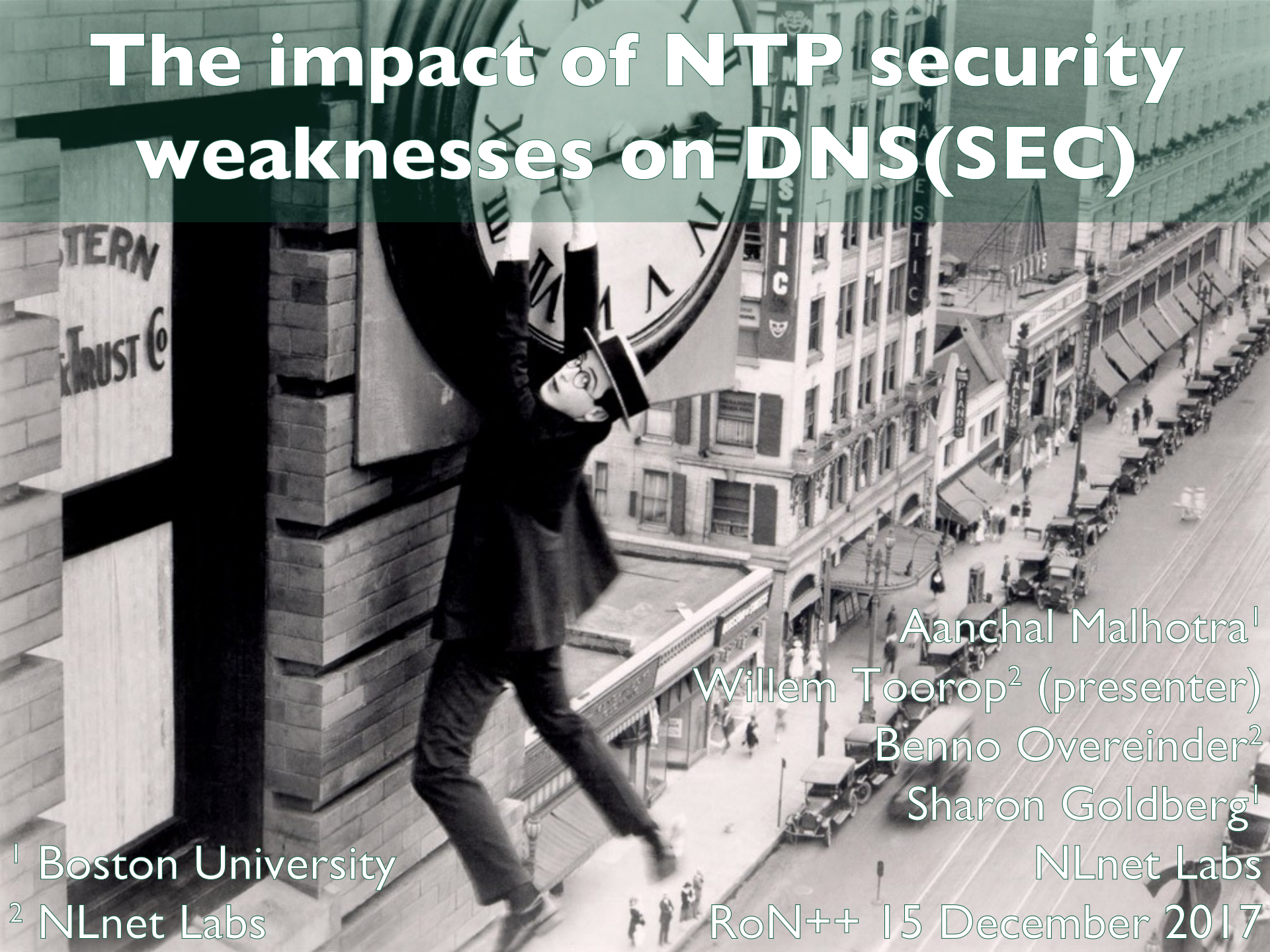
The impact of NTP security weaknesses on DNS(SEC)



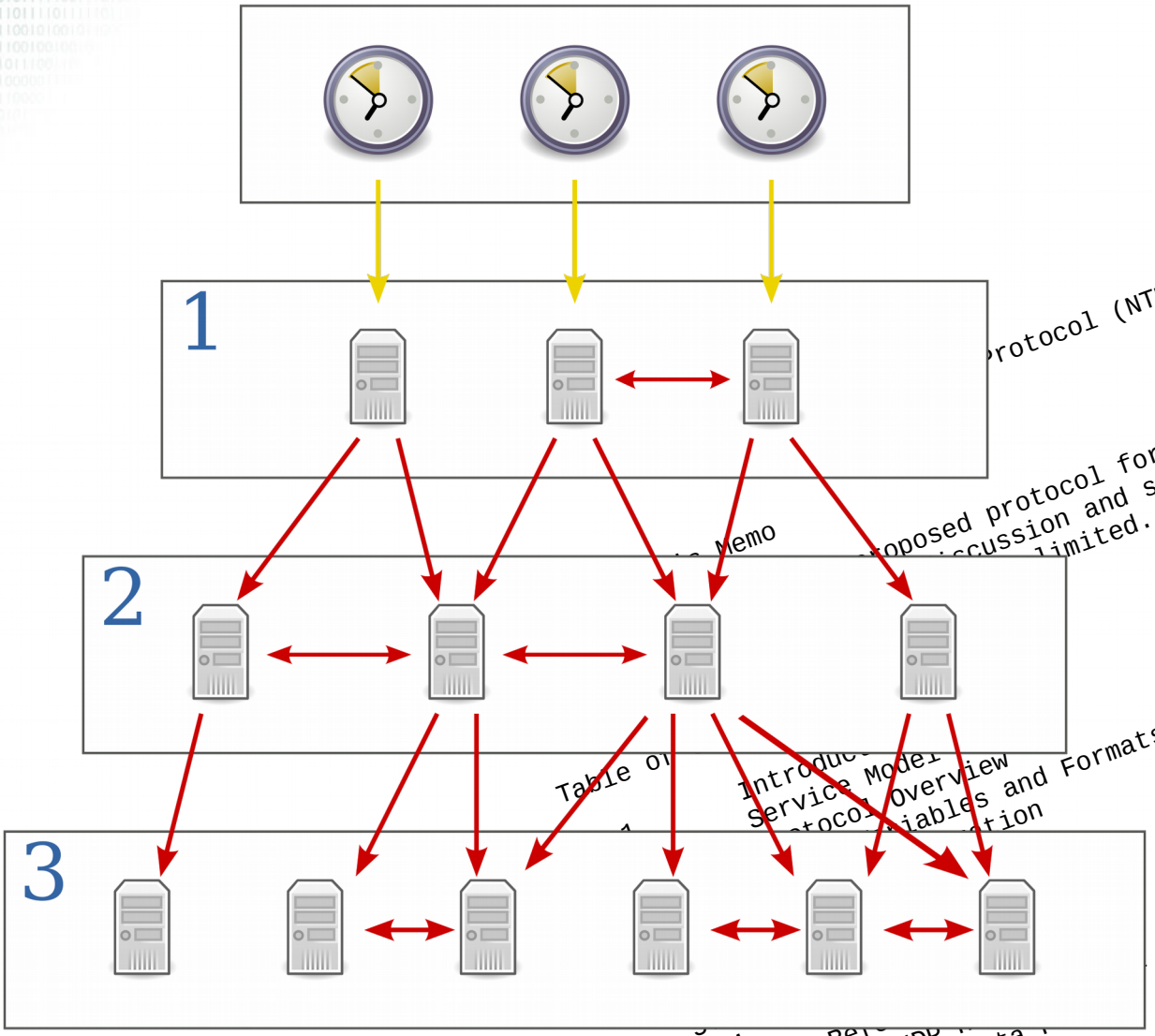
Aanchal Malhotra[1]
Willem Toorop[2] (presenter)
Benno Overeinder[2]
Sharon Goldberg[1]

[1] Boston University
[2] NLnet Labs

NLnet Labs

RoN++ 15 December 2017

Network Time Protocol



D.L. Mills
M/A-COM Linkabit
September 1985

Protocol (NTP)

proposed protocol for the ARPA-Internet
discussion and suggestions for improvements.
limited.

Memo

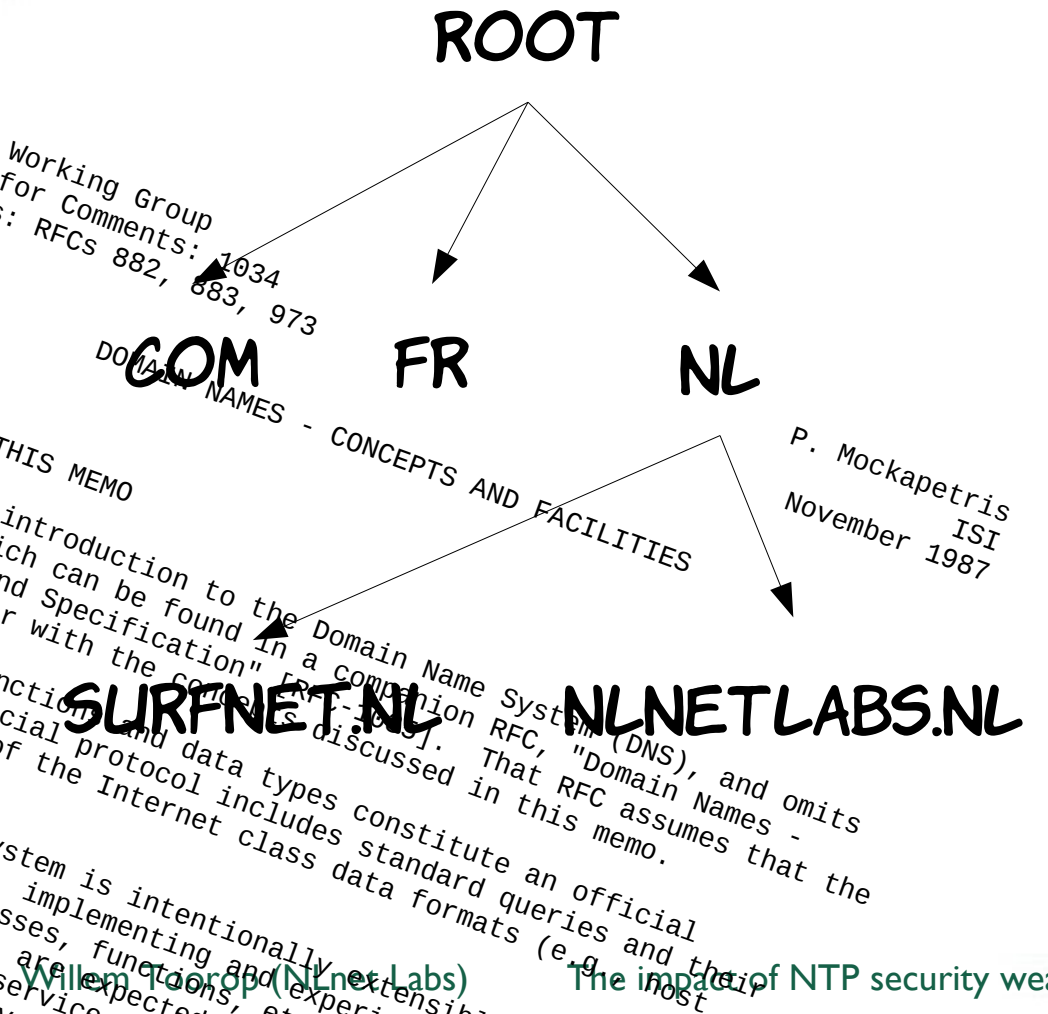
Table of

Introduc
Service Model
Protocol Overview
Variables and Formats
tion

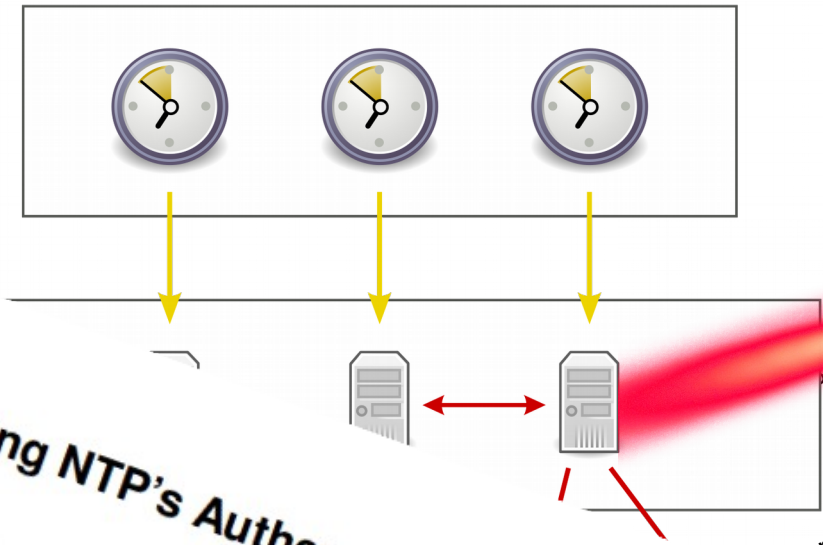
5.4. Ref
6. UDP
Appendix A. NTP Data
Appendix B. NTP Data

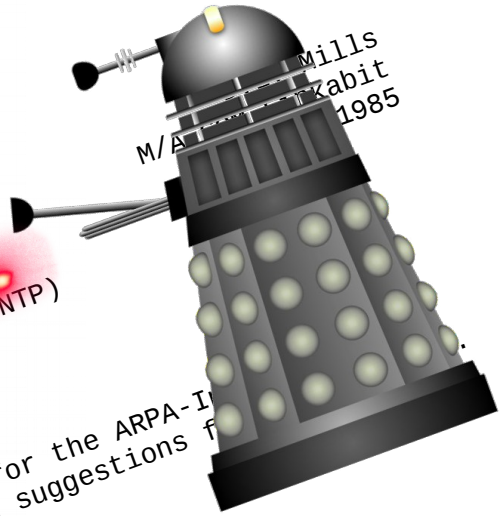
Network Time Protocol (NTP), a protocol
network clocks using a set of distribut
ilt on the User Datagram Protocol
connectionless transport mechanism.
the ICMP Timestamp mes

Domain Name System



NTP Weaknesses





Protocol (NTP)

sed protocol for the ARPA-I
sion and suggestions f
ted.

Mills
Kabit
1985

Attacking NTP's Authenticated Broadcast

Aanchal Malhotra
Boston University
aanchal4@bu.edu

Sharon Goldberg
Boston University
goldbe@cs.bu.edu

ACT

two attacks on the Network Time Protocol (NTP)'s
ically-authenticated broadcast mode. First, we
lay attack that allows an on-path attacker to
ck a broadcast client to a specific time. Sec-
t a denial-of-service (DoS) attack that al-
attacker to prevent a broadcast client from
s system clock; to do this, the attacker
single malformed broadcast packet per
r DoS attack also applies to all other
e 'ephemeral' or 'preemptable' (includ-
etc). We then use network measure-
ce that NTP's broadcast and other
e modes are being used in the
ing why NTP's current
cryptographic
adcast

mended by the NTP specification [11] and requ
open-source NTP reference implementation *ntpd*,
provide sufficient protection against attacks on
mode. We consider both (1) on-path attacks, whe
tacker occupies a privileged position on the path
NTP client and one of its servers, and (2) off-pat
where the attacker can be anywhere on the
not observe the traffic between clien
We present an on-path
broadcast mode (CVE
to get stuck at
denial-of

NTP Weaknesses

[1] Attacking the Network Time Protocol.

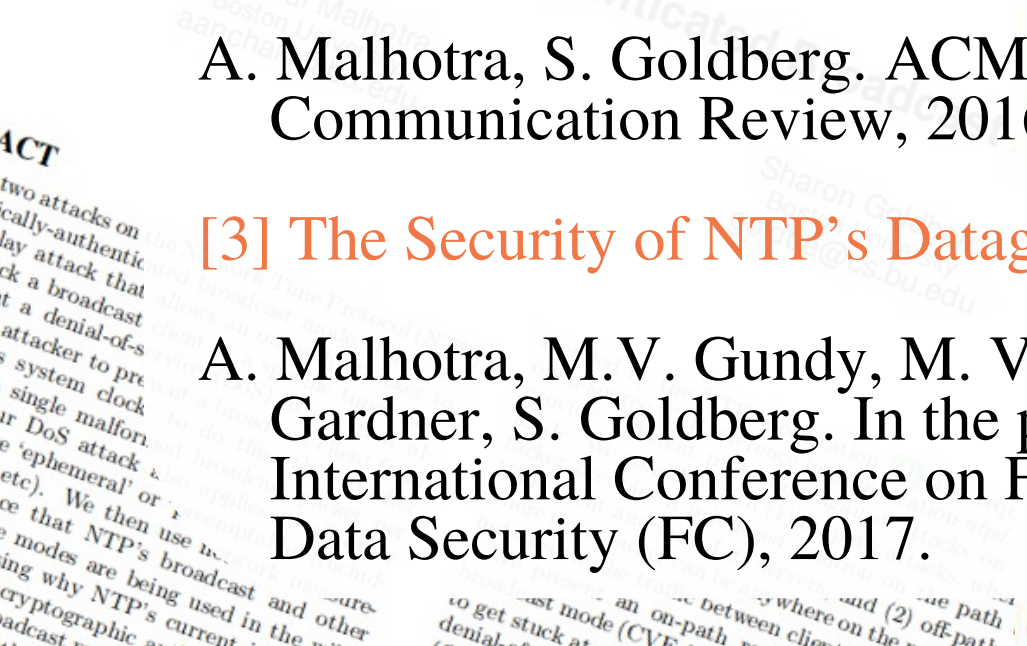
A. Malhotra, I. Cohen, E. Brakke, S. Goldberg. In the proceedings of The Network & Distributed System Security Symposium (NDSS), CA, 2016.

[2] Attacking NTP's Authenticated Broadcast Mode.

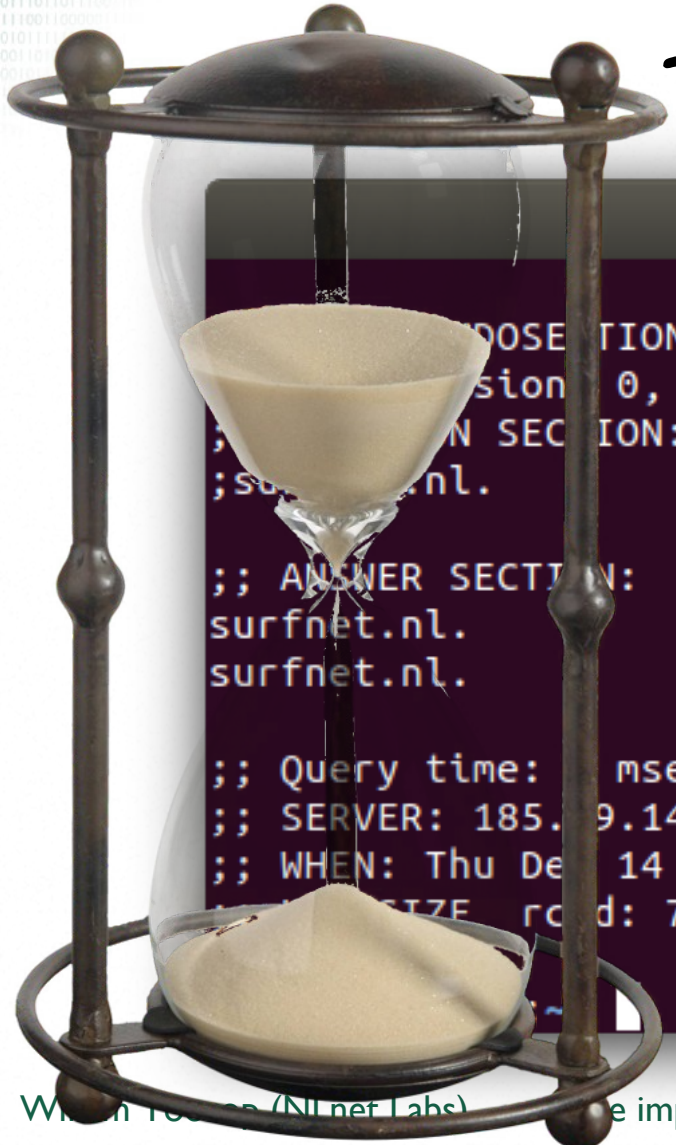
A. Malhotra, S. Goldberg. ACM SIGCOMM, Computer Communication Review, 2016.

[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.



How does DNS depend on time?



TTL (TIME TO LIVE) = TIME SPAN

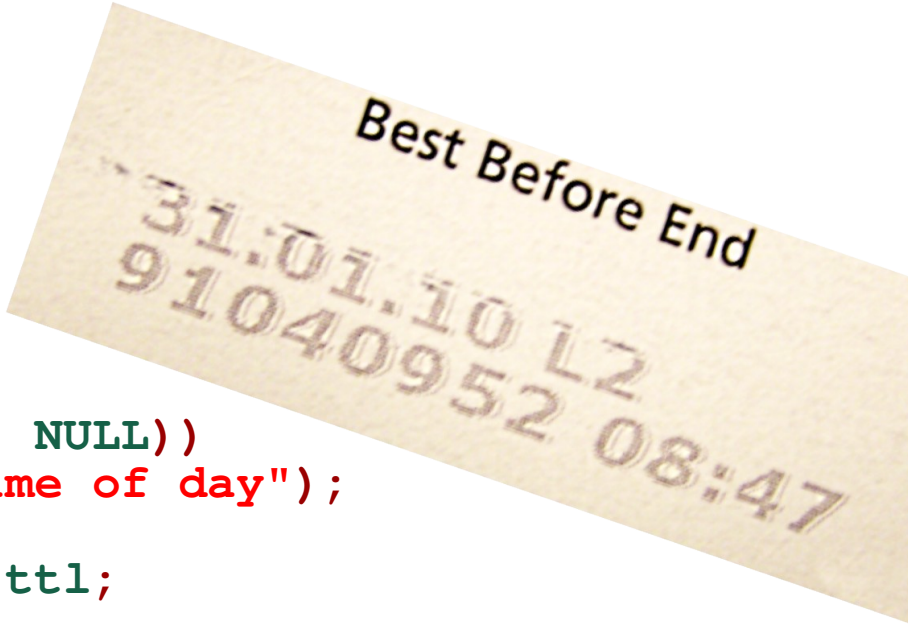
```
willem@makaak: ~
                                    IN      A
;; ANSWER SECTION:
surfnet.nl.             356     IN      A       192.87.108.15
surfnet.nl.             356     IN      A       145.100.190.243

;; Query time:  msec
;; SERVER: 185. 9.140.100#53(185.49.140.100)
;; WHEN: Thu De  14 11:59:10 CET 2017
;;  d: 71
```

How do software implementations deal with time spans?


```
struct RRset_t {
        uint8_t          dname;
        uint16_t         rrtype;
        uint16_t         rrclass;
        struct timeval   expiry;
        void            *rdata[];
};

if (gettimeofday(&rrset->expiry, NULL))
        perror("Could not get time of day");
else
        rrset->expiry.tv_sec += ttl;
```

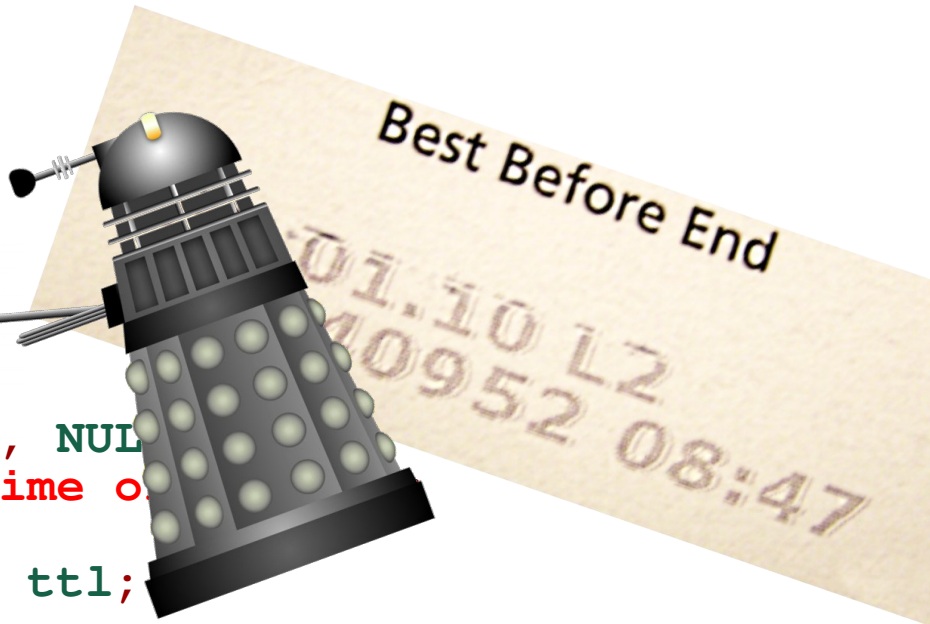


How do software implementations deal with time spans?

TIME SPAN TRANSLATED TO TIME STAMP
FROM SYSTEM TIME ← UPDATED BY NTP

```
struct RRset_t {
        uint8_t          dname;
        uint16_t         rrtype;
        uint16_t         rrclass;
        struct timeval   expiry;
        void            *rdata[];
};

if (gettimeofday(&rrset->expiry, NUL
        perror("Could not get time o
else
        rrset->expiry.tv_sec += ttl;
```



Why is this bad?

TIME SPAN TRANSLATED TO TIME STAMP
FROM SYSTEM TIME ← UPDATED BY NTP

- NTP vulnerabilities [1, 2, 3] can be leveraged for off-path attacks on DNS cache:
  - Cache-expiration attack (Time shifted forward)
  - Cache-sticking attack (Time shifted backwards)

Recommendation

- Not a protocol problem 
- Deal with implementations ONLY!

```
struct RRset_t {
        uint8_t          dname;
        uint16_t         rrtype;
        uint16_t         rrclass;
        struct timespec  expiry;
        void            *rdata[];
};

if (clock_gettime(CLOCK_MONOTONIC_RAW, &rrset->expiry))
        perror("Could not get time of day");
else
        rrset->expiry.tv_sec += ttl;
```

- Unspecified starting point
- Monotonically increasing
- not subject to NTP adjustments
- or by adjustments from adjtime

draft-aanchal-time-implementation-guidance

Recommendation

- Not a protocol problem
- Deal with implementation ONLY!

Terminology

A CLOCK IS A FUNCTION THAT MAPS TIME TO A CLOCK TIME VALUE

USE RAW CLOCK TIME STAMP INSTEAD OF REAL CLOCK TIME STAMP

draft-aanchal-time-implementation-guidance

DNSSEC


Certificate of Authenticity
Let it be known
that this guitar was handmade by
Lynn Ellsworth and Patrick Coleman of
Lynn Ellsworth Guitars LLC in 2014.
This particular guitar is the very first Les Paul style guitar fro
Relic Master Series.
The single cutaway Les Paul style body is made fr
weathered Redwood. The hardware is black with
bridge pickup is a Seymour Duncan Quarter P
bridge. The neck pickup is a DiMarzio Red
Gibson with a Rosewood fing
LYNN ELLSWORTH

How does DNSSEC depend on time?

```
willem@makaak: ~
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;surfnet.nl.                    IN A

;; ANSWER SECTION:
surfnet.nl.             781 IN A 145.100.190.243
surfnet.nl.             781 IN A 192.87.108.15
surfnet.nl.             781 IN RRSIG A 8 2 [illegible] (
                                20171227234559 20171213113957 36919 surfnet.nl.
                                P8j[illegible]YSWX[illegible]qtJ9j07oA/Y9y0mYLv
                                [illegible]dkvQ4flqlsgB[illegible]S/Q3Vb4bEmhsXJ5SeKgIAhMW7E9c
                                Ozy30JrVERWz[illegible]m/U5lv4+Mfvk0iQfo/1dRfUYsac23ey
                                Mi9oAoZ627[illegible]en3O9aHgH91x3g+5HR5ML4L/DNOE= )
```

EXPIRATION & INCEPTION
AS WALL CLOCK
TIME STAMPS

How do software implementations deal with wall clock time stamps?


```
struct timeval now;

if (gettimeofday(&now, NULL))
        perror("Could not get time of day");

else if (now < rrset->rrsig.inception)
        verify_error("Not yet valid");

else if (now > rrset->rrsig.expiration)
        verify_error("Not valid anymore");
```

Recommendation

- Fundamental problem with the protocol 
- Have to use real clock time (i.e. system time)

The only solution

- Fix Network Time Protocols 

draft-aanchal-time-implementation-guidance

Recommendation

- Fundamental problem with the protocol 
- Have to use real clock time (i.e. system time)

The only solution

- Fix Network Time Protocols 

Impact?

- Denial of Service attacks
- Disable DNSSEC by shifting before 15 July 2010

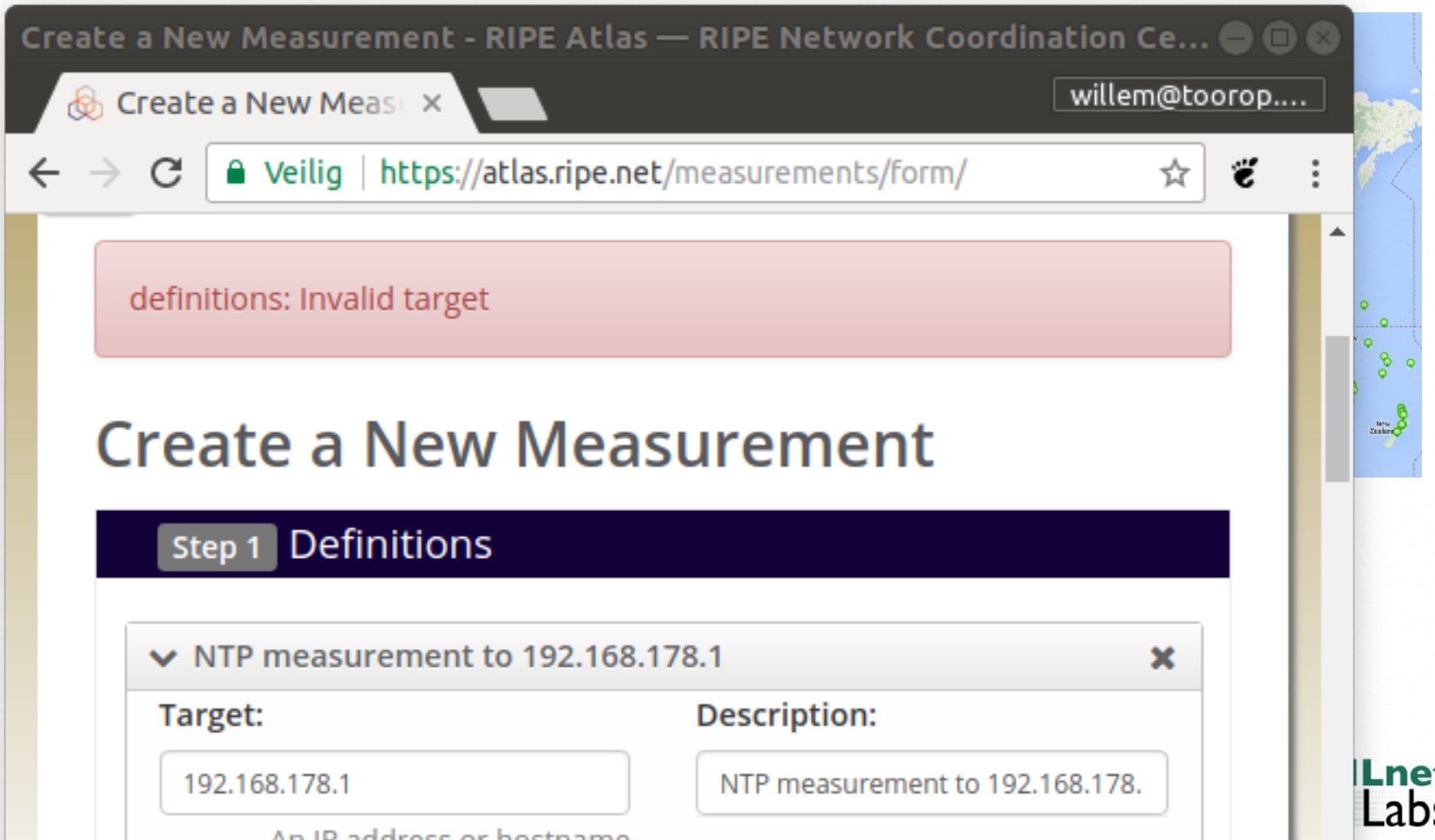
draft-aanchal-time-implementation-guidance

Measure the attack surface RIPE ATLAS

- Which resolvers run NTP?
  Target probe's resolvers (DHCP?)

Measure the attack surface
RIPE ATLAS

- Which resolvers run NTP?



Measure the attack surface
RIPE ATLAS

- Which resolvers run NTP? Target probe's resolvers (DHCP?)
- Target resolvers with public IPs +
- Try to discover IPs


```
willem@makaak: ~
willem@makaak:~$ dig o-o.myaddr.l.google.com. TXT +short
"62.216.31.207"
willem@makaak:~$ dig whoami.akamai.net A +short
194.109.133.206
willem@makaak:~$
```

Measure the attack surface
RIPE ATLAS

Measurements don from 21 till 27 October 2017

	# resolvers	
Total	+- 18500	on 10320 probes
With public IP resolvers	8244	on 4594 probes

Answering NTP time queries	2021	(24.5%)
Answering NTP control queries from public internet	75	
Answering NTP control queries from NLNOG RING node from same ASN	26	
Total answering NTP control queries	**101**	**(1.23%)**

Measure the attack surface
Open Resolvers

From August 2017 list of the Open Resolver Project

	# resolvers	
Total	16.5M	
Targeted	6.5M	
Still answering DNS queries (Nov 2017)	2.3M	
Answered REFUSED (authoritatives)	1.7M	

Open resolvers	600K	
Answering NTP queries	3.7%	24.5% on ATLAS
Answering NTP control queries	**0.93%**	1.23% on ATLAS

De impact of NTP security weaknesses on DNS(SEC)

- Sophisticated attacks possible
- Script-kiddie attacks less so
  (DOS of DNSSEC resolvers)
- Attack surface around 1% of resolvers

- Software takes a common approach towards (wall/real) clock time stamps and time spans
- Not just RRset TTLs (also network timeouts etc.)

draft-aanchal-time-implementation-guidance