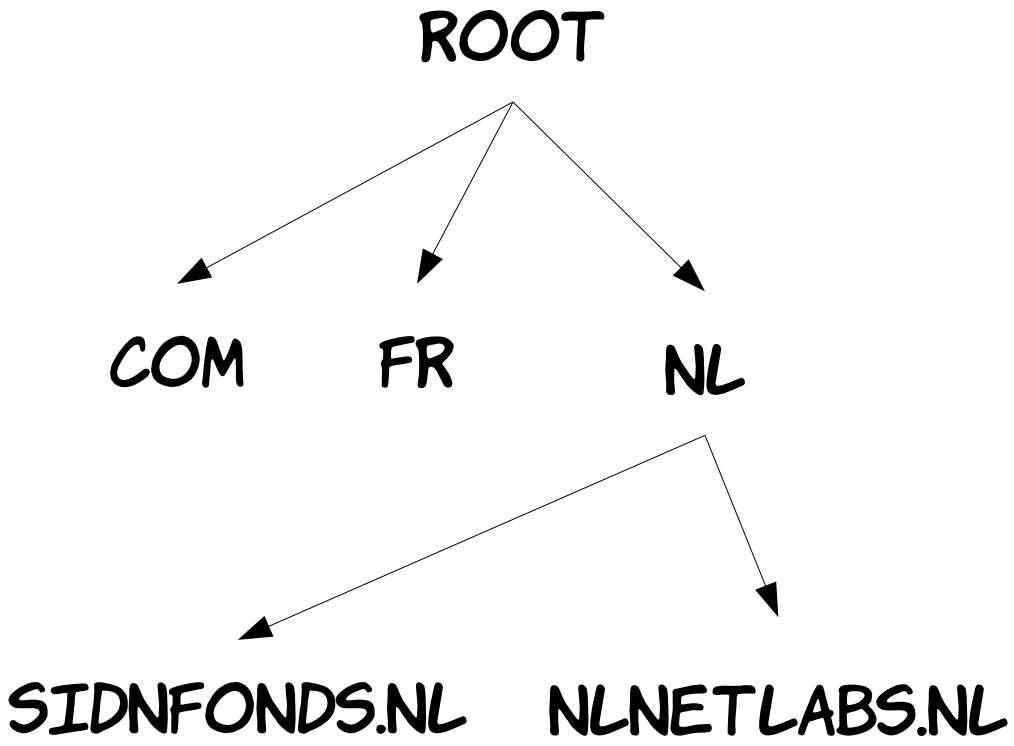
De impact van NTP security tekortkomingen op DNS(SEC)

Willem Toorop
NLnet Labs

SIDNfonds Startbijeenkomt call 1 2017

Domain Name System



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

DNSSEC

Total number of secure delegations: 7375455

Zone	DNSSEC	NSEC(3)	Signed
nl.	true	NSEC3	2618262
com.br	true	NSEC3	771183
cz.	true	NSEC3	638970
se	true	NSEC	607290
com.	true	NSEC3	588136
no.	true	NSEC3	431968
eu.	true	NSEC3	365356
fr.	true	NSEC3	337751
be.	true	NSEC3	132395
net.	true	NSEC3	113548
hu.	true	NSEC3	111436

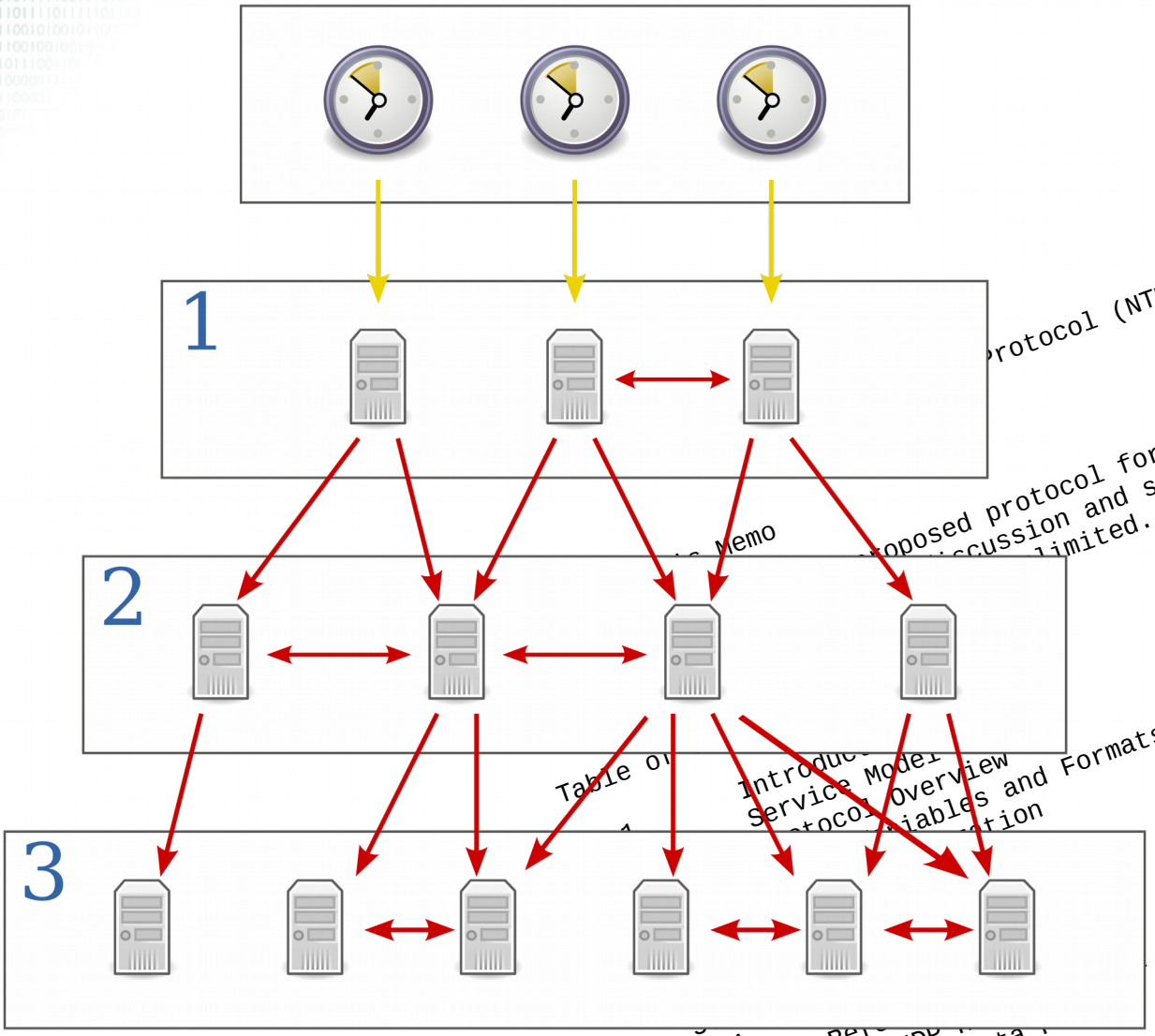
DNSSEC


Certificate of Authenticity
Let it be known
that this guitar was handmade by
Lynn Ellsworth and Patrick Coleman of
Lynn Ellsworth Gui
SLC in 2014.
This particular guitar is the very
guitar fro
Relic
The single cutaway Les Paul s
weathered Redwood. The hardw
bridge pickup is a Seymour Du
bridge. The neck pickup is a D
Gibson wi
Tenminste houdbaar tot :
22/04/2015
L221 12:42

DNSSEC


Certificate of Authenticity
Let it be known
that this guitar was handmade by
Lynn Ellsworth and Patrick Coleman of
Lynn Ellsworth Gui
LLC in 2014.
This particula
the very
guitar fro
Tenminste houdbaar tot :
22/04/2015
221 12:42

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

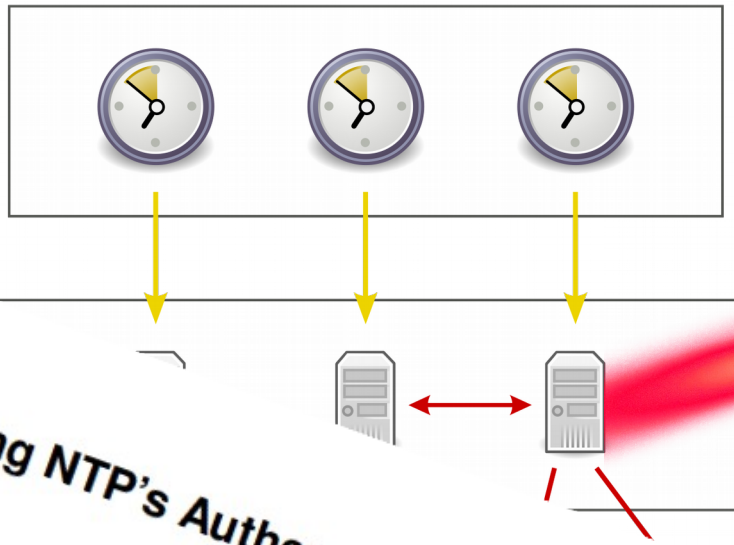
Table of

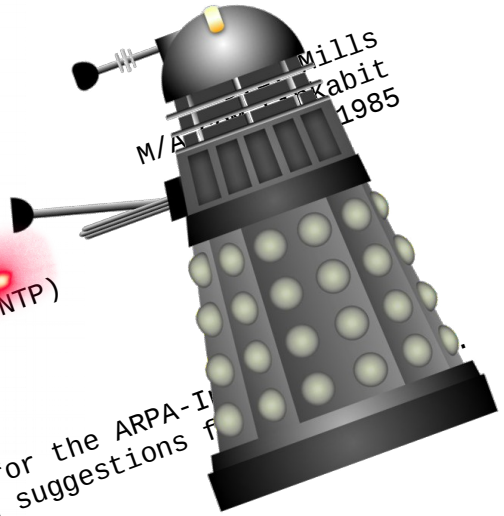
Introduction
Service Model
Protocol Overview
Variables and Formats
Operation

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

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

Network Time Protocol





Protocol (NTP)

Mills
Kabit
1985

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

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

De impact van NTP security tekortkomingen op DNS(SEC)

- WAT ZIJN DE KWETSBAARHEID VAN DNS / DNSSEC IMPLEMENTATIES VOOR TIMINGAANVALLEN?
- WAT ZIJN DE AFHANKELIJKHEID VAN HET NEDERLANDSE DNS-ECOSYSTEEM VAN DOOR NTP VERKREGEN TIJD?
- WAT ZIJN DE DAARDOOR INHERENTE KWETSBAARHEID VOOR NTP-ATTACKS?