ENOG– June 2021

Network Time Security (NTS)

The Road to Deployment

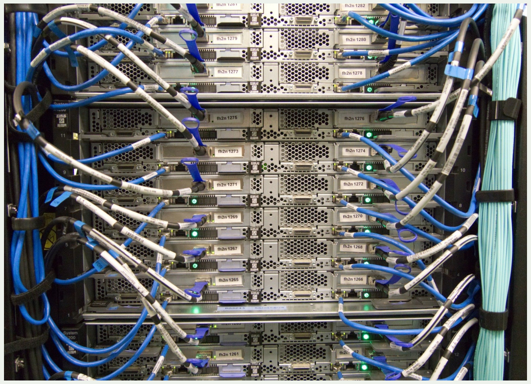
Internet Society

Karen O'Donoghue
Director, Internet Trust Technology
odonoghue@isoc.org

Humans have always measured time…

©Marilyn Shea, 2004

Accurate time is vitally important.

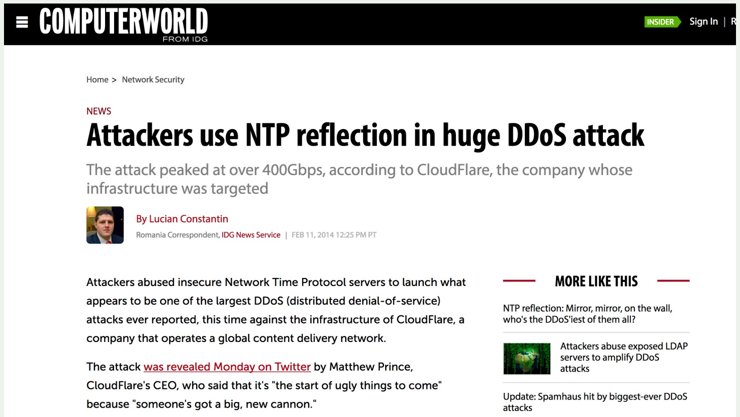


Time ⟷ Security

Security has not been a high priority of the network time synchronization community in the past…

- What has changed...
  - Increasing interconnection and decentralization
  - Increasing evidence of the impact of inadequate security
  - Interdependency between security and time
  - Legal and Compliance requirements

Attacks are occurring…



Home > Network Security

NEWS

Attackers use NTP reflection in huge DDoS attack

The attack peaked at over 400Gbps, according to CloudFlare, the company whose infrastructure was targeted

By Lucian Constantin
Romania Correspondent, IDG News Service | FEB 11, 2014 12:25 PM PT

Attackers abused insecure Network Time Protocol servers to launch what appears to be one of the largest DDoS (distributed denial-of-service) attacks ever reported, this time against the infrastructure of CloudFlare, a company that operates a global content delivery network.

The attack was revealed Monday on Twitter by Matthew Prince, CloudFlare's CEO, who said that it's "the start of ugly things to come" because "someone's got a big, new cannon."

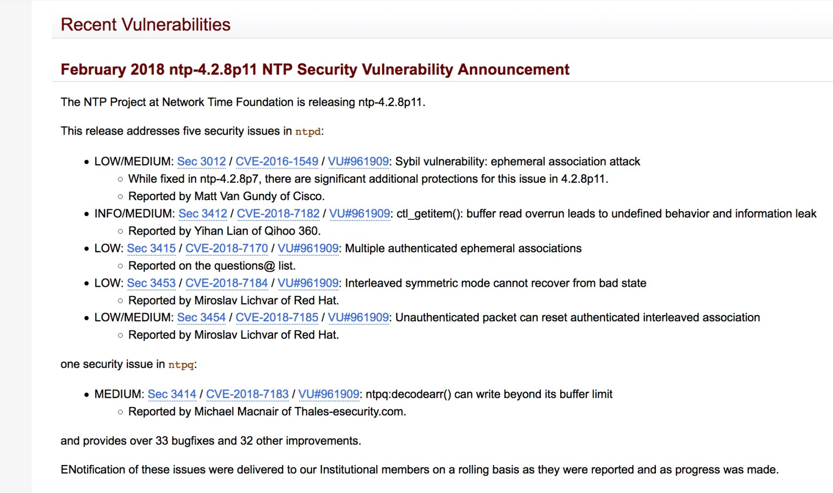
MORE LIKE THIS

NTP reflection: Mirror, mirror, on the wall, who's the DDoS'iest of them all?

Attackers abuse exposed LDAP servers to amplify DDoS attacks

Update: Spamhaus hit by biggest-ever DDoS attacks

Vulnerabilities are being discovered…



Recent Vulnerabilities

February 2018 ntp-4.2.8p11 NTP Security Vulnerability Announcement

The NTP Project at Network Time Foundation is releasing ntp-4.2.8p11.

This release addresses five security issues in `ntpd`:

- LOW/MEDIUM: Sec 3012 / CVE-2016-1549 / VU#961909: Sybil vulnerability: ephemeral association attack
  - While fixed in ntp-4.2.8p7, there are significant additional protections for this issue in 4.2.8p11.
  - Reported by Matt Van Gundy of Cisco.
- INFO/MEDIUM: Sec 3412 / CVE-2018-7182 / VU#961909: ctl_getitem(): buffer read overrun leads to undefined behavior and information leak
  - Reported by Yihan Lian of Qihoo 360.
- LOW: Sec 3415 / CVE-2018-7170 / VU#961909: Multiple authenticated ephemeral associations
  - Reported on the questions@ list.
- LOW: Sec 3453 / CVE-2018-7184 / VU#961909: Interleaved symmetric mode cannot recover from bad state
  - Reported by Miroslav Lichvar of Red Hat.
- LOW/MEDIUM: Sec 3454 / CVE-2018-7185 / VU#961909: Unauthenticated packet can reset authenticated interleaved association
  - Reported by Miroslav Lichvar of Red Hat.

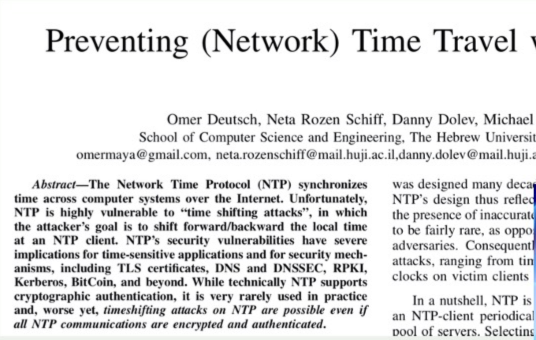
one security issue in `ntpq`:

- MEDIUM: Sec 3414 / CVE-2018-7183 / VU#961909: ntpq:decodearr() can write beyond its buffer limit
  - Reported by Michael Macnair of Thales-esecurity.com.

and provides over 33 bugfixes and 32 other improvements.

ENotification of these issues were delivered to our Institutional members on a rolling basis as they were reported and as progress was made.

Research is happening…



Preventing (Network) Time Travel with Chronos

Omer Deutsch, Neta Rozen Schiff, Danny Dolev, Michael Schapira
School of Computer Science and Engineering, The Hebrew University of Jerusalem
omermaya@gmail.com, neta.rozenschiff@mail.huji.ac.il,danny.dolev@mail.huji.ac.il, schapiram@huji.ac.il

Abstract*—The Network Time Protocol (NTP) synchronizes time across computer systems over the Internet. Unfortunately, NTP is highly vulnerable to "time shifting attacks", in which the attacker's goal is to shift forward/backward the local time at an NTP client. NTP's security vulnerabilities have severe implications for time-sensitive applications and for security mechanisms, including TLS certificates, DNS and DNSSEC, RPKI, Kerberos, BitCoin, and beyond. While technically NTP supports cryptographic authentication, it is very rarely used in practice and, worse yet, *timeshifting attacks on NTP are possible even if all NTP communications are encrypted and authenticated.

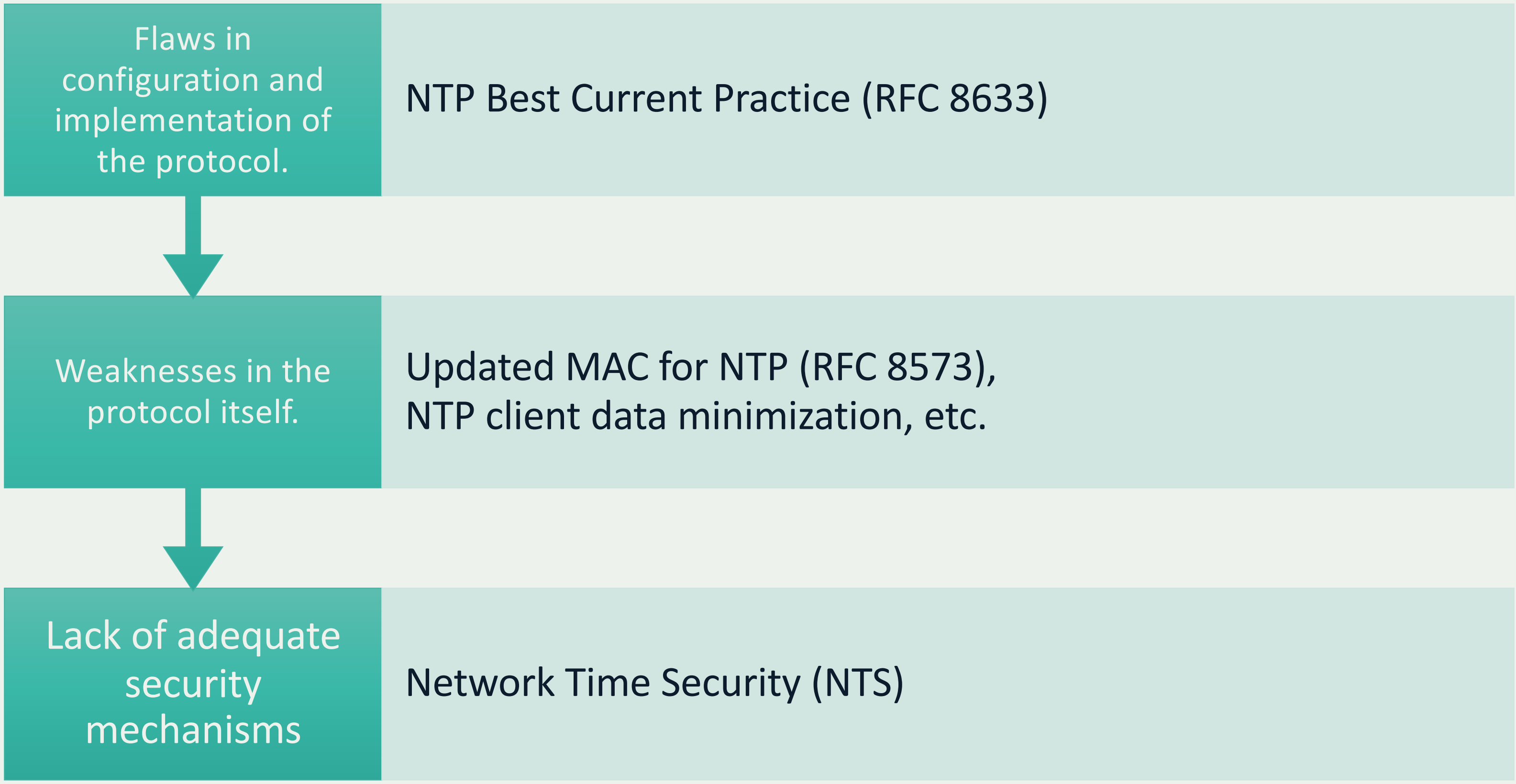
was designed many decad
NTP's design thus reflec
the presence of inaccurat
to be fairly rare, as oppo
adversaries. Consequent
attacks, ranging from tin
clocks on victim clients

In a nutshell, NTP is
an NTP-client periodical
pool of servers. Selecting

Paper from NDSS 2018. (https://www.ndss-symposium.org/ndss2018/programme/#02A

Image courtesy of Wes Hardaker

IETF approach to the problem…



Flaws in configuration and implementation of the protocol.

NTP Best Current Practice (RFC 8633)

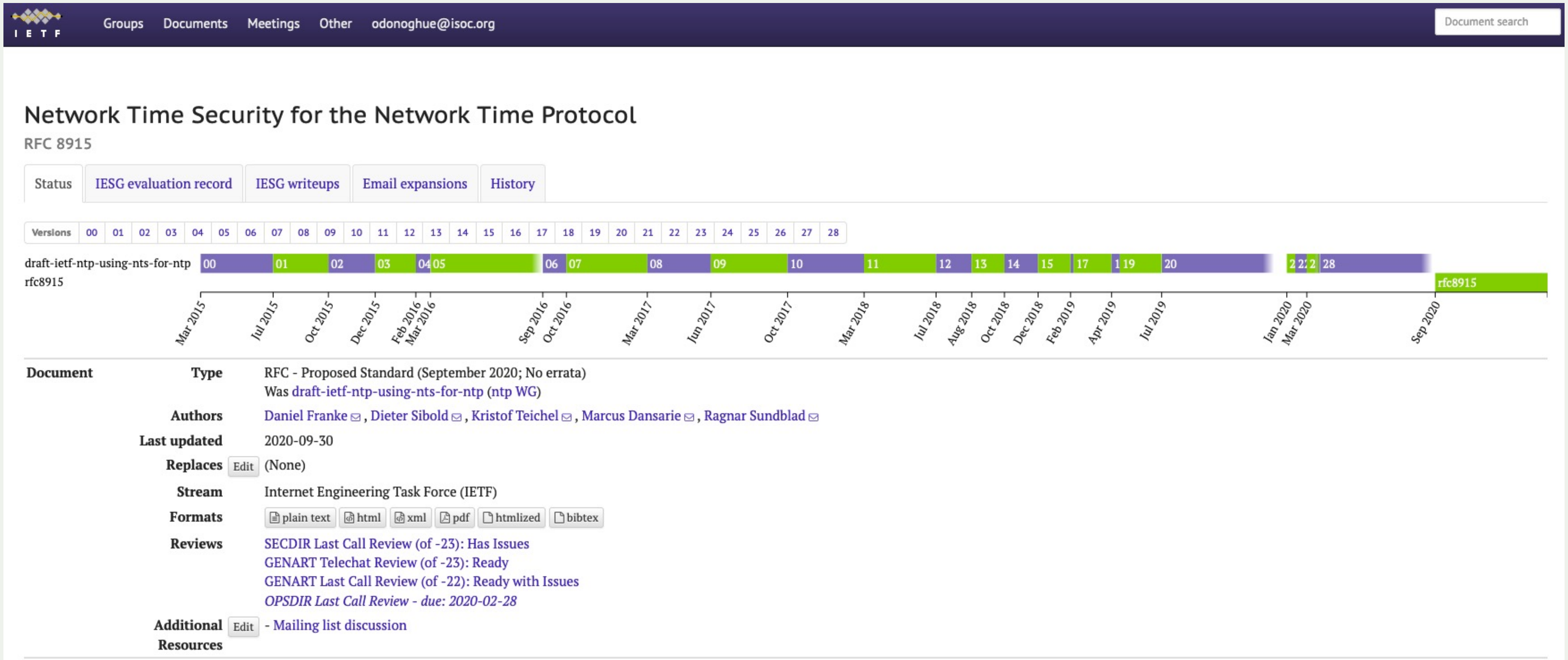
Weaknesses in the protocol itself.

Updated MAC for NTP (RFC 8573),
NTP client data minimization, etc.

Lack of adequate security mechanisms

Network Time Security (NTS)

Network Time Security (NTS)



Network Time Security for the Network Time Protocol

RFC 8915

Document	**Type**	RFC - Proposed Standard (September 2020; No errata) Was draft-ietf-ntp-using-nts-for-ntp (ntp WG)
	Authors	Daniel Franke ✉ , Dieter Sibold ✉ , Kristof Teichel ✉ , Marcus Dansarie ✉ , Ragnar Sundblad ✉
	Last updated	2020-09-30
	Replaces Edit	(None)
	Stream	Internet Engineering Task Force (IETF)
	Formats	plain text html xml pdf htmlized bibtex
	Reviews	SECDIR Last Call Review (of -23): Has Issues GENART Telechat Review (of -23): Ready GENART Last Call Review (of -22): Ready with Issues *OPSDIR Last Call Review - due: 2020-02-28*
	Additional Resources Edit	- Mailing list discussion

Network Time Security (NTS)

NTS provides:

- Integrity for NTP packets
- Unlinkability (once an NTS session has been established and if the client uses data minimization techniques)
- Request-Response consistency (for avoiding replay attacks)
- Authentication of servers
- Authorization of clients (optionally)
- Support for NTP client-server mode only

NTS includes:

- NTS Key Establishment protocol (NTS-KE)
  - TLS to establish key material and negotiate some additional protocol options
- NTS extensions for NTPv4
  - A collection of NTP extension fields for cryptographically securing NTPv4 using key material previously negotiated using NTS-KE.
  - Suitable for client/server mode

Basic phases of NTS secured NTP

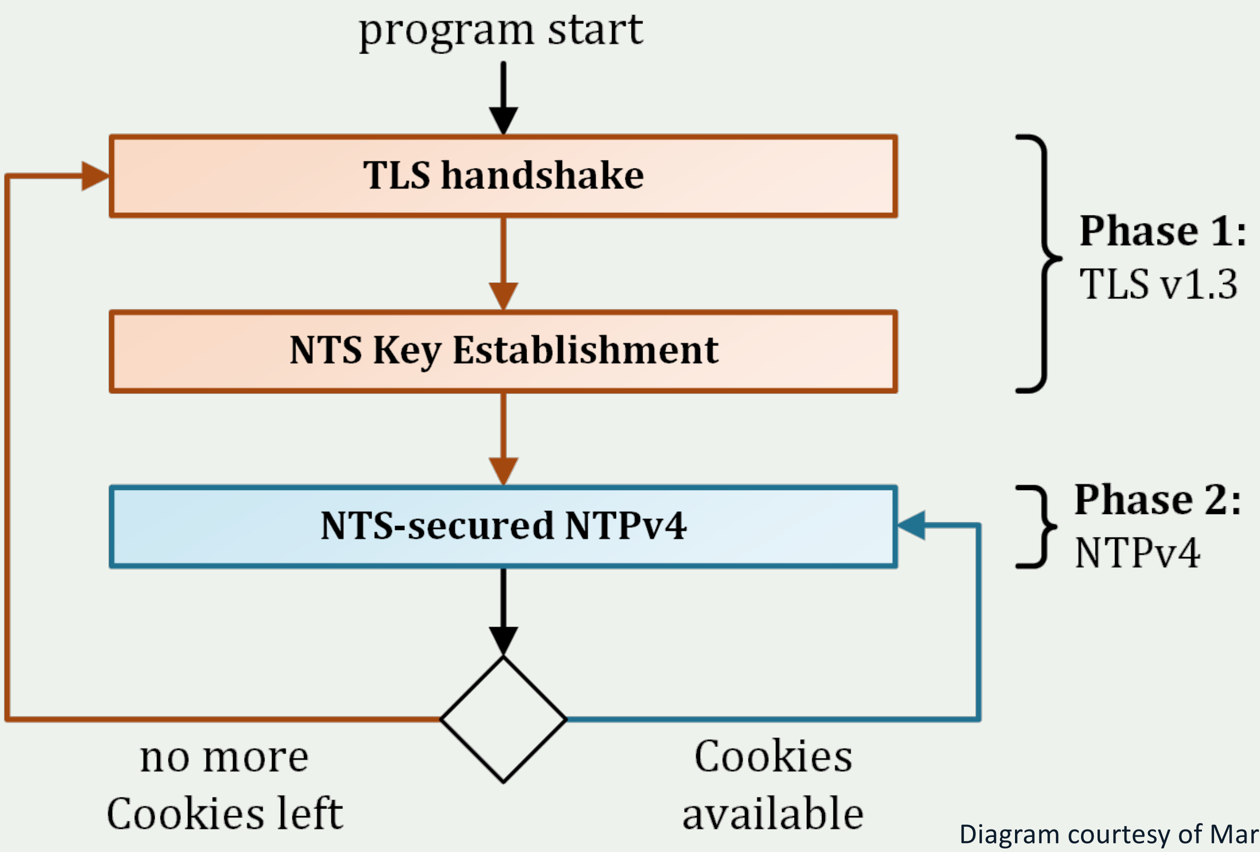


Diagram courtesy of Martin Langer, Ph.D. student, Ostfalia University of Applied Sciences, Germany.

NTS secured NTP system components

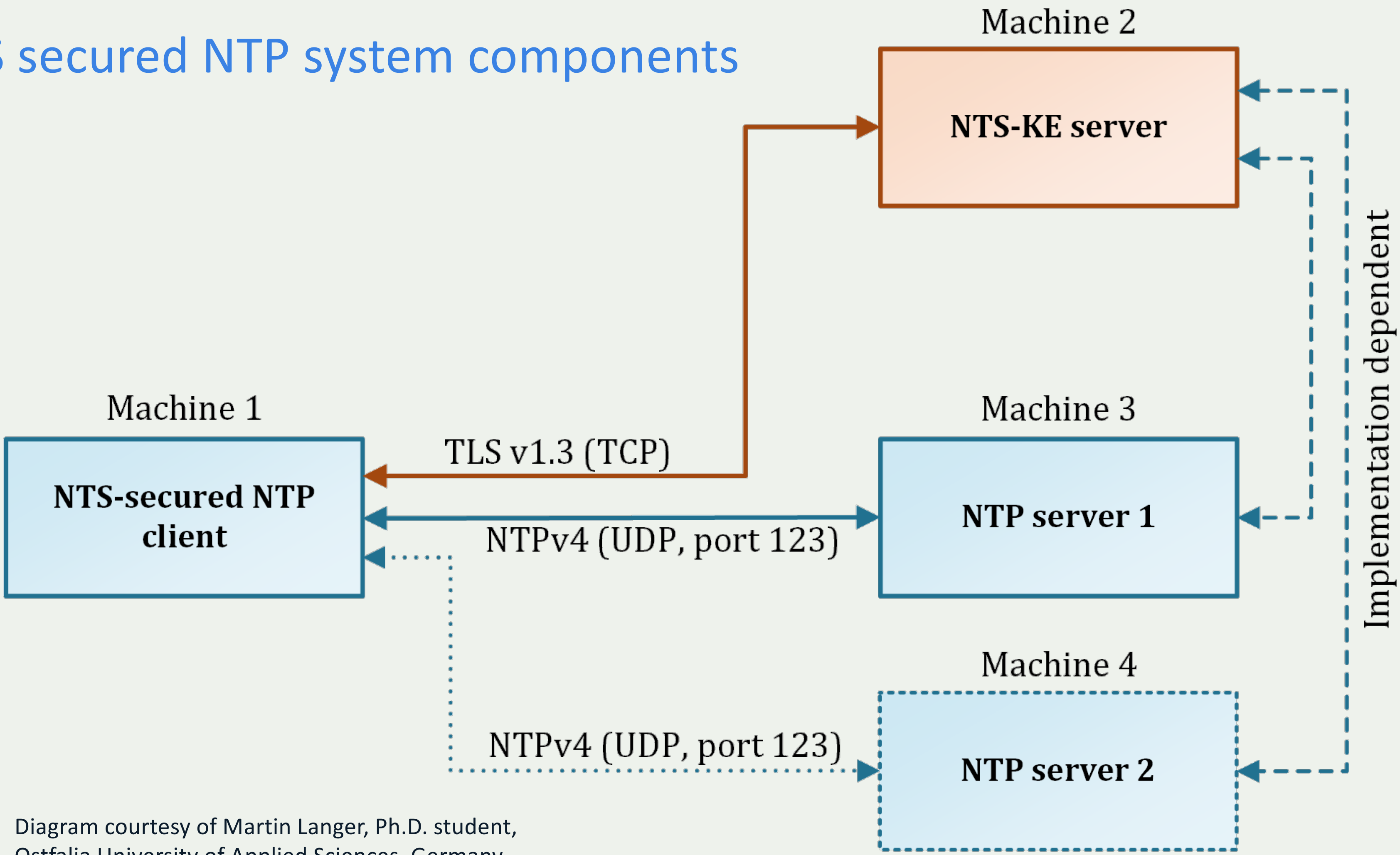


Diagram courtesy of Martin Langer, Ph.D. student,
Ostfalia University of Applied Sciences, Germany.

NTS Key Exchange phase

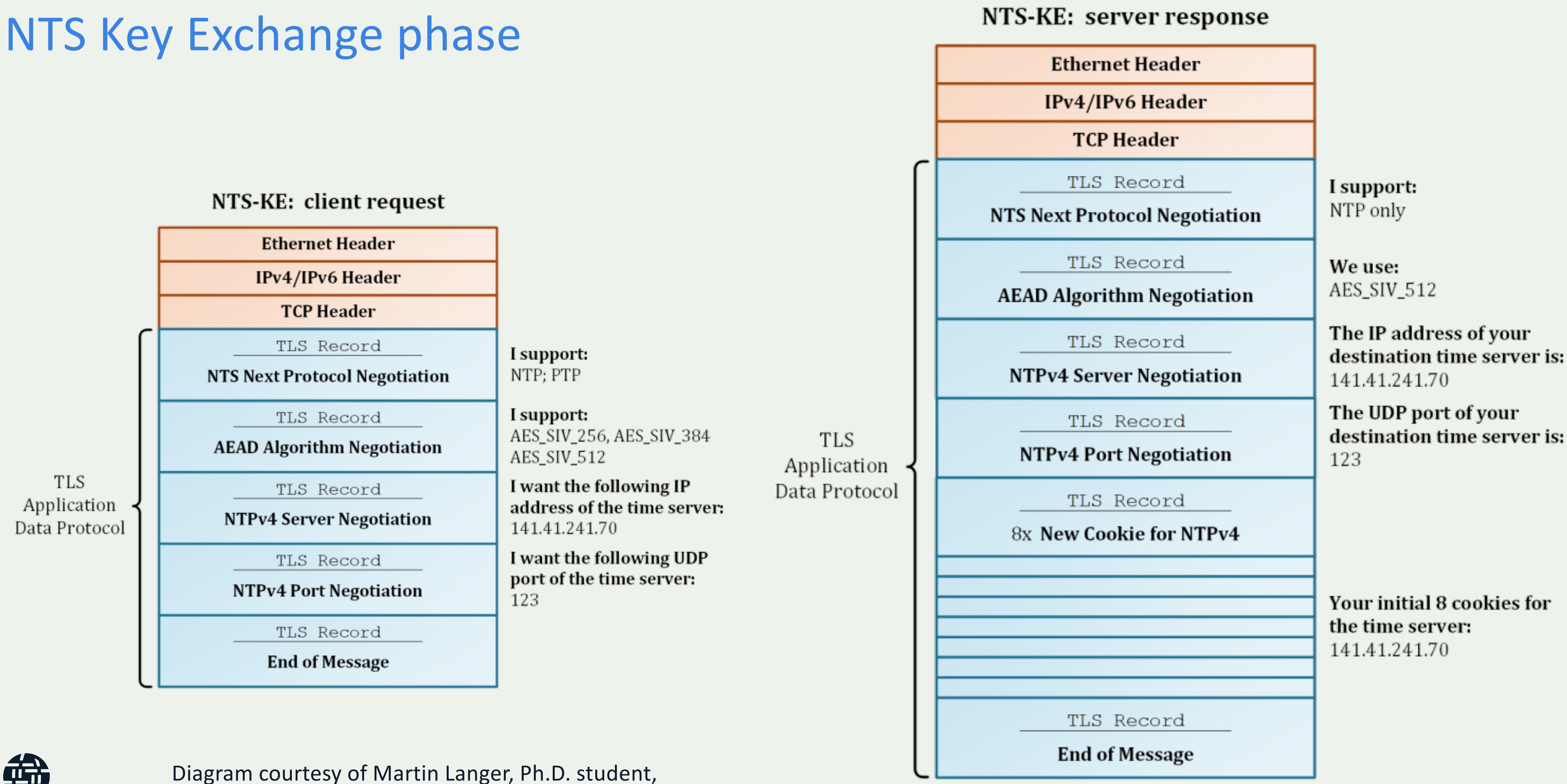


Diagram courtesy of Martin Langer, Ph.D. student,
Ostfalia University of Applied Sciences, Germany.

NTS Extension Fields for NTP

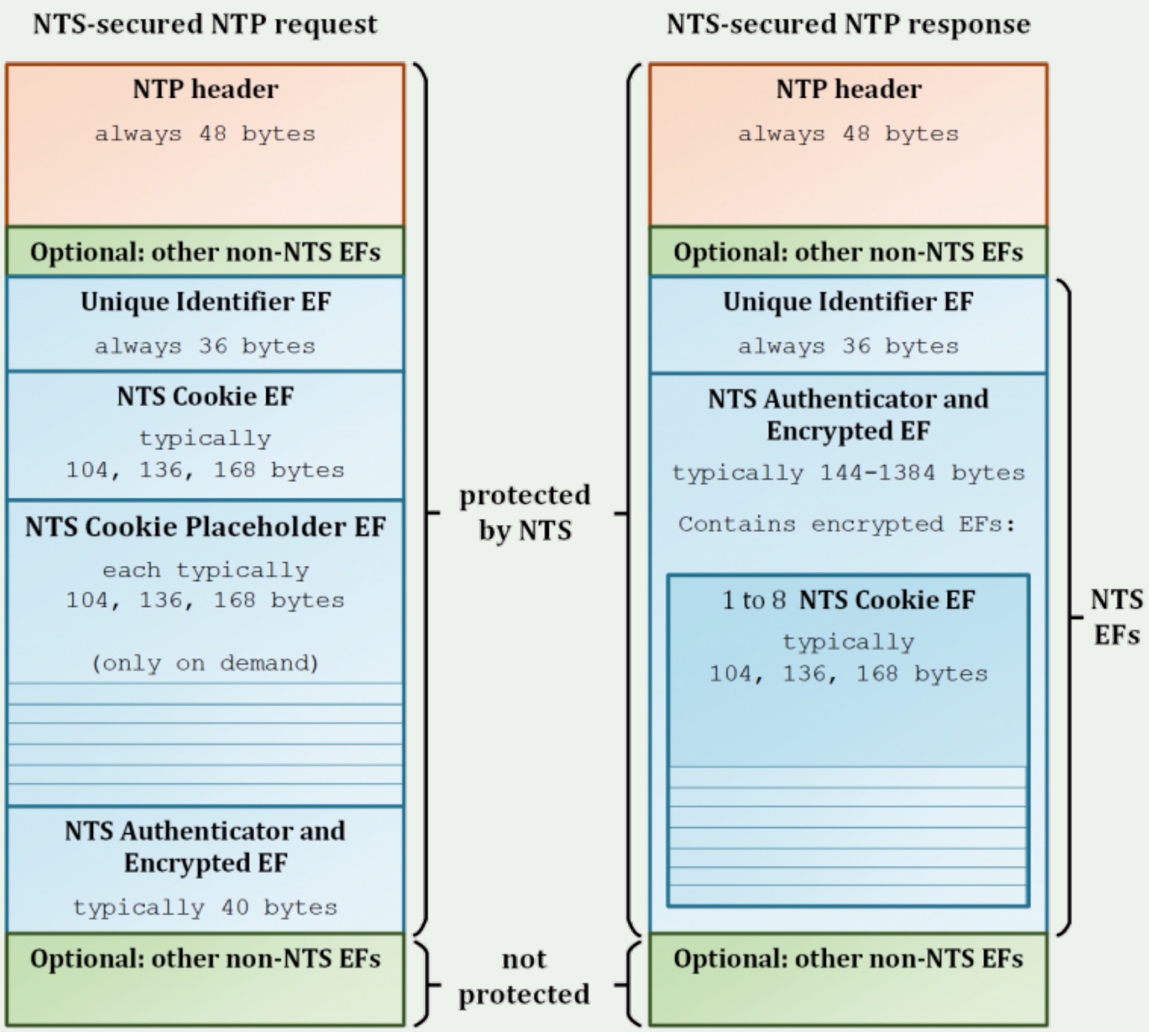
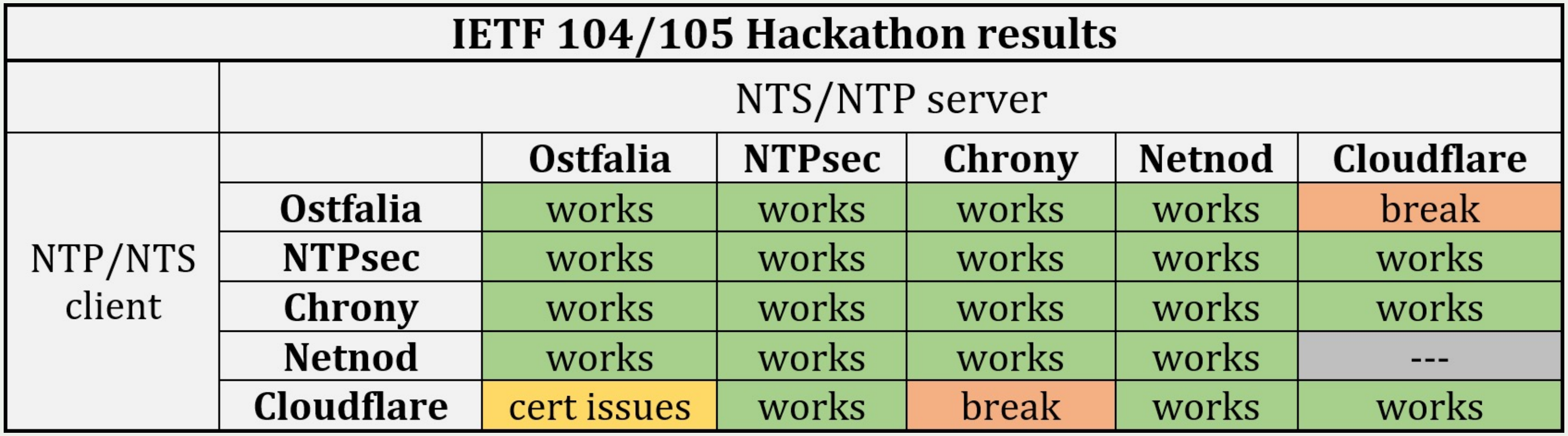


Diagram courtesy of Martin Langer, Ph.D. student, Ostfalia University of Applied Sciences, Germany.

Recent basic interoperability testing



IETF 104/105 Hackathon results						
	NTS/NTP server					
		Ostfalia	**NTPsec**	**Chrony**	**Netnod**	**Cloudflare**
NTP/NTS client	**Ostfalia**	works	works	works	works	break
	NTPsec	works	works	works	works	works
	Chrony	works	works	works	works	works
	Netnod	works	works	works	works	---
	Cloudflare	cert issues	works	break	works	works

Note: This table represents the results of two specific test event and may not reflect current operational status.

It’s time to focus on the road to deployment…

Steps on the road to NTS deployment

- Technology / Standards Development
- Preliminary / Prototype Implementations
- Interoperability Testing
- Production quality open source implementations
- Commercial products
- Tools for testing and troubleshooting
- Preliminary deployments
- Lessons Learned and Best Practices
- Large scale deployments

Building a community

- Network operators
- Time service providers
- Enterprise IT groups

Maturing the NTS products

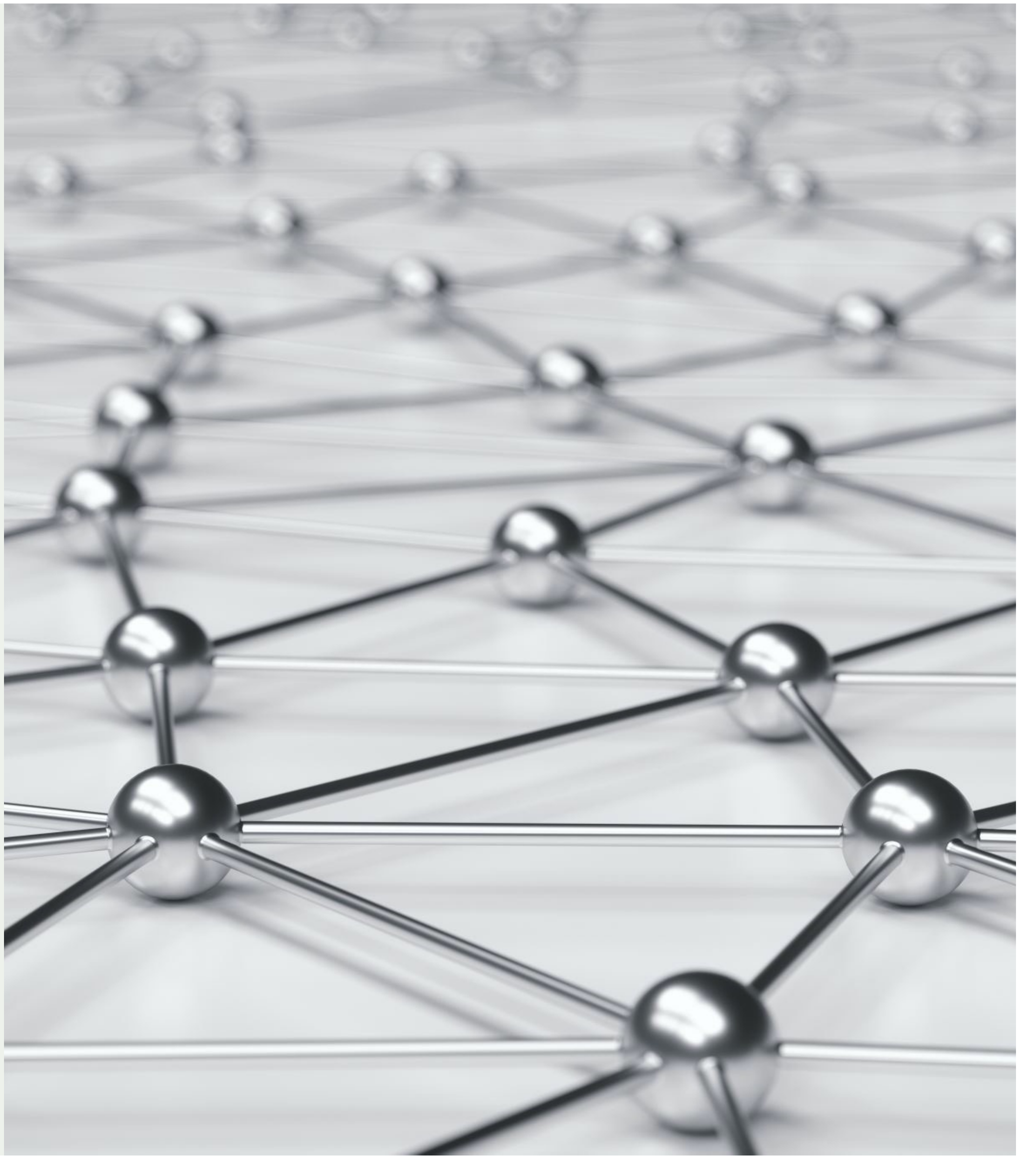
- Distributed multi-party testbed
- Virtual test events
- Test and measurement tools

Developing NTS deployment guidance

- Lessons Learned and BCPs
- Monitoring Tools

Expanding NTS deployment

- Training
- Resources



It is Time to Act!

- The NTS for NTP specification is published.
- Discussions are underway in IEEE 1588 to specify portions of NTS for PTP.
- Open source implementations and testing are underway.
- It is time to build solutions, test deployments, and gather lessons learned.

Resources

NTP Working Group

- https://datatracker.ietf.org/group/ntp/about/

NTS Specification

- https://www.rfc-editor.org/info/rfc8915

NTS enabled NTP services

- Netnod (https://www.netnod.se/time-and-frequency/network-time-security)
- Cloudflare https://www.cloudflare.com/time/

Open Source NTS implementation

- Chrony (https://chrony.tuxfamily.org/index.html)

Recent NTS Blog Posts:

- https://fedoramagazine.org/secure-ntp-with-nts/
- https://weberblog.net/network-time-security-new-ntp-authentication-mechanism/
- https://www.netnod.se/time-and-frequency/how-to-use-nts
- https://blog.cloudflare.com/secure-time/

Thank you.

Karen O’Donoghue

Director, Internet Trust Technology

odonoghue@isoc.org

Rue Vallin 2
CH-1201 Geneva
Switzerland

11710 Plaza America Drive
Suite 400
Reston, VA 20190, USA

Rambla Republica de Mexico 6125
11000 Montevideo,
Uruguay

66 Centrepoint Drive
Nepean, Ontario, K2G 6J5
Canada

Science Park 400
1098 XH Amsterdam
Netherlands

3 Temasek Avenue, Level 21
Centennial Tower
Singapore 039190

internetsociety.org
@internetsociety