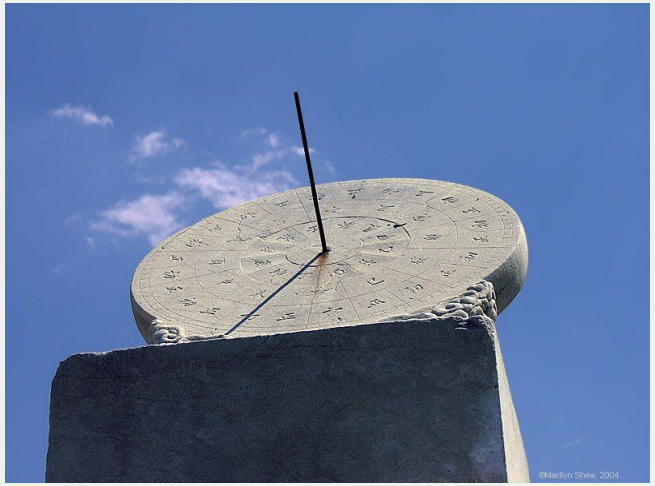
LACNIC – 6 May 2020

# Network Time Security (NTS)

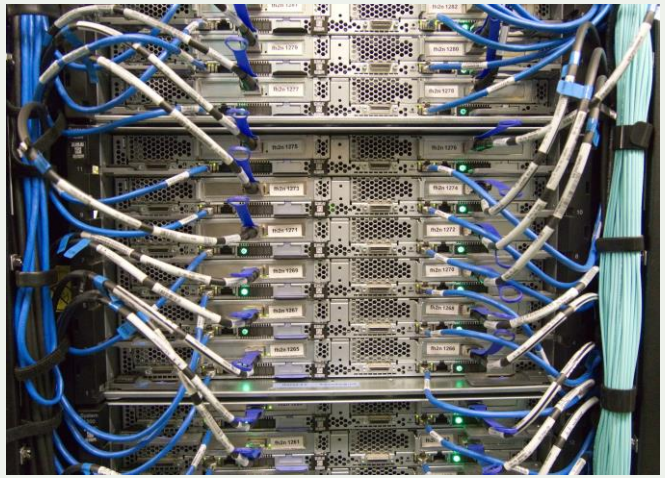
## The Road to Deployment


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

# Humans have always measured time…



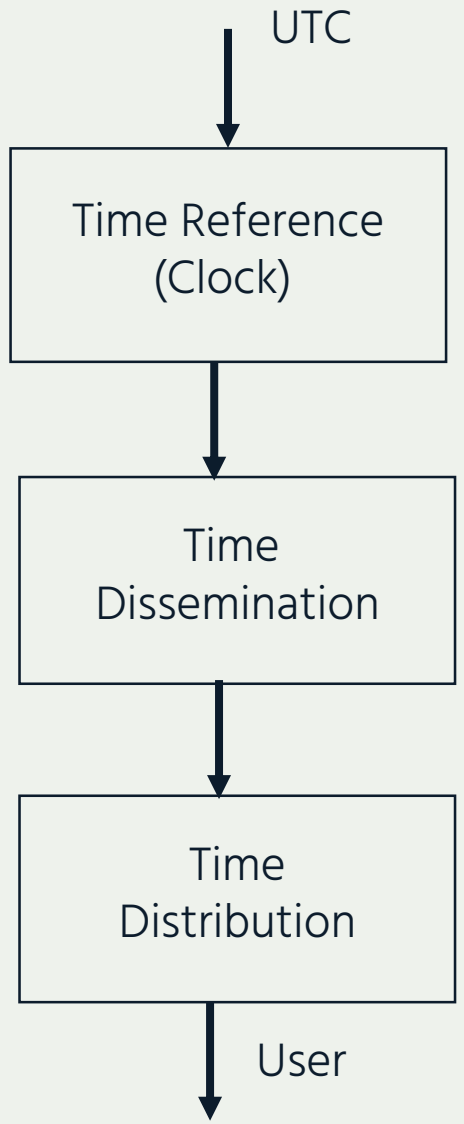

# Accurate time is vitally important.






# Where does accurate time come from?

- Time Reference
  - A time source traceable to a reference (e.g. UTC(USNO))
- Time Dissemination
  - Distribution of time and frequency information (e.g. GNSS)
- Time Distribution and Synchronization
  - Distribution of time to users and applications (e.g. NTP and PTP)



# Network Time Synchronization

Two basic network time synchronization protocols:

- Network Time Protocol (NTP): Defined by the IETF (RFC 5905)
- Precision Time Protocol (PTP) : Defined by IEEE 1588

NTP and PTP both:

- Exchange time information over a network for the purposes of clock synchronization
- Use this exchanged time information to determine the offset between two independent clocks
- Form a hierarchical tree structure as the basis for the distribution of time information
- Are somewhat resilient in the presence of packet loss

# Time ⟷ Security

Security has not been a high
priority of the 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…

COMPUTERWORLD
FROM IDG

INSIDER Sign In | R

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.

# Multiple sources of problems…

Flaws in configuration and implementation

Weaknesses in the actual protocol itself

Lack of adequate security mechanisms

And yet…

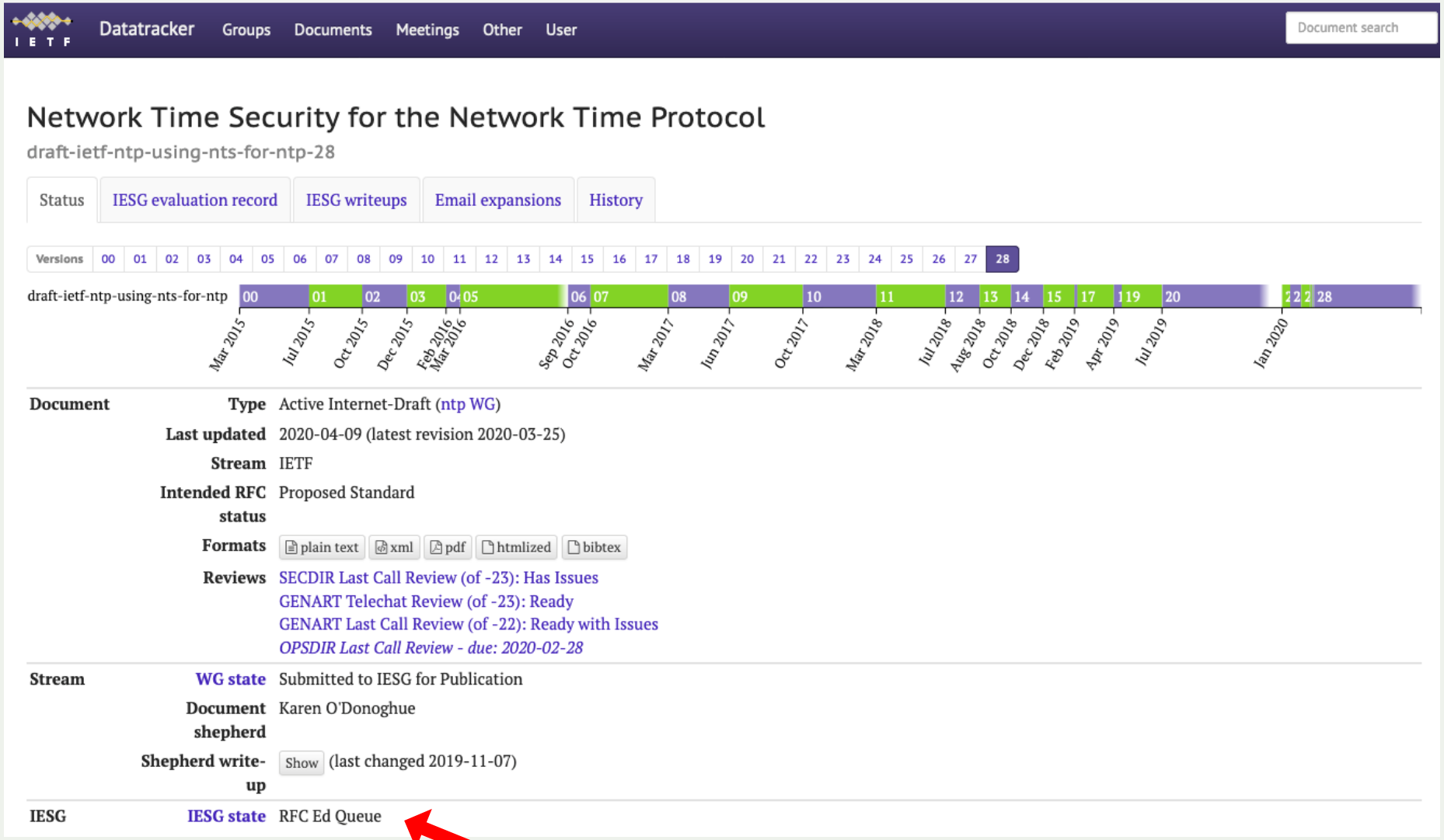
We had not had an updated specification for time synchronization security in 8+ years.

Until 2020!

# 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),<br>NTP client data minimization, etc. |
| Lack of adequate security mechanisms | Network Time Security (NTS) |

# Network Time Security (NTS)




NTS Approved by IESG in March 2020!

# 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

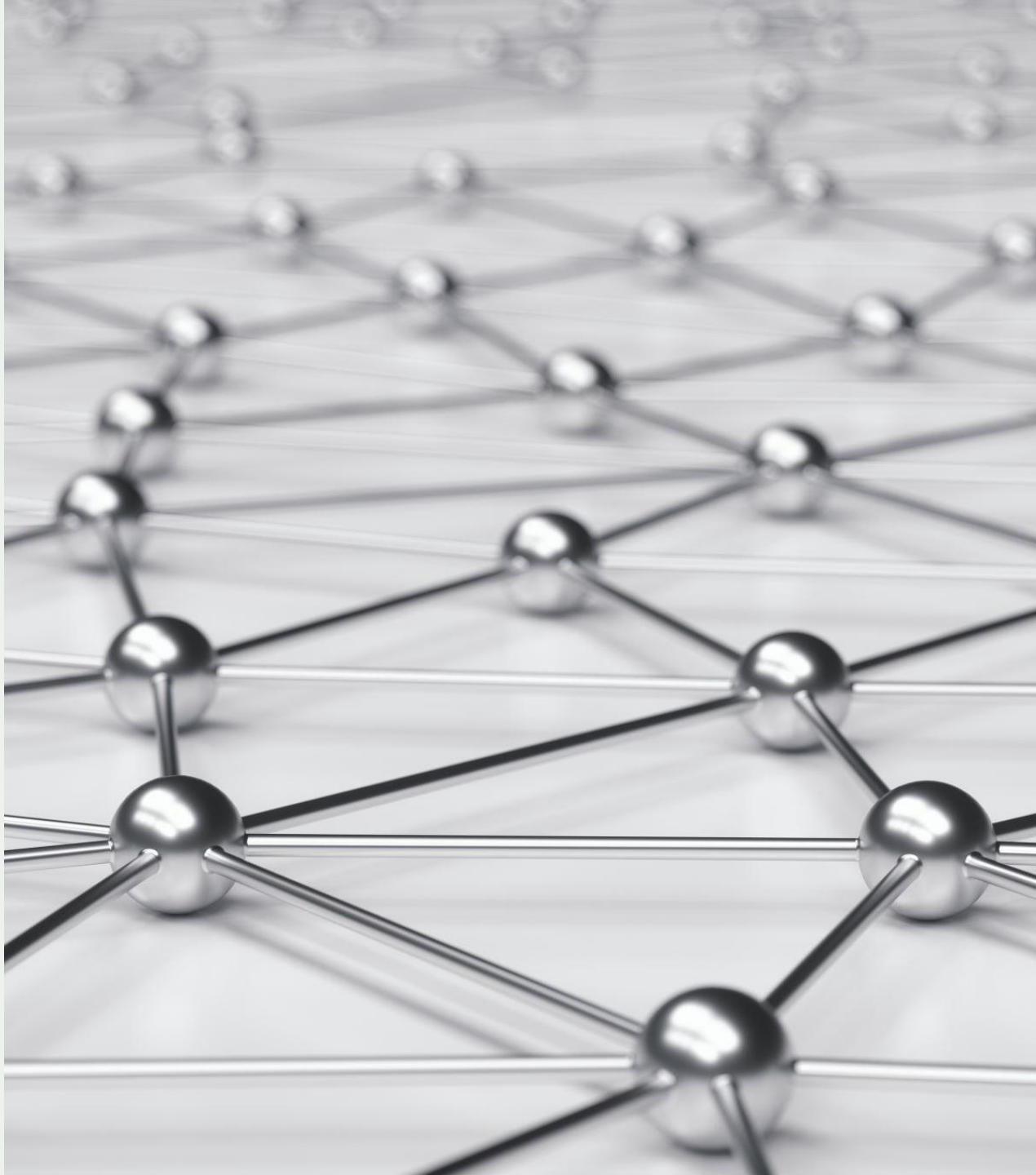
# It’s time to focus on the road to deployment…

# 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

# Internet Society Time Security Project

| | |
|---|---|
| Building a community (of key collaborators) | •Network operators<br>•Time service providers<br>•Enterprise IT groups |
| Maturing the NTS products | •Distributed multi-party testbed<br>•Virtual test events<br>•Test and measurement tools |
| Developing NTS deployment guidance | •Lessons Learned and BCPs<br>•Monitoring Tools |
| Outreach to expand NTS deployment | •Training<br>•Resources |



# It is Time to Act!

The Internet Society is looking for potential collaborators:

- Network operators, developers, potential testbed participants, time service providers

Join us:

- Send email to odonoghue@isoc.org

Follow us:

- https://www.internetsociety.org/issues/time-security/

Any questions?

# A few resources

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

https://www.internetsociety.org/blog/2017/09/time-synchronization-security-trust/

https://www.internetsociety.org/resources/doc/2017/new-security-mechanisms-network-time-synchronization-protocols/

https://www.netnod.se/time-and-frequency/network-time-security

https://www.netnod.se/time-and-frequency/how-to-use-nts

# 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