12 June 2018

TNC 18, Trondheim, Norway

Time and Security: An uneasy relationship

Karen O'Donoghue

odonoghue@isoc.org

Accurate Time needs Good Security?

Good Security needs Accurate Time?

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.

Research is occurring…

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 decades ago and without security in mind.

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

Image courtesy of Wes Hardaker

And yet…

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

It is (past) time to secure time…

Multiple sources of problems…

- Flaws in configuration and implementation of existing protocols
- Weaknesses in the protocol itself (protocol tweaks/clarifications)
- Lack of adequate security mechanisms

Existing time security specifications…

- Network Time Protocol (NTP)
  - Pre-shared key scheme for server authentication in the core specification (scaling issues) (RFC 5905 – 2010)
  - Autokey – Authentication of time servers using PKI (known flaws) (RFC 5906 – 2010)

- IEEE 1588 Precision Time Protocol (PTP)
  - Annex K – Group source authentication, message integrity, and replay attack protection (defined as Experimental, flaws identified) (IEEE 1588-2008)

Requirements for Time Synchronization Security

Internet Engineering Task Force (IETF)
Request for Comments: 7384
Category: Informational
ISSN: 2070-1721

T. Mizrahi
Marvell

October 2014

Security Requirements of Time Protocols
in Packet Switched Networks

Abstract

As time and frequency distribution protocols are becoming increasingly common and widely deployed, concern about their exposure to various security threats is increasing. This document defines a set of security requirements for time protocols, focusing on the Precision Time Protocol (PTP) and the Network Time Protocol (NTP). This document also discusses the security impacts of time protocol practices, the performance implications of external security practices on time protocols, and the dependencies between other security services and time synchronization.

NTP and the IETF

IETF approach to the problem…

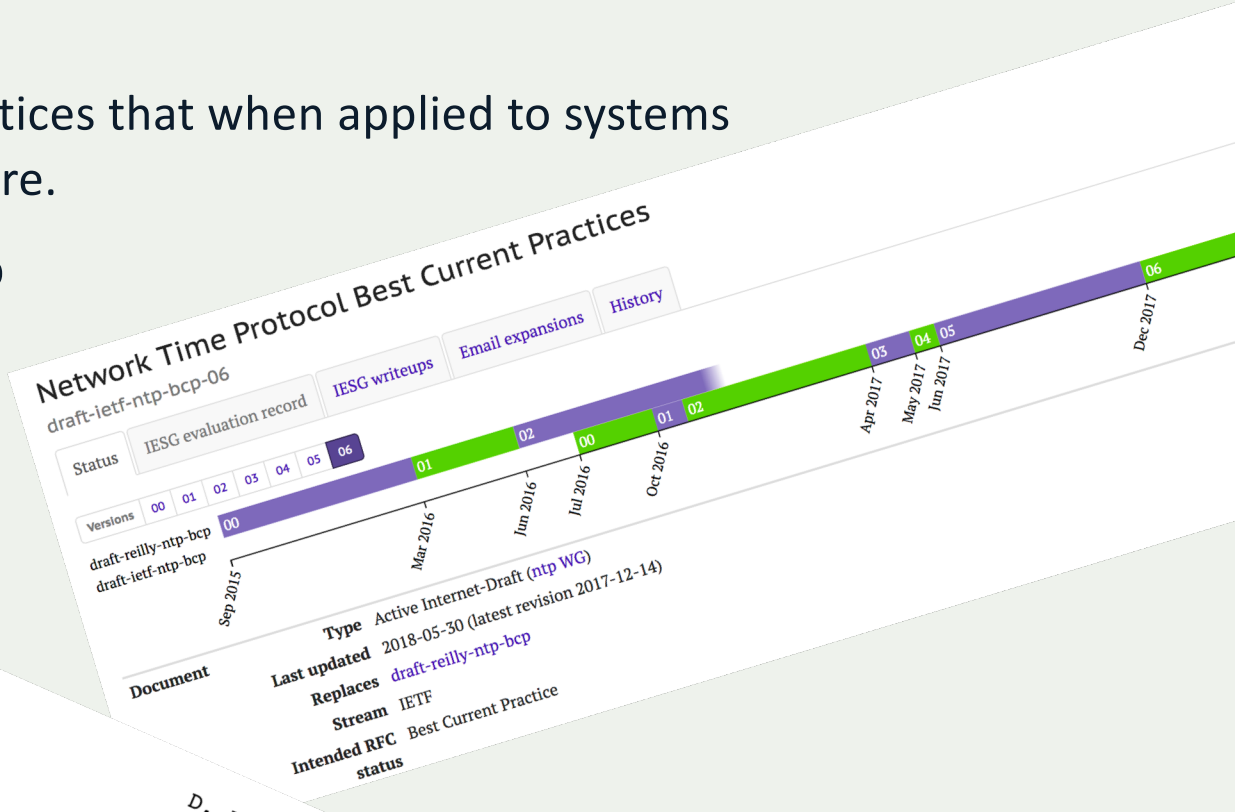
- Flaws in configuration and implementation of existing protocols
  - NTP Best Current Practice

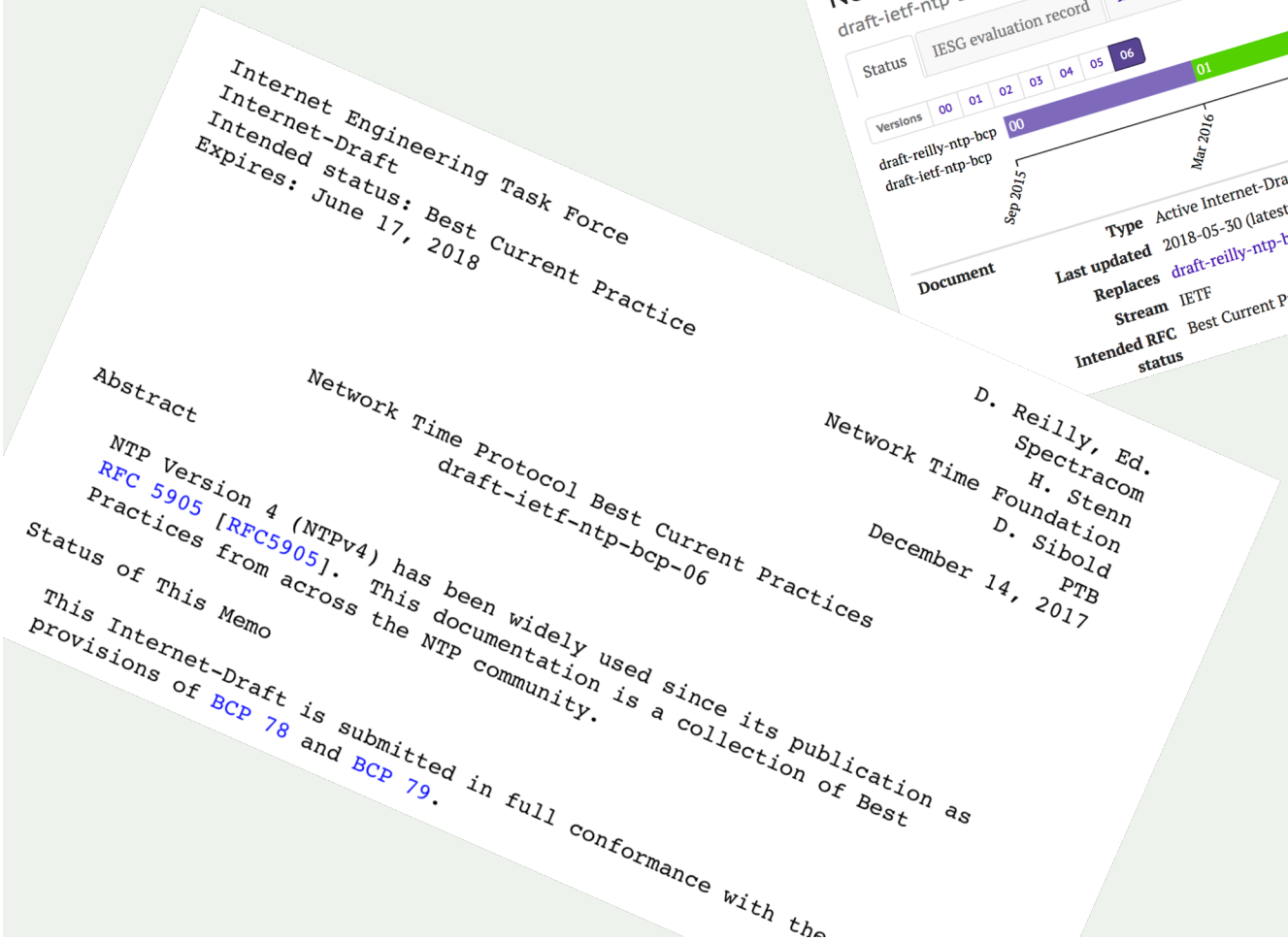
- Weaknesses in the protocol itself (protocol tweaks/clarifications)
  - Updated MAC for NTP, NTP client data minimization, etc.

- Lack of adequate security mechanisms
  - Network Time Security (NTS)

NTP Best Practices

- There are a number of best practices that when applied to systems can improve their security posture.
- Proposed BCP: draft-ietf-ntp-bcp
- Submitted for publication




Internet Engineering Task Force
Internet-Draft
Intended status: Best Current Practice
Expires: June 17, 2018

Network Time Protocol Best Current Practices
draft-ietf-ntp-bcp-06

D. Reilly, Ed.
Spectracom
H. Stenn
Network Time Foundation
D. Sibold
PTB
December 14, 2017

Abstract

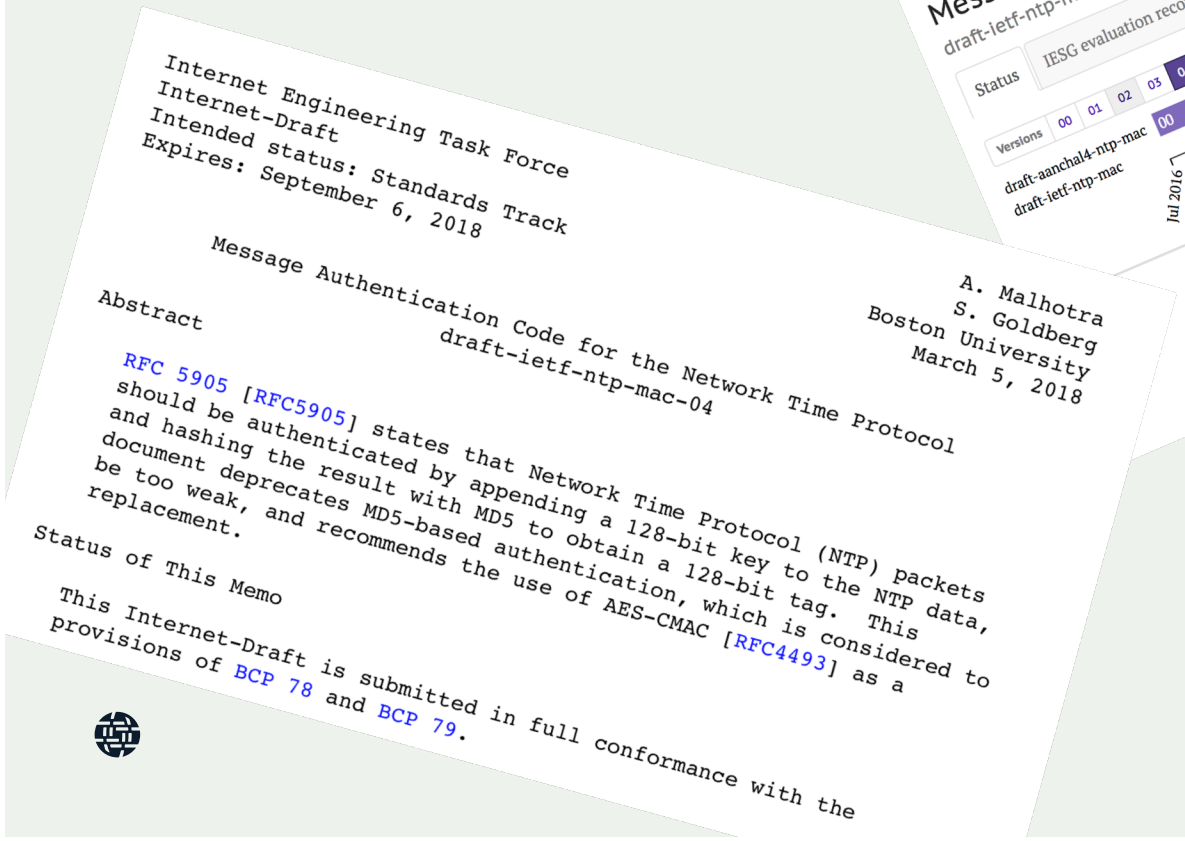
NTP Version 4 (NTPv4) has been widely used since its publication as RFC 5905 [RFC5905]. This documentation is a collection of Best Practices from across the NTP community.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Updated MAC for NTP

- Speaking of algorithm agility…
- Proposed Standard:
  Message Authentication Code for the Network Time Protocol
  - Replaces MD5 with AES-CMAC
  - Submitted for Publication



Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: September 6, 2018

A. Malhotra
S. Goldberg
Boston University
March 5, 2018

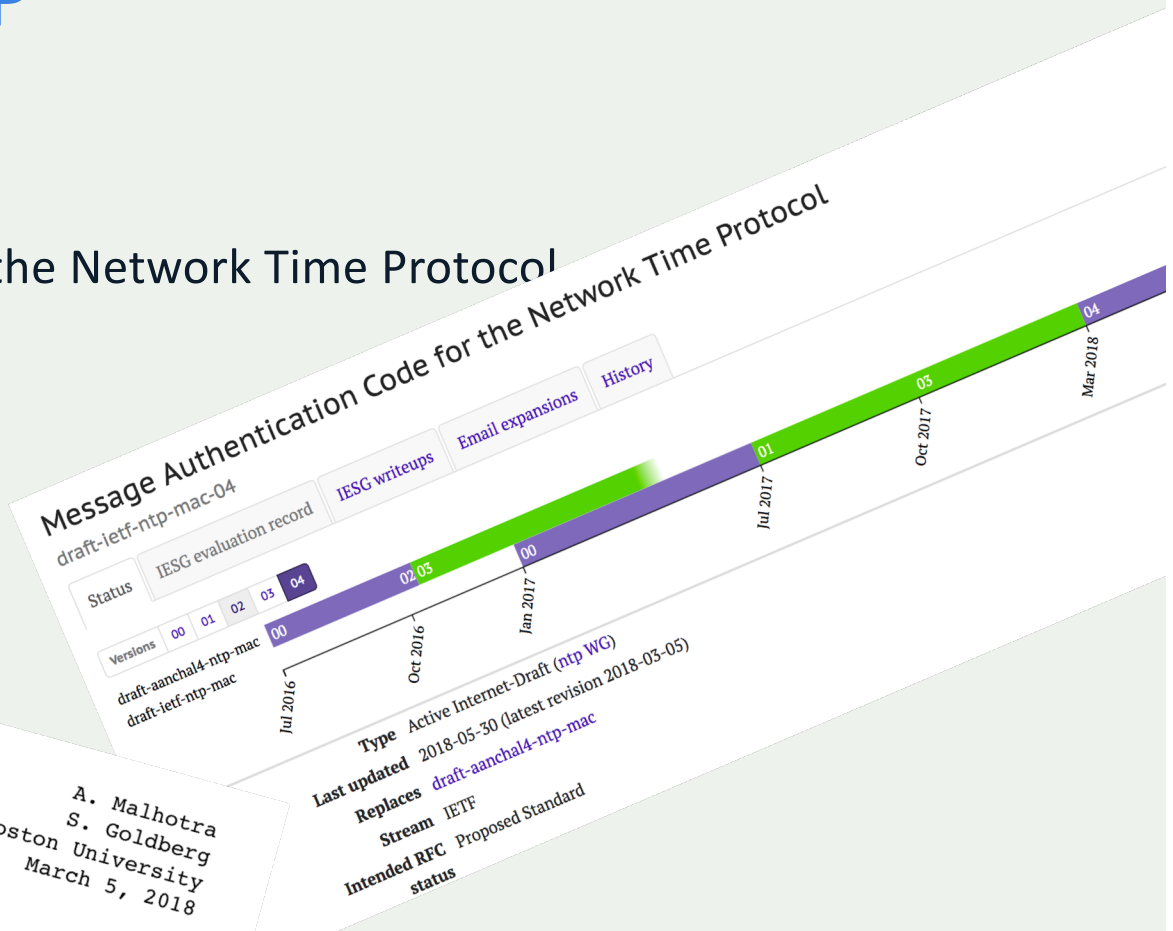
Message Authentication Code for the Network Time Protocol
draft-ietf-ntp-mac-04

Abstract

RFC 5905 [RFC5905] states that Network Time Protocol (NTP) packets should be authenticated by appending a 128-bit key to the NTP data, and hashing the result with MD5 to obtain a 128-bit tag. This document deprecates MD5-based authentication, which is considered to be too weak, and recommends the use of AES-CMAC [RFC4493] as a replacement.

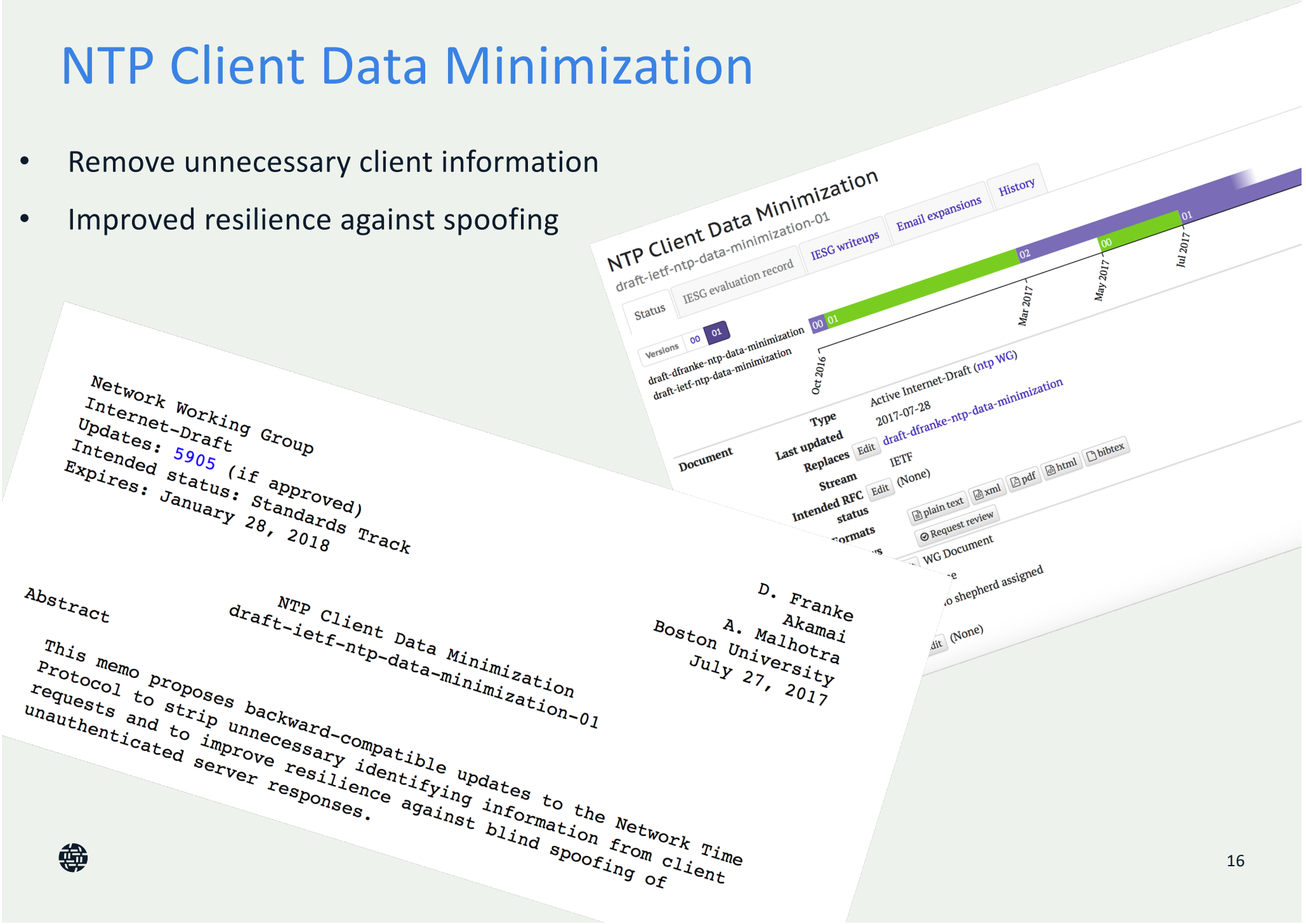
Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

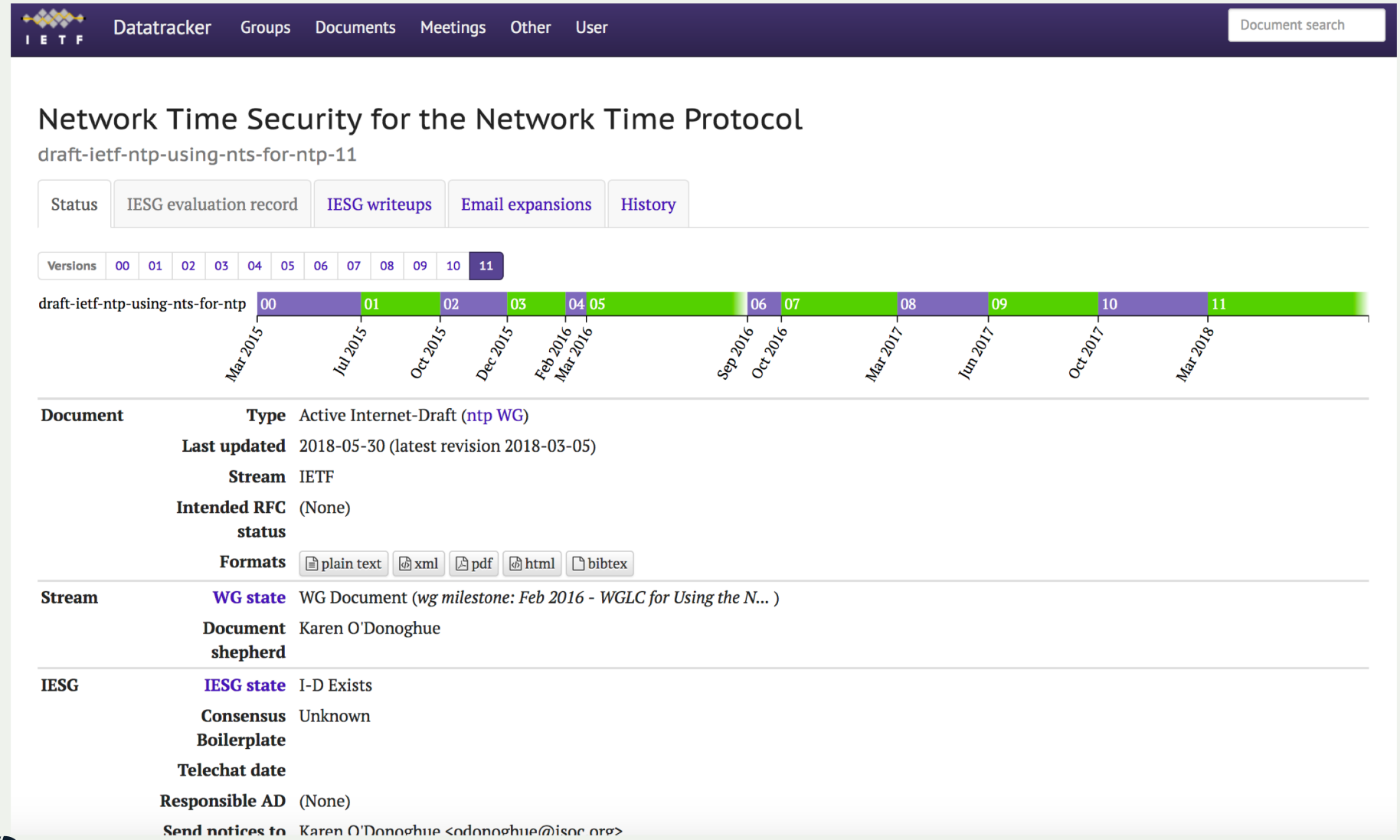


NTP Client Data Minimization

- Remove unnecessary client information
- Improved resilience against spoofing



The ongoing evolution of NTS



Network Time Security (NTS) provides…

- NTS for NTP: draft-ietf-ntp-using-nts-for-ntp
  - Integrity for NTP packets (not confidentiality)
  - 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 client-server mode only
    - Symmetric and broadcast modes have been deferred

- Caveat emptor!!! (This is not published (done) yet…)

TLS for NTP Security

- 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

NTP Extension Fields to support NTS

- NTS Unique-Identifier extension:
  - A 32-octet random value which serves as nonce and protects the client against replay attacks.
- NTS Cookie extension:
  - Information that enables the server upon receipt to re-calculate keys. The server therefore does not have to keep per-client state. This EF is opaque to the client.
- NTS Cookie Placeholder extension:
  - Sent whenever the client wishes to receive a new cookie. The server has to send an NTS Cookie extension for each received NTS Cookie Placeholder extension. This EF enables NTS to fulfill the unlinkability requirement.
- NTS Authenticator and Encrypted Extensions extension:
  - Contains the ICV which is computed over the NTP header and any preceding EF. It is calculated by applying the Authenticated Encryption with Associated Data approach.

IEEE and PTP

IEEE 1588 Security Approach

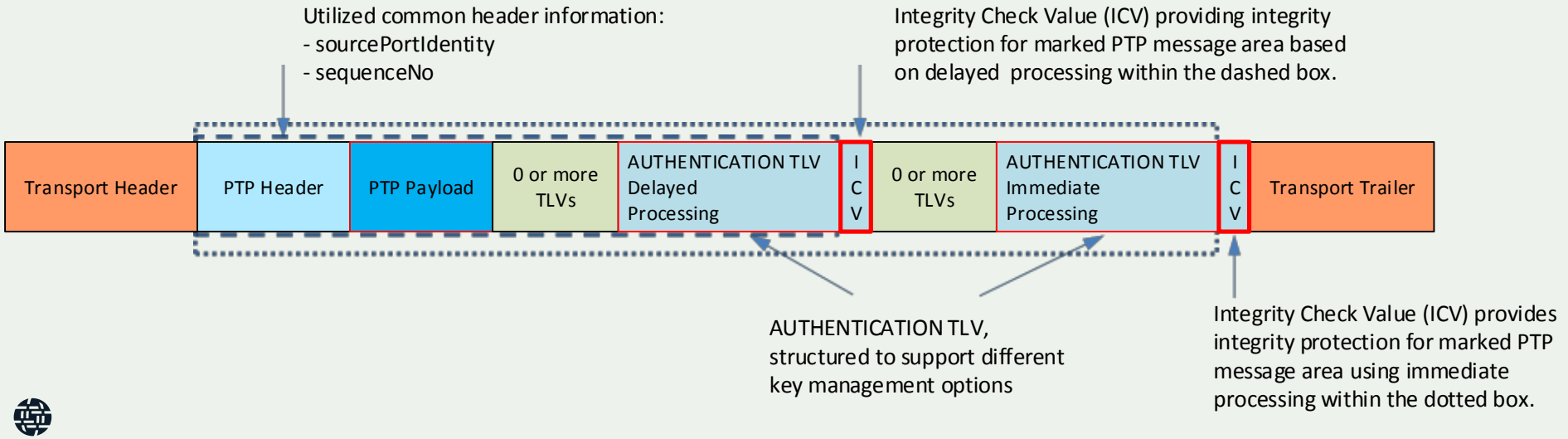
- IEEE 1588 security will include a set of mechanisms and tools that can be used together or individually.
- Individual mechanisms will be optional.
- The specific mechanisms chosen will vary by application and environment.
  - Expect future profile development in this area

IEEE 1588 Security: Multi-pronged Approach

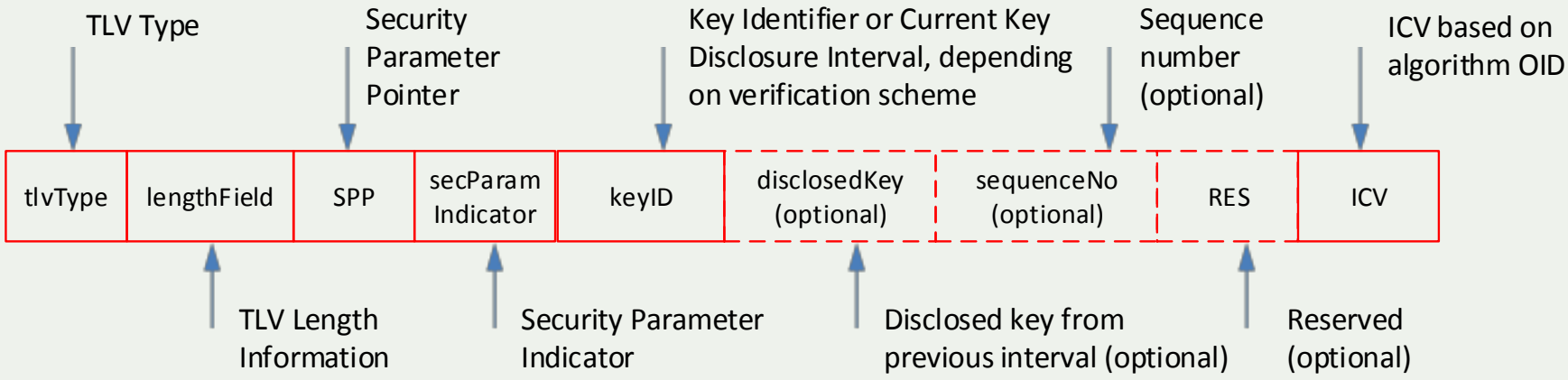
- PTP Integrated Security Mechanisms (Prong A)
- External Transport Security Mechanisms (Prong B)
- Architecture Guidance (Prong C)
- Monitoring and Management Guidance (Prong D)

PTP Integrated Security Mechanism (Prong A)
PTP Packet

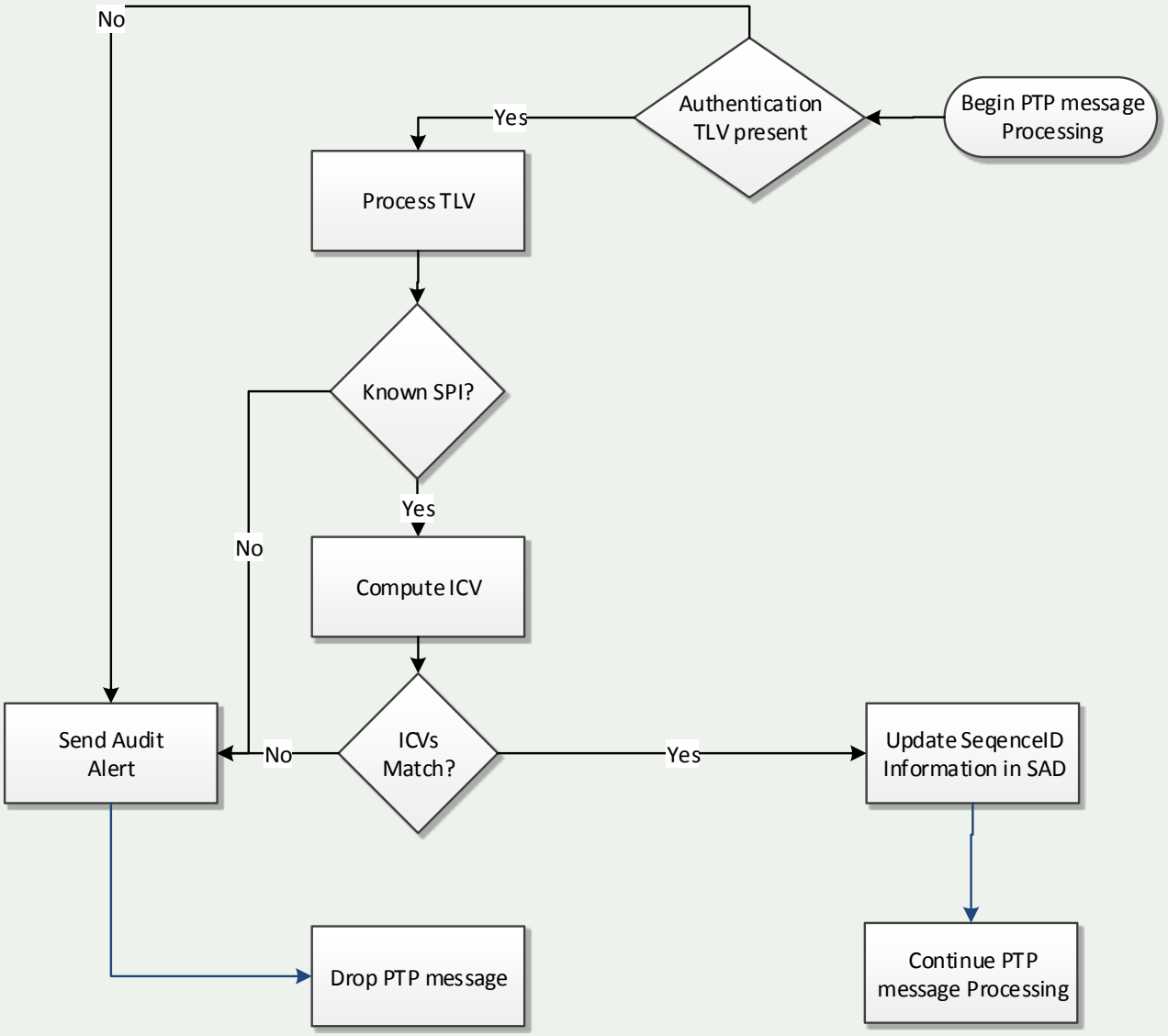
- TLV definition and processing rules (normative but optional)
- Information on example key management schemes (informative)
  - Future specification of specific key management schemes in IETF



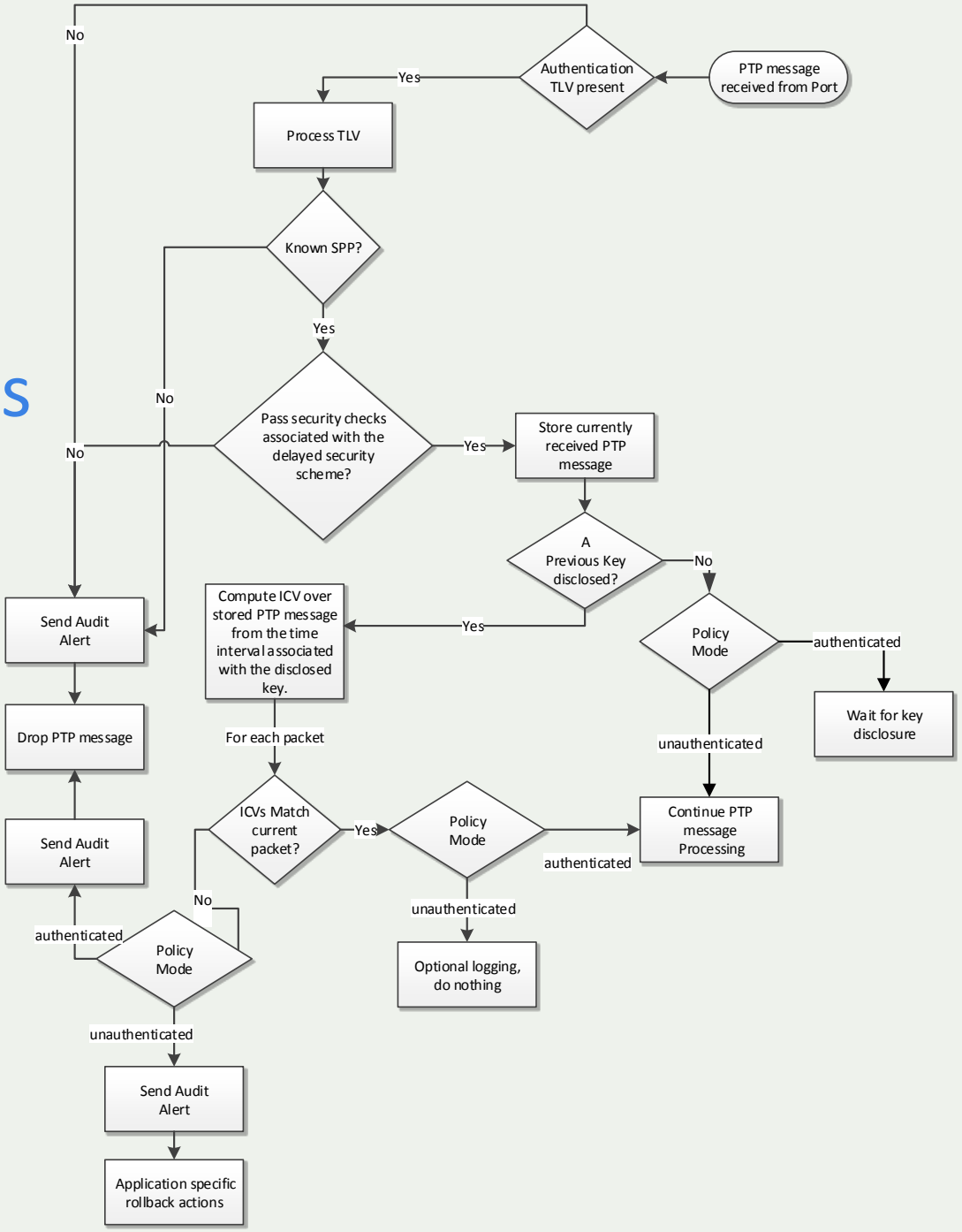
PTP Integrated Security Mechanism (Prong A): PTP Security TLV



PTP Packet Processing



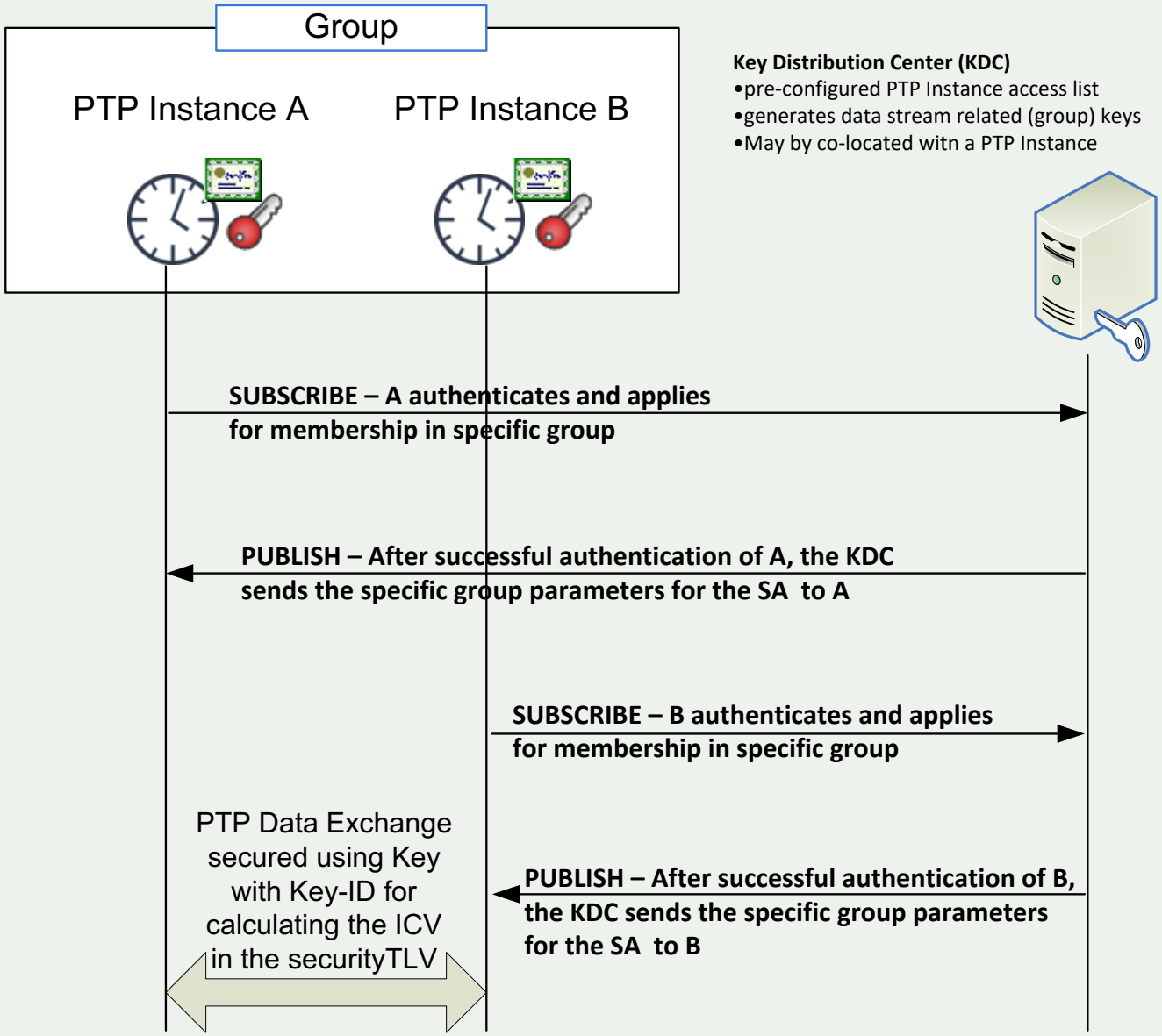
PTP Security Process



Key Management (therein lies the rub…)

- Static key distribution by some form of out of band mechanism
  - Good for getting started but not a long term solution
- Instant key sharing (GDOI)
- Delayed key sharing (TESLA)

Instant key sharing using GDOI

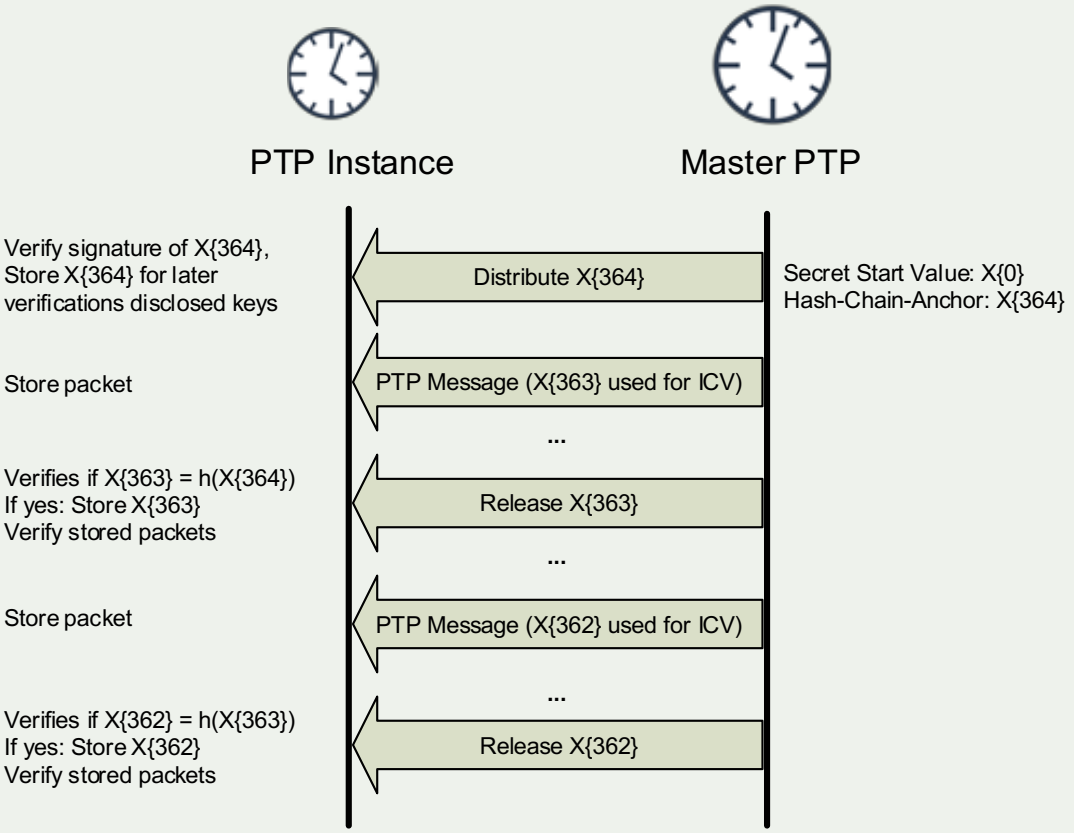


Delayed key sharing using TESLA

Timeline (Days)

X{0} Start Value	X{1} Day 363	X{2} Day 362	…	X{361} Day 3	X{362} Day 2	X{363} Day 1	**X{364} Hash-Chain-Anchor**

X{0} is the Secret Start Value
X{1} = Hash(X{0}) **X{2} = Hash(X{1})** **…** **X{364} = Hash(X{363})**
X{364} is the Hash-Chain-Anchor signed by the Master Clock



External Transport Security Mechanisms (Prong B)

- MACSec
  - Based on IEEE 802.1AE Media Access Control (MAC) Security
  - Integrity protection between two IEEE 802 ports
  - Key management is manual or based on MACsec Key Agreement (MKA) specified in IEEE 802.1X-2010.
- IPSec
  - Base architecture defined in IETF RFC 4301
  - Node authentication and key exchange defined in RFC 7296
  - Integrity checking and encryption of data defined in RFC 4303

Architecture Guidance (Prong C)

- Redundancy
  - Redundant timing systems
  - Redundant PTP grandmasters
  - Redundant paths

Monitoring and Management Guidance (Prong D)

- Definition of parameters in IEEE 1588 data sets that can be monitored to detect security problems
- A recommendation to not use unsecure management protocols including IEEE 1588 native management

… and Best Practices!

Next Steps

Final remarks

- The time is now…
- Implementers, testers, and researchers welcome!
- Done is better than perfect!
- Contact me if you are interested in helping:
  - Karen O'Donoghue, odonoghue@isoc.org

Acknowledgements and Thanks…

Co-authors: Steffen Fries and Dieter Sibold

IEEE 1588 Contributors: Steffen Fries, Dieter Sibold, Tal Mizrahi, Jeff Dunn, Doug Arnold, Stefano Ruffini, John Eidson, Opher Ronen, Silvana Rodriques, Bill Dickerson, Mikael Johansson, …

NTP Contributors: Harlan Stenn, David Mills, Denis Reilly, Danny Mayer, Sharon Goldberg, Aanchal Malhotra, Daniel Franke, Rich Salz, Miroslav Lichvar, Dieter Sibold, Kristof Teichel, Russ Housley, …

… and many more that I have neglected to mention here…

… it really does take a village…

Questions?

http://www.dailymail.co.uk/news/article-2284287/Youre-going-wrong-way-Moment-confused-fish-tried-swim-opposite-direction-hundreds-companions-enormous-shoal.html

Thank you.

Karen O’Donoghue

Research Analyst
odonoghue@isoc.org

Visit us at
www.internetsociety.org
Follow us
@internetsociety

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120