Secure PTP Using TLS Key Management

a proposal by

Douglas Arnold
Meinberg-USA

Agenda

The Synchronization Experts.

- Terminology
- PTP AUTHENTICATION TLV
- Network Time Security
- TLS Key Exchange
- PTP with NTS
- Summary

First two stages of grieving about lack of network timing security

1. Denial

- Me: “Are you interested in security for timing protocols?”
- Network operator: “No. Our network is very secure.”
- Me: “Call me after something bad happens.”
- Perhaps network security and timing are handled by different groups in a large organization. And they don’t talk to each other.

2. Anger

- Network operator: “What security is there for NTP and PTP?”
- Me: “NTP has an obsolete security mechanism, and PTP has nothing yet.”
- Network operator: “What the heck are you standards people doing?”

Executive Summary / Glossary

The Synchronization Experts.

Transport Layer Security (TLS)

- Cryptographic network security protocol
- Used in web browsing, email, messaging, and VoIP

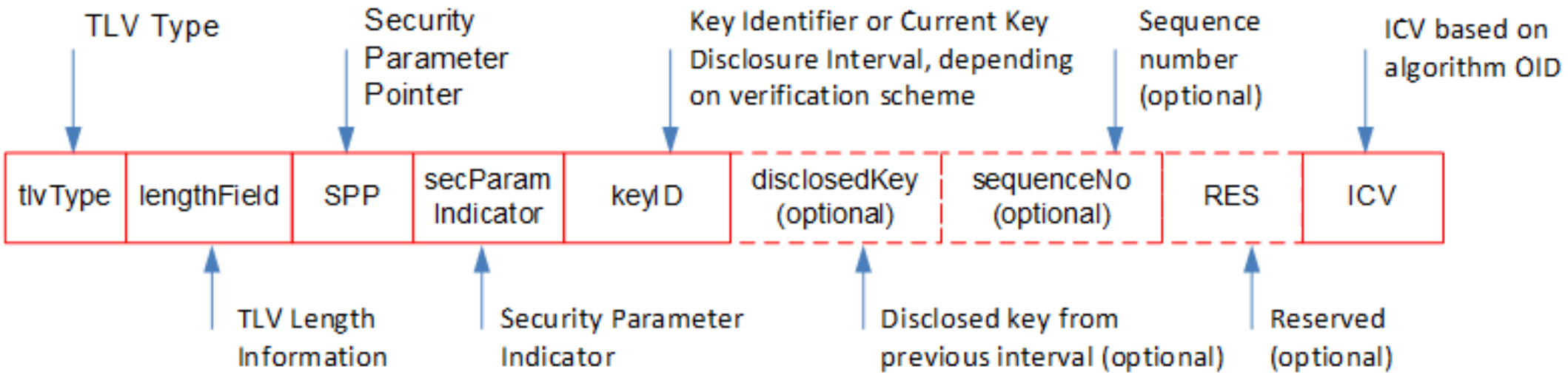
Network Time Security (NTS)

- Draft IETF RFC approved for publication
- https://datatracker.ietf.org/doc/draft-ietf-ntp-using-nts-for-ntp/
- Adaptation of TLS for unicast mode client-server NTP
- Time server manufacturers are going to implement this

Authentication TLV

- TLV = Type length value, a standard method for extending network messages
- PTP message extension for message integrity protection and possibly source authentication
- Defined in IEEE 1588-2019
- Requires a yet unspecified key management system to secure PTP
- NTS key management could be adapted for unicast PTP

PTP Authentication TLV



PTP Authentication TLV

The Synchronization Experts.

Security Parameter Pointer

- Indicates a specific entry in a security association database
- Allows a PTP instance to have secure communications with multiple network elements - for example a slave talking to a grandmaster and a monitoring node

Security Parameter Indicator

- Flags field indicating whether optional fields are present
- We don’t need any of the optional fields for NTS
- Set to all zeros

Key ID

- Indicates which key is being used
- Points to an entry in the security association database

ICV

- Integrity Check Value
- A hash code

Properties of NTS

The Synchronization Experts.

Starts with TLS Key Establishment (KE) Server

- Needed to start
- Then client and server continue without KE server

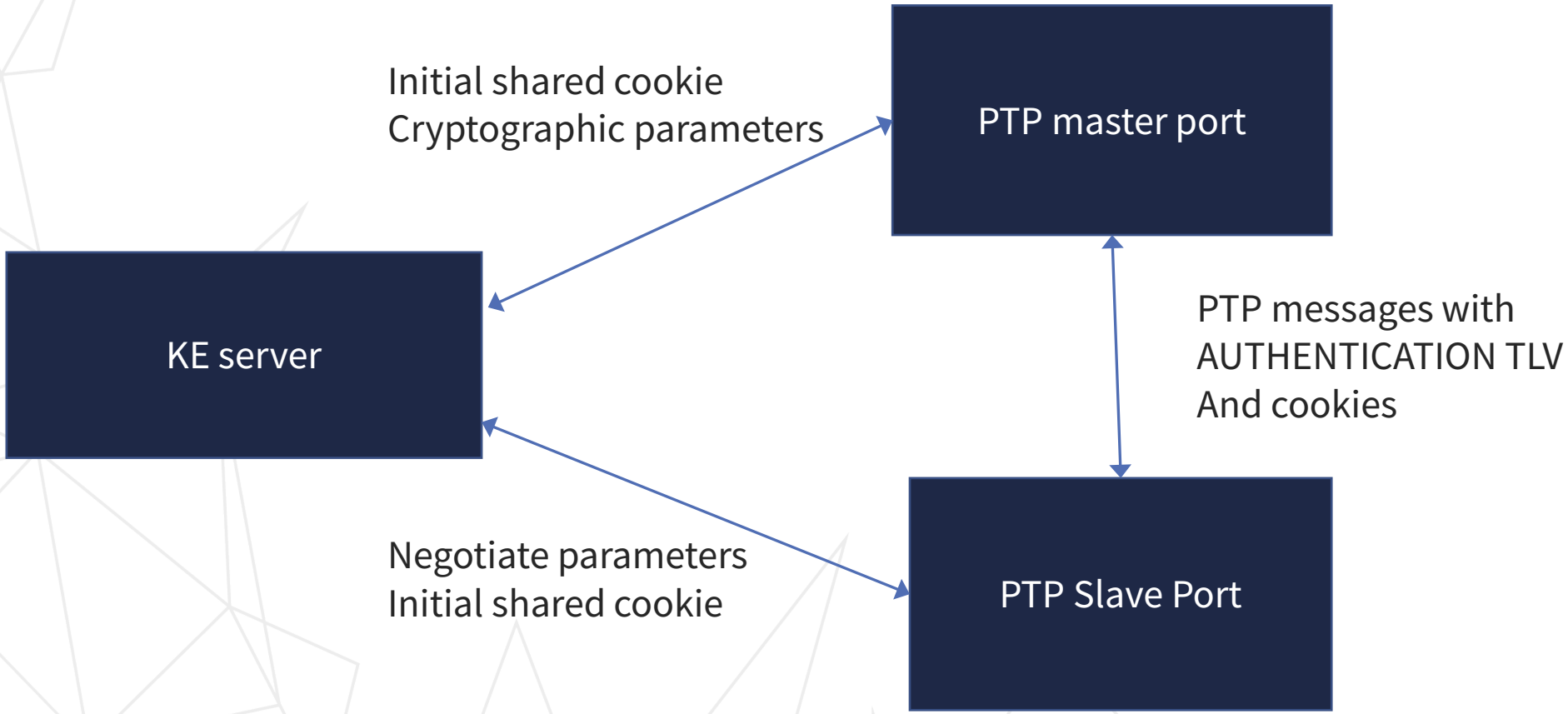
Properties of NTS

- NTP severs are stateless: don’t save data about any specific client
- Works only for unicast NTP
- Includes and ICV (hash code)
- Includes encryption
  - Needed to transfer keys, not to protect timestamps

PTP profile which could use NTS

- Unicast with negotiation
- IPv4 or IPv6 mapping

TLS Key Exchange Server



NTS Cookies

The Synchronization Experts.

S2M Cookie TLV

- ID of current S2M key
- ID of current M2S key (if different)
- Negotiated algorithm and parameters

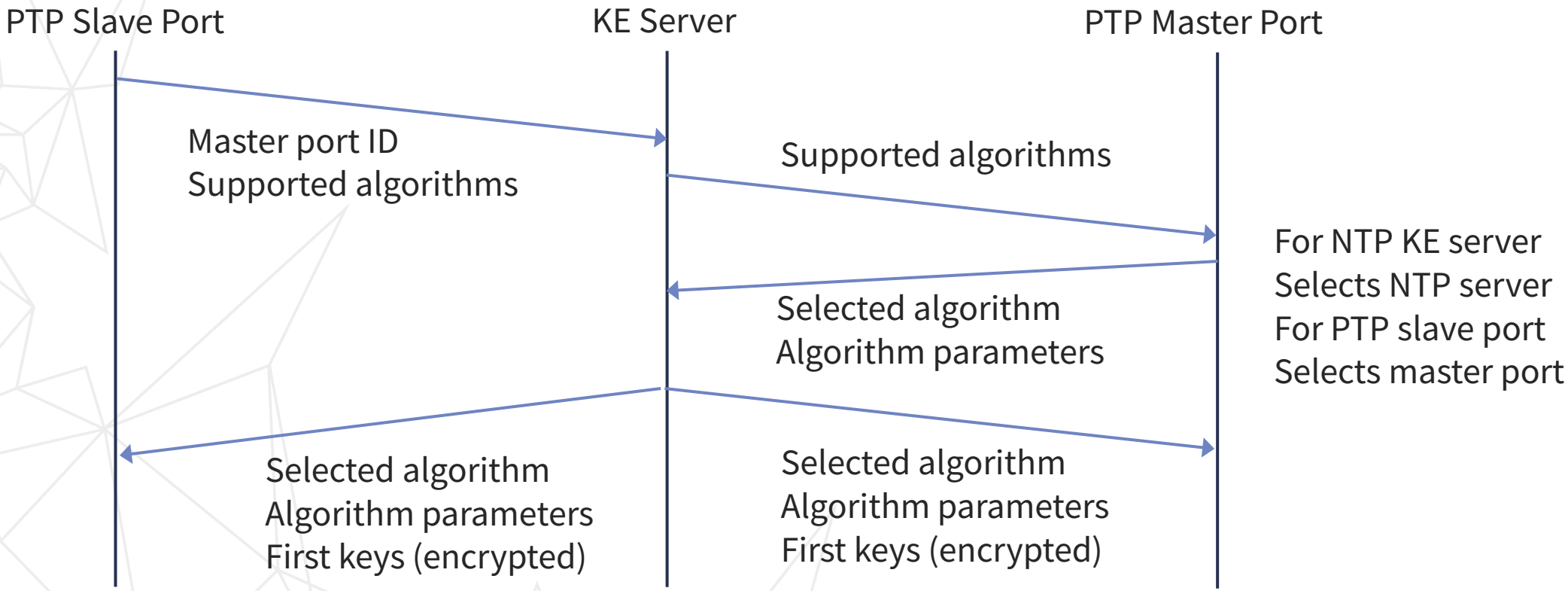
M2S Cookie TLV (Send encrypted)

- Next keys and IDs
- Negotiated algorithm and parameters

The cookie scheme allows NTP severs to not keep state for each client

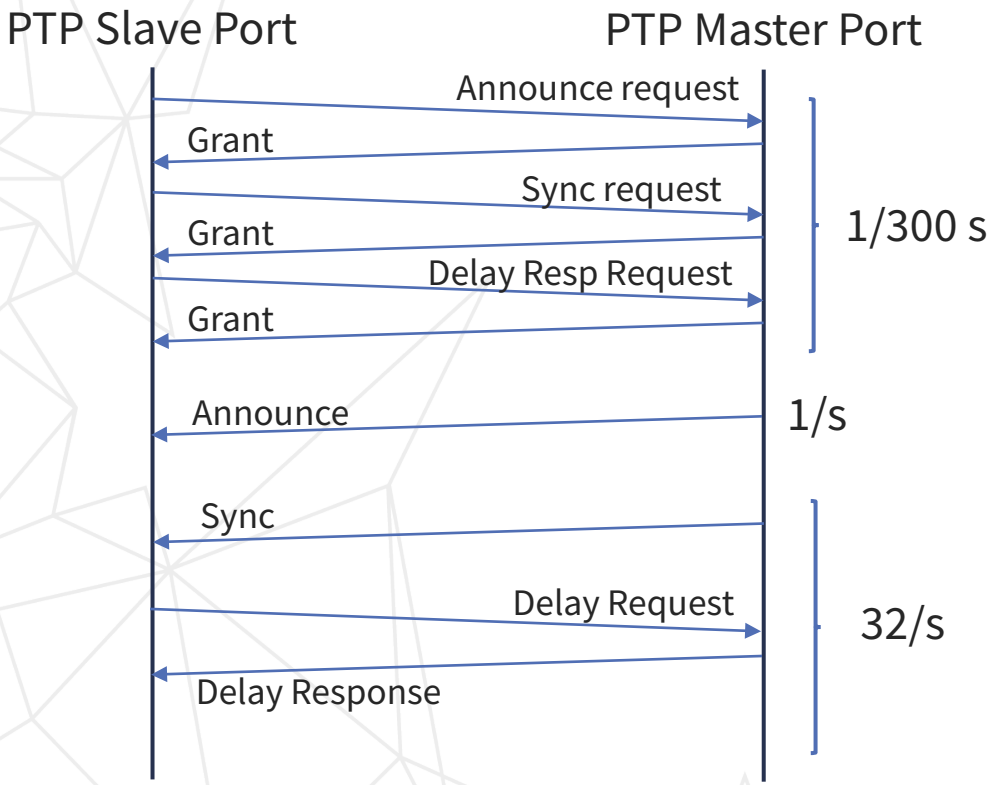
- NTP servers can have a very large numbers or clients
- NTP servers do keep keys in a list with index numbers
- PTP master ports keep data on slaves, but we retain this scheme so that NTS can secure both NTP and PTP

TLS Handshake for PTP

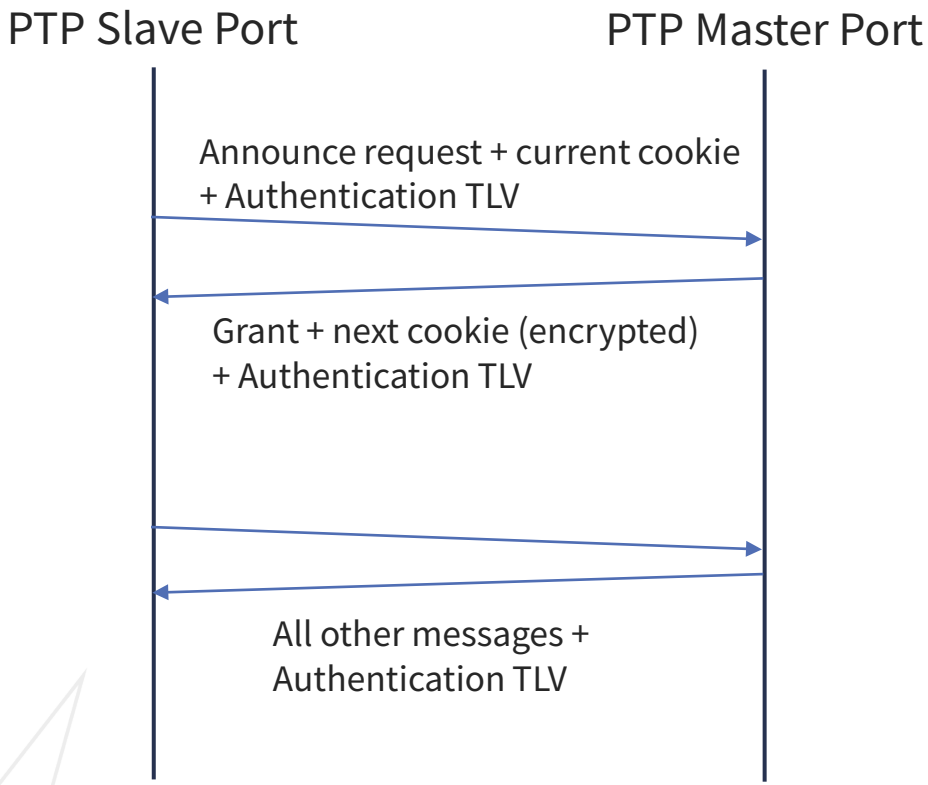


After initial shared cookie, master port generates new cookies

TLS Handshake for PTP



Traditional Unicast PTP



Unicast PTP with NTS

Summary

The Synchronization Experts.

NTS for NTP

- New security option to replace autokey
- Covers unicast client-server NTP only
- ~~Likely~~ Certain to be implemented in commercial time servers
- Uses TLS for algorithm negotiation and initial keys
- Subsequent keys generated by server

NTS for PTP

- Appropriate for layer 3 unicast PTP
- Cookies exchanged during announce message negotiation
- Keys used in AUTHENTICATION TLV

Dankeschön !!!

Questions and comments welcome:
doug.Arnold@meinberg-usa.com