Emerging Solutions in

Time Synchronization Security

Karen O'Donoghue, odonoghue@isoc.org

IEEE/NIST Challenges in the Smart Grid Workshop, 7 September 2014

Internet Society

Agenda

- Why Security Now?
- Requirements
- What currently exists?
- IEEE 1588
- IETF NTP NTS
- Next steps and parting thoughts…

Internet Society

Why Security Now?

- **Increasing interconnection and decentralization**
- **Increasing evidence of the impact of inadequate security**
- **Interdependency between security and time**
- **Legal and Compliance requirements**

Internet Society

Requirements for Time Synchronization Security

- **RFC 7384: Security Requirements of Time Protocols in Packet Switched Networks, Oct 2014**
  - Threat model
    - Internal versus external attacker
    - Man-in-the-middle versus injection
    - Threats
    - Requirements analysis
- **IEEE 1588 requirements analysis**
  - https://ieee-sa.centraldesktop.com/1588/file/27229936/
  - (contact me for access to this document if necessary)

Internet Society

RFC 7384: Threats

- Manipulation of time synchronization packets,
- Masquerading as a legitimate participant in the time synchronization protocol,
- Replay of legitimate packets,
- Tricking nodes into believing time from the wrong master,
- Intercepting and removing valid synchronization packets,
- Delaying legitimate time synchronization packets on the network,
- Denial of service attacks on the network at layer 2 and layer 3,
- Denial of service by overloading the cryptographic processing components,
- Denial of service by overloading the time synchronization protocol,
- Corruption of the time source used by the grand master,
- Protocol design and implementation vulnerabilities, and
- Using the time synchronization protocol for broader network surveillance and fingerprinting types of activities.

Internet Society

RFC 7384: Requirements

- Authentication and authorization of a clock's identity,
- Integrity of the time synchronization protocol messages,
- Prevention of various spoofing techniques,
- Protection against Denial of Service (availability),
- Protection against packet replay,
- Timely refreshing of cryptographic keys,
- Support for both unicast and multicast security associations,
- Minimal impact on synchronization performance,
- Confidentiality of the data in the time synchronization messages,
- Protection against packet delay and interception, and
- Operation in a mixed secure and non-secure environment.

Internet Society

What currently exists?

- **Network Time Protocol (NTP)**
  - **Pre-shared key scheme for server authentication in the core specification (scaling issues)**
  - **Autokey – Authentication of time servers using PKI (known flaws)**
- **IEEE 1588 Precision Time Protocol**
  - **Annex K – Group source authentication, message integrity, and replay attack protection (defined as Experimental, flaws identified)**

Internet Society

Proposed 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.**

Internet Society

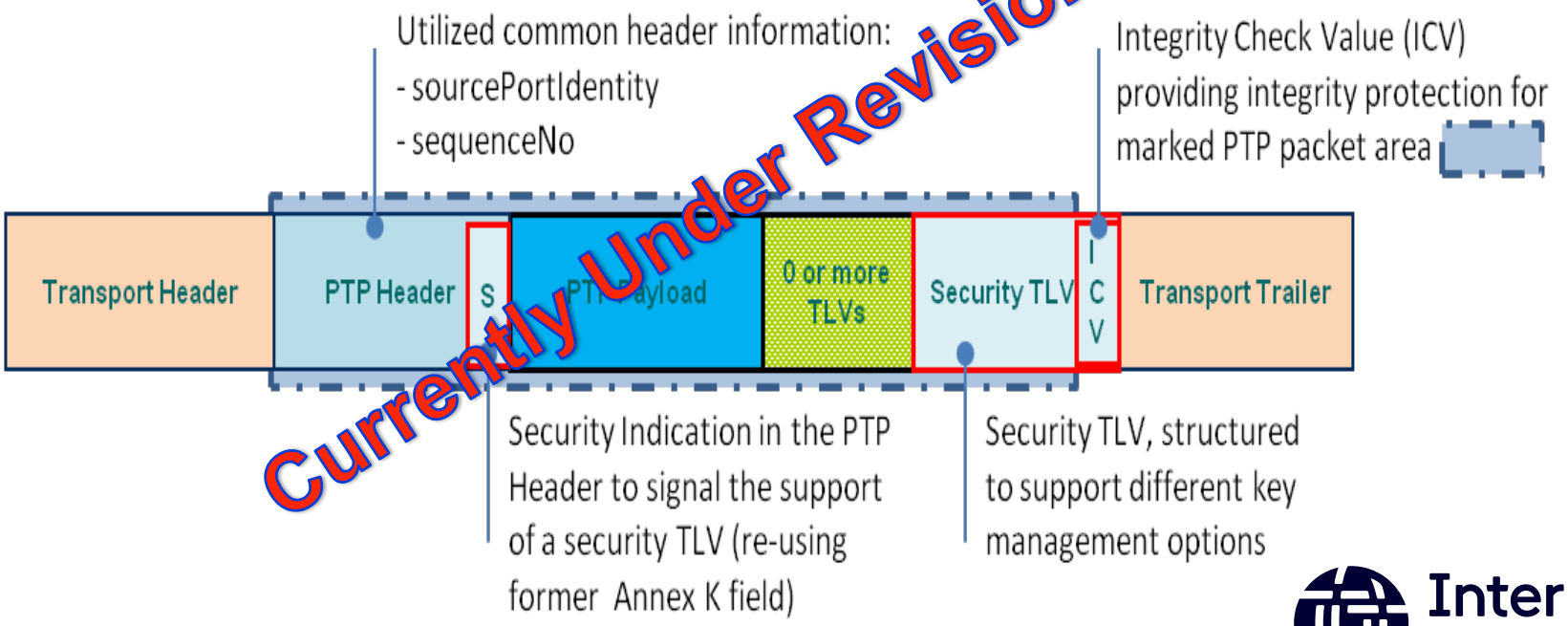
IEEE 1588 Security

- **The 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)

Internet Society

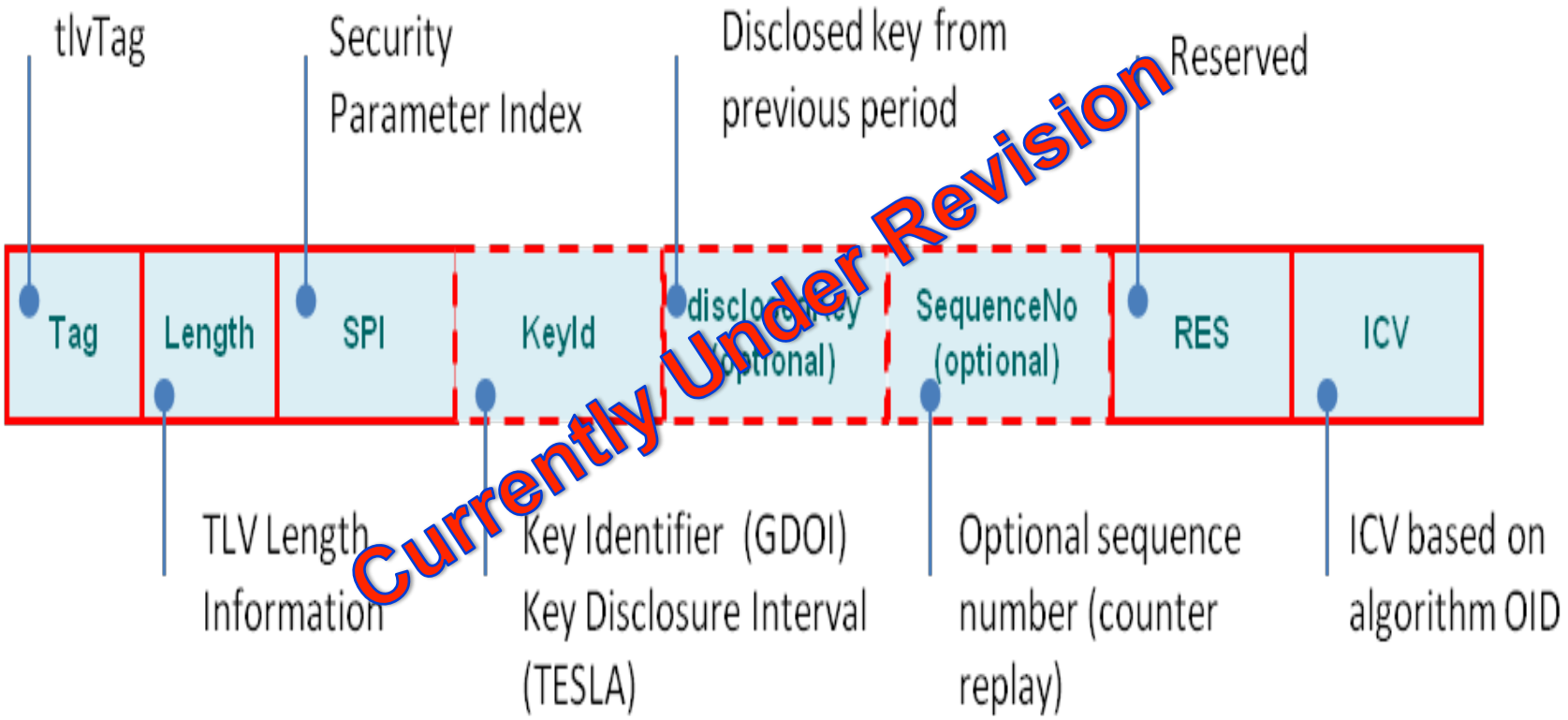
PTP Integrated Security Mechanism (Prong A)

- **TLV definition and processing rules (proposed option within IEEE 1588)**
- **Guidance of key management schemes (informative)**
  - **Specification of key management schemes in IETF**



Internet Society

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



Internet Society

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**

Internet Society

Architecture Guidance (Prong C)

- **Redundancy**
  - **Redundant timing systems**
  - **Redundant PTP grandmasters**
  - **Redundant paths**
- **Inherent measurements**
  - **Delay and offset measurements**

Internet Society

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**

Internet Society

IETF Network Time Security (NTS)

- **NTS – Work in Progress**
  - **Original core set of documents**
    - Generic approach: draft-ietf-ntp-network-time-security
    - Mapping of NTS to NTP: draft-ietf-ntp-using-nts-for-ntp
    - Protecting NTS with CMS: draft-ietf-ntp-cms-for-nts-message
  - **Additional documents under discussion**
    - DTLS mechanism for NTP: draft-dfranke-nts
    - Improving privacy for NTP: draft-dfranke-ntp-data-minimization
    - Evaluation of MAC algorithms for use with NTP: draft-aanchal4-ntp-mac

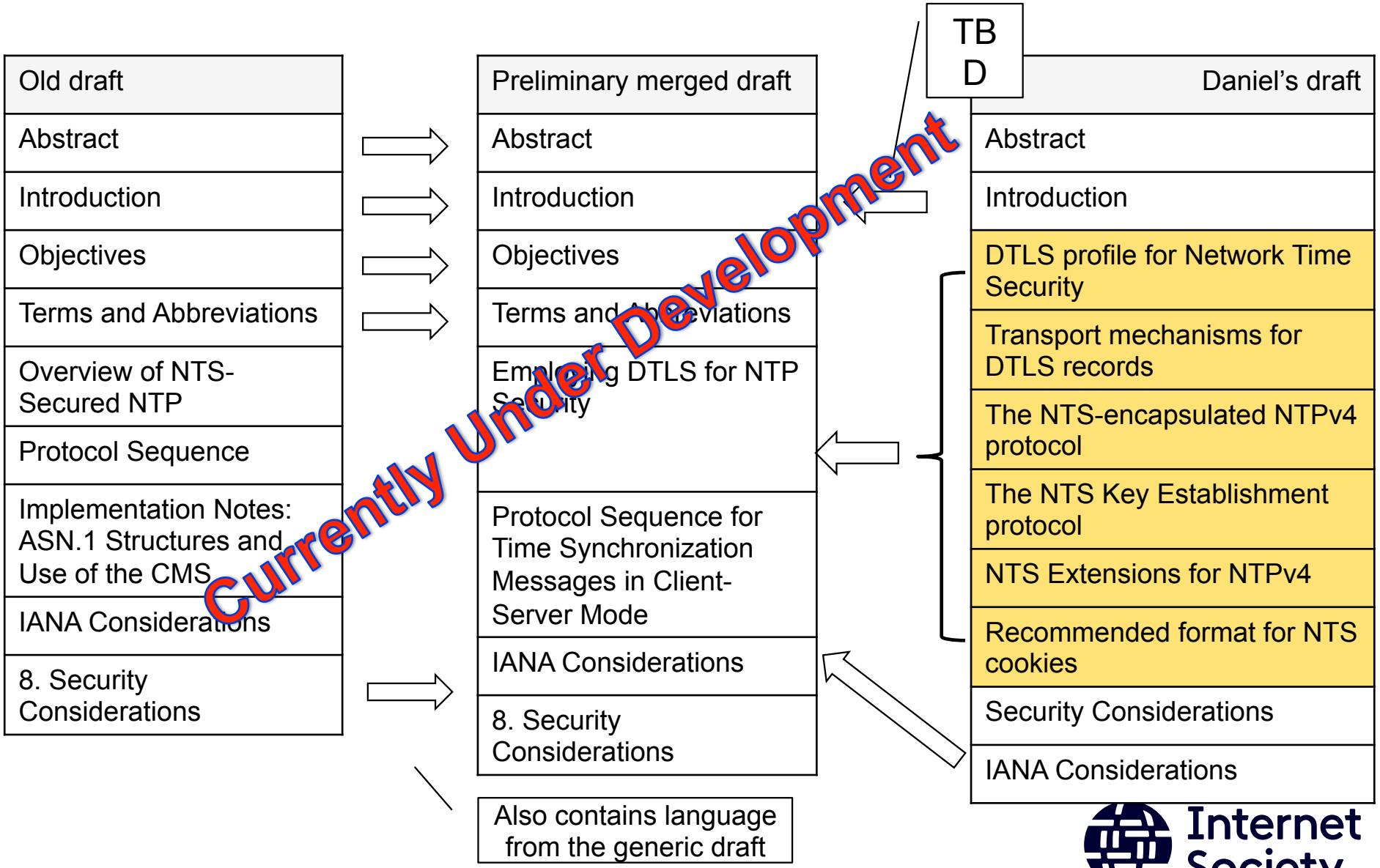
Internet Society

IETF Network Time Security (NTS)

- **Recent Decisions (still to be confirmed by NTP WG):**
  - **Key Exchange Protocol**
    - No custom key exchange being defined
    - Combination of DTLS and TLS in different combinations:
      - For client/server mode, TLS out of band to establish keys, transmission of timing information over UDP/123
      - For symmetric mode, TLS (or DTLS) on port other than UDP/123 to establish keys, transmission of timing information over TLS
      - For control mode, DTLS on port other than UDP/123 to establish keys
  - **Privacy – requirement to prevent linkability**
    - Need to address in base NTP as well as NTS

Internet Society

Merge of NTS for NTP draft with new proposal



Internet Society

Best Practices

- There are a number of best practices that when applied to systems can improve their security posture.
- Both IEEE 1588 and NTP are addressing these types of topics:
  - IEEE 1588 – additional section in draft annex
  - IETF NTP – proposed BCP: draft-ietf-ntp-bcp

Internet Society

Next Steps

- IEEE 1588
  - Complete proposal for next revision of IEEE 1588
  - Continue specification of key management options
- NTS
  - Revise NTS specifications
  - Publish BCP
  - Incorporate additional fixes to base specification (RFC 5905)
- Gather feedback from implementers and users

Internet Society

Final remarks

- **Why has this been so hard?**
- **When will we be done?**
- **Hopefully these solutions will be aligned to help development, deployment, and operation!**
- **Contact me if you are interested in helping:**
  - **Karen O'Donoghue, odonoghue@isoc.org**

Internet Society