Secure Time Synchronization –

Key Management enabling the use of the integrated security in the Precision Time Protocol

Steffen Fries, Andrej Görbing, Andreas Güttinger, Siemens
Herb Falk, Outside the Box Consulting Services
Douglas Arnold, Meinberg

WSTS May 9, 2024

MEINBERG OTB Consulting Services SIEMENS

Agenda

- Requirements for PTP security
- PTP security options
- PTP security using GDOI
- Summary

Time Synchronization using the Precision Time Protocol (IEEE 1588)

Application Example in Power Utility Substation

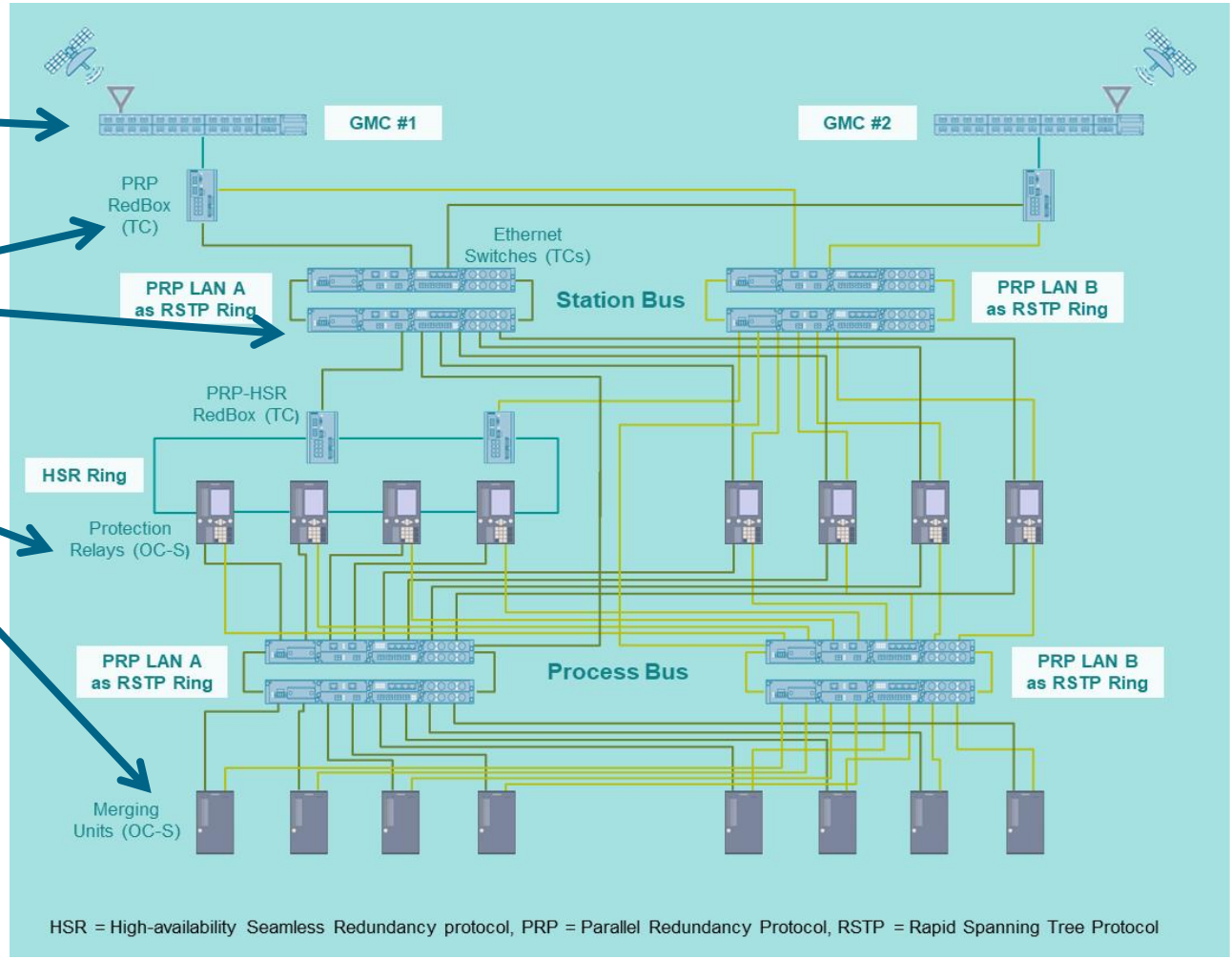
- Grandmaster clocks (GMC)

  IEEE 1588 time synchronization to station bus and process bus networks
- Ethernet switches and redundancy boxes

  Transparent clock (TC) or boundary clock (BC) function
- Protection relays, merging units and other intelligent electronic devices (IEDs)

  Ordinary time receiver clock (OC-S) function
- Seamless redundancy

  IEC 62439-3 HSR and PRP, the latter in combination with IEEE 802.1Q RSTP

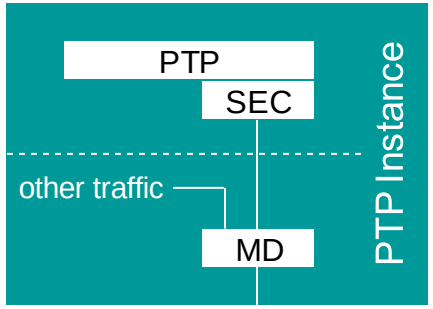


Time Synchronization using the Precision Time Protocol (IEEE 1588)

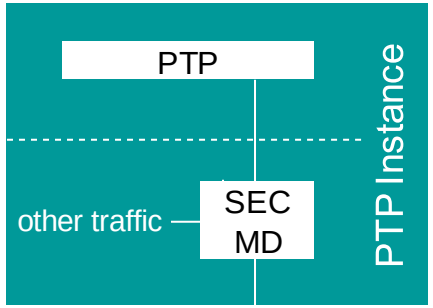
PTP Security Motivation and Approach

PTP security options

- PTP Instances using PTP integrated security option
  - Prong A: AUTHENTICATION TLV
  - Requires automated key management not defined in IEEE 1588-2019



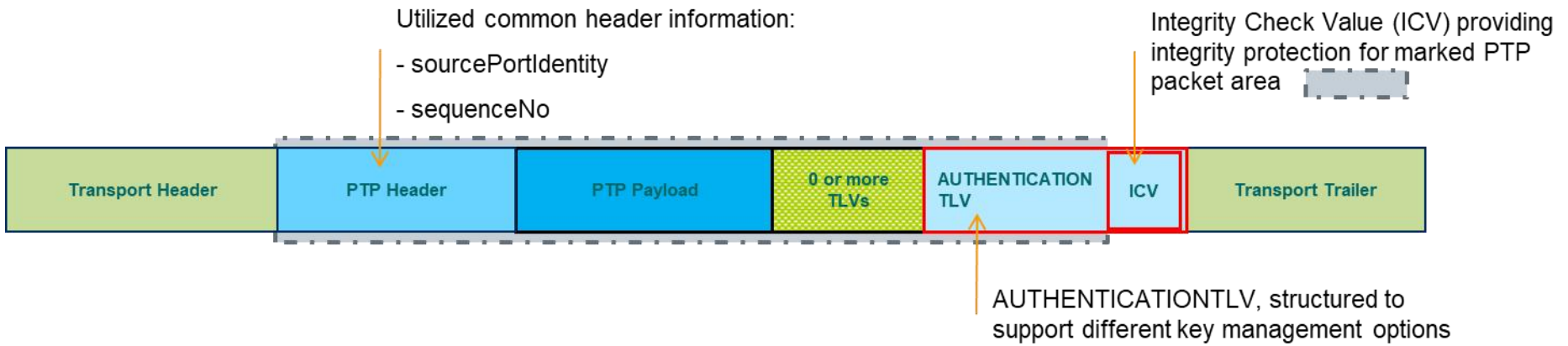
- PTP Instances using PTP external transport specific security means:
  - Prong B: MACsec or IPSec
  - MACsec and IPSec configurations defines for data might not work well for well for timing
    - Encryption for data privacy makes timestamping difficult
    - Second configuration for timing might be required



- Further Guidance
  - Prong C: Architecture means
  - Prong D: System monitoring

Time Synchronization using the Precision Time Protocol (IEEE 1588)
PTP Integrated Security Option

- Approach: Enhancement of PTP packets with AuthenticationTLV to provide source authentication and message integrity

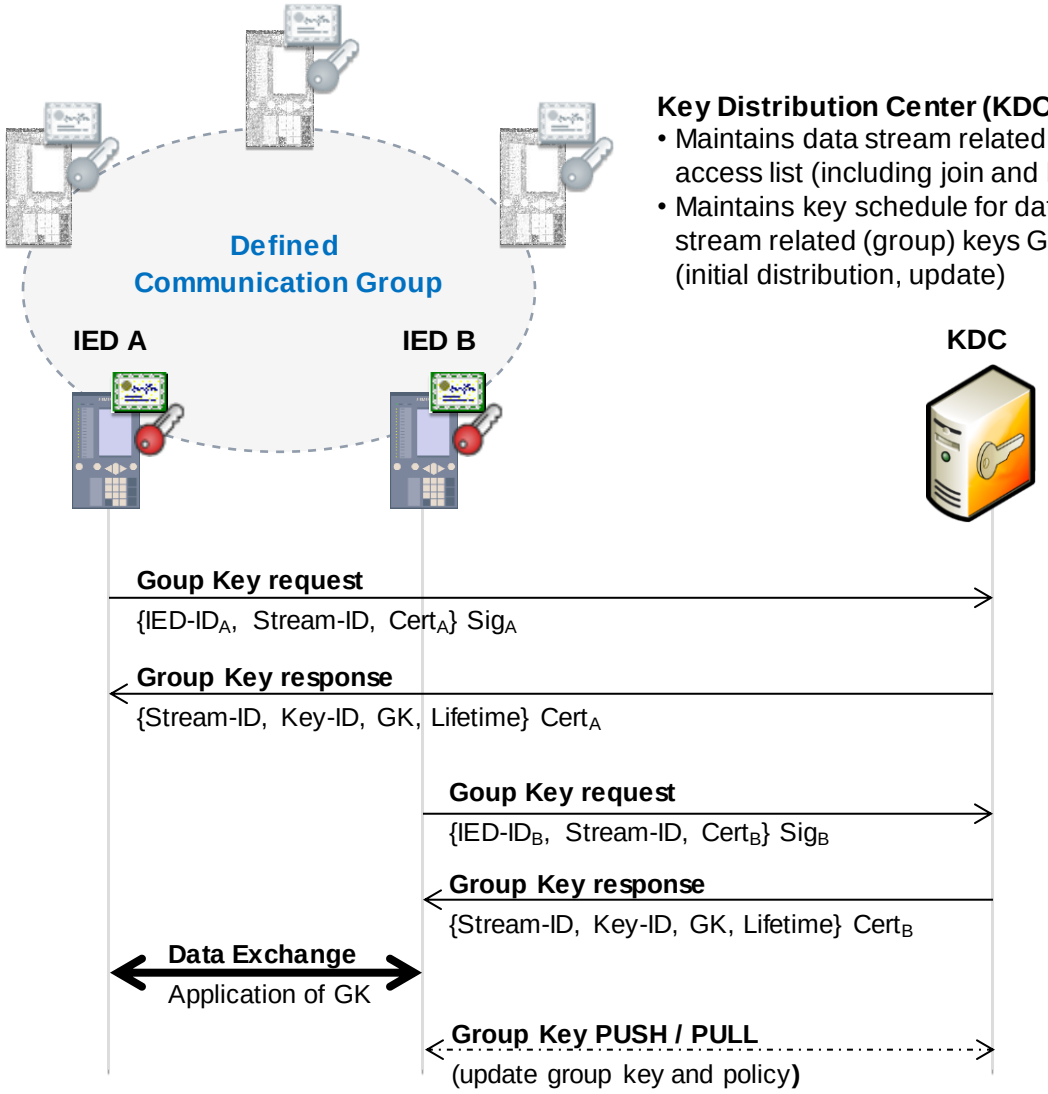


- Necessary **prerequisite** for the integrated security option is a **(group-)key management** to allow for automated distribution of cryptographic and security (note that manual management is also possible, but impractical for large networks).
- IEEE 1588:2019 refers to example key management schemes, which also support group-based communication to tackle both, unicast and multicast PTP
  - Group Domain of Interpretation (GDOI, IETF RFC 6407)
  - Timed Efficient Stream Loss Tolerant Authentication (TESLA, IETF RFC 4082)
- Further work started in IETF to enhance Network Time Security (NTS, IETF RFC 8915) to provide PTP security parameter
- So far guidelines for use with PTP defined only for GDOI (IEEE 1588d-2023 Amendment to IEEE 1588-2019)

Time Synchronization using the Precision Time Protocol (IEEE 1588)

Handling the Prerequisite: Key Management supporting the PTP Security Option

- Power systems can be secured using the IEC 62351 series
- **IEC 62351-9:2023 is the key management standard** defining management of X.509 credentials as well as group keys and associated security policies
  - Utilizes and defines enhancements for GDOI to distribute security parameter for protocols GOOSE, SV, and PTP
  - Directly addresses requirements of recently finished IEEE 1588 amendment 1588d for group based key management
- Interaction
  - PTP Instances authenticate towards KDC using PTP instance specific X.509 credentials
  - KDC distributes group key and group policy
  - KDC performs dynamic management of groups enabled through PULL and PUSH support
- **Resulting standard** has no specifics for power systems and **can be applied also in other domains**

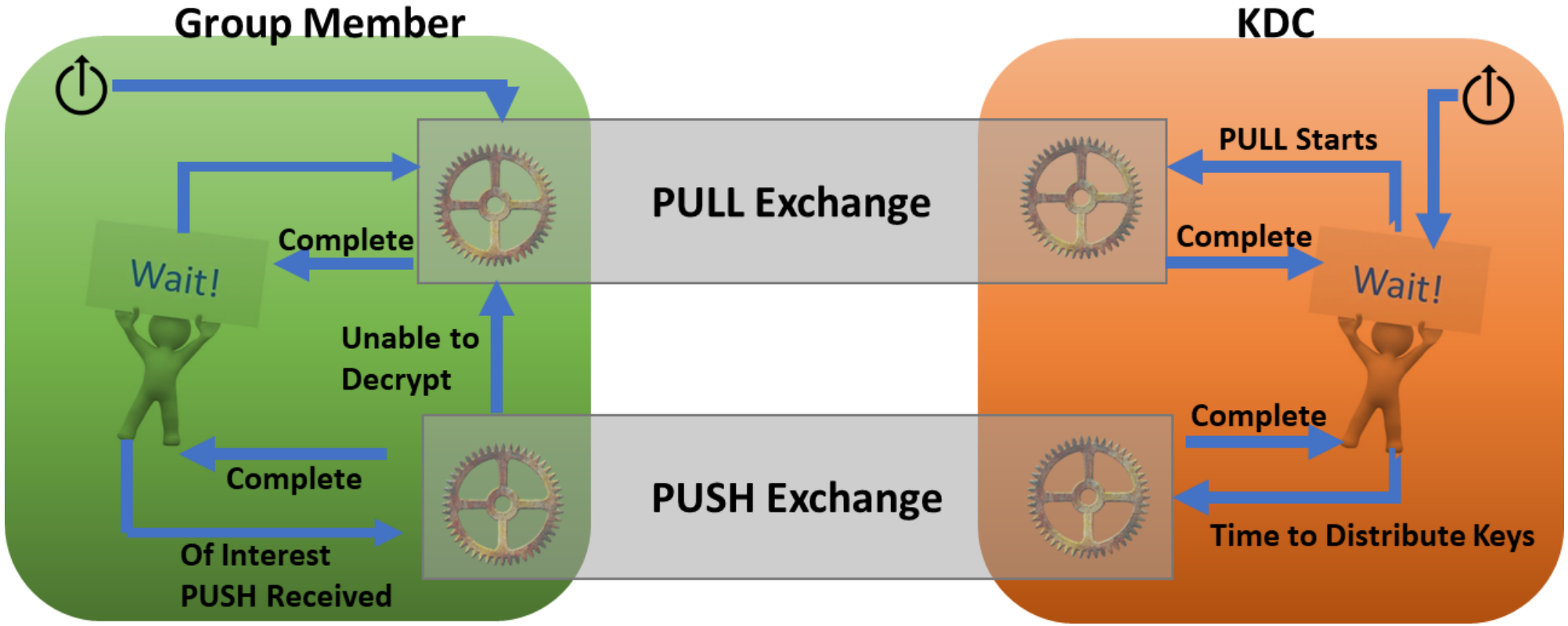


Group Key Management supporting PTP Security Option
OT Centric application of IEC 62351-9 GDOI

- Policies: Set by utilities
  - Authentication and integrity protection is mandatory
  - Encryption optional
  - Key rotation period
- Two keys (Current & Next) and policies are delivered simultaneously, which protects 2x the rotation period during outages
- Enhanced resiliency
  - Key Delivery Assurance (KDA) allows the Key Distribution Server (KDC) to know which devices have received keys, and can be configured to pause Key Rotation based on a percentage of confirmed recipients
- Redundant KDCs

Group Key Management supporting PTP Security Option

IEC 62351-9 GDOI can support Large Deployments



Push can be a multicast and reach 1000s of devices with a single message

Group Key Management supporting PTP Security Option
Eco-system (adoption)

- Source code for GDOI clients
  - JP Embedded, Triangle Microworks, SISCO
- For IEC 61850 GOOSE,R-GOOSE, etc.
  - Devices: GE, Schneider Electric, Siemens, Toshiba, and other vendor(s) that are to remain nameless.
  - Monitoring/Testing: Triangle MicroWorks, Doble, Nozomi (IDS)
  - KDC: PCItek
  - Integrator(s): G&W
- Several companies are known to be adding support for these technologies

Summary

- PTP is vulnerable to
  - Message manipulation
  - Message injection
- PTP security components
  - AUTHENTICATION TLV – protects message integrity
  - Automated key management – Scales to large networks, verifies PTP node authorization
- Group-based key management supported by IEC 62351-9 enhancing GDOI
  - Easiest key management to configure
  - Allows TCs to be part of security mechanism
  - IEEE 1588d-2023 amendment describes use of GDOI with PTP

Contacts

Steffen Fries
Principal Engineer
Siemens, Technology, Germany

E-mail steffen.fries@siemens.com

Herb Falk
Managing Director
Outside the Box Consulting, USA

E-mail herb.falk@otb-consultingservices.com

Andreas Güttinger
Security Architect
Siemens, Smart Infrastructure, Germany

E-mail: andreas.guettinger@siemens.com

Doug Arnold
Principal Technologist
Meinberg, USA

E-mail: doug.arnold@meinberg-usa.com

Andrej Görbing
System Architect Communication
Siemens, Smart Infrastructure, Germany

E-mail: andrej.goerbing@siemens.com

SIEMENS

Backup

Time Synchronization using the Precision Time Protocol (IEEE 1588)

PTP Security Threats and Requirements

Security Threats

- Unauthorized manipulation of synchronization messages to influence time-based execution and audit
- False Grandmaster
  - With false Clock Quality values and/or low Priority1 value.
  - Wins BMCA
- Other PTP message injection
  - Replay attack
  - Impersonate Grandmaster

Security Requirements

- Fundamental Requirements
  - Identify and authenticate PTP Instances
  - Detect unauthorized changes of PTP messages
- Boundary conditions
  - Support of unicast und multicast message delivery
  - Transparent clocks → intermediate components (switches) change PTP message (correction value)
  - Automated key management to scale for large networks

PTP Security Discussion
Importance of AUTHENTICATION TLV proven experimentally

- Recent Research by Marist College and IBM
  - Experimentally demonstrated attacks with injected and manipulated messages in PTP networks
  - Tested both ptp4l (open source) and commercial PTP implementations
  - Both injected and manipulated messages were rejected when they did not have an AUTHENTICATION TLV message with a correct ICV
  - See for example:

L. McPadden, E. Herrera, C. Decusatis, P. Wojciak, C. Kaiser, S. Guendert, "Covert Channels and Data Injection Vulnerabilities for IEEE 1588 Precision Time Protocol using PTP4L," Proceedings of the 55th Annual Precise Time and Time Interval Systems and Applications Meeting, pp 77-86, Long Beach CA, January 2024.

Covert Message Channels and Attack Vectors for IEEE Precision Time Protocol

Luke Jacobs *, Casimer DeCusatis *, Paul Wojciak **, Clay Kaiser **, and Steve Guendert **
* Marist College, Poughkeepsie, NY
** IBM Corporation, Poughkeepsie, NY USA

Abstract— **The IEEE 1588 standard, known as Precision Time Protocol (PTP), is an emerging candidate for high precision timing and clock distribution networks. We present experimental results from a PTP test bed that demonstrate new types of covert channel communications, which allow PTP protocol to be used for data exfiltration and other network communication that violates the implemented cybersecurity policy. We then expand upon this work to demonstrate two new zero-day vulnerabilities in the PTP protocol, and develop proof-of-concept exploits for these attacks. In one attack, we demonstrate a novel man-in-the-middle (MITM) packet injection exploit against the PTP network that produces large, incorrect timing offsets at PTP timeReceiver nodes. In a second attack, we demonstrate the use of specific meta-data payloads to generate large time Transmitter (i.e. master clock) offsets, and to manipulate not just the clock offset but the actual clock frequency itself. We also investigate proposed mitigation techniques, including the use of NTS secured NTP with PTP concurrently which is suggested by some of our experimental results using Timemaster.**

Keywords—PTP, NTP, timing, cybersecurity

Introduction

1. **Introduction**

The IEEE 1588 standard, known as Precision Time Protocol (PTP) [1], is an emerging candidate for high precision timing networks, including clock distribution and synchronization. It is a follow-on to the widely used Network Time Protocol (NTP) [2] in applications which require enhanced timing performance. Many enterprise-class data centers, telecommunications back haul systems, cloud service providers, high performance computing applications, and others rely on a timing subsystem that is used to synchronize networked servers and other data processing equipment. Theoretically NTP can achieve timing accuracy of up to 1 ms, although in practice accuracies of tens to hundreds of ms are fairly common. Recently, a need for more accurate time synchronization has emerged. According to recent regulatory requirements in the financial sector [3,4], servers must be synchronized to within 50 - 100 millisecond drift tolerance of the NIST atomic clock, while proposed standards call for tolerances as low as 1 microsecond in some applications. These timing synchronization requirements are significantly lower than a standard NTP implementation can achieve. While some vendors have developed proprietary timing protocols that partially address these needs, they require additional wiring infrastructure that can be costly and problematic to deploy, and are often incompatible with extended distance fiber optic wavelength multiplexing links and software-defined network (SDN) controllers. Thus, there is a strong desire to design future timing networks around an open industry standard clock protocol with improved accuracy, such as the PTP protocol. In a previous paper [5], we described three security vulnerabilities in the current release of PTP, and discussed potential mitigation techniques.

In this paper, we present experimental results from a PTP test bed that demonstrate new types of covert channel communications, which allow the PTP protocol to be used for data exfiltration and other network communications that violate the implemented cybersecurity policy. We then expand upon this work to demonstrate two new zero-day vulnerabilities in the PTP protocol, and develop proof-of-concept exploits for these attacks. In one attack, we demonstrate a novel man-in-the-middle (MITM) packet injection exploit against the PTPv2 network which is used to produce large, incorrect timing offsets at PTP timeReceiver nodes. In a second attack, we demonstrate the use of specific meta-data payloads to generate large timeTransmitter clock offsets (i.e. master clock; note that at the time of this writing, IEEE standard notation for PTP4L systems as used in this testing refers to the master clock, while emerging standards plan to use timeTransmitter notation for this feature; in order to avoid confusion, we have been advised to continue using the master clock notation for this paper). Further, we can manipulate not just the clock offset but the actual clock frequency itself. We also discuss proposed mitigation techniques for these vulnerabilities.

2. **Covert channels in PTPv2**

A covert channel refers to a communication path used to transfer information between processes that are normally not allowed to communicate with each other under the current cybersecurity policy. Since a covert channel was not designed for communication, it often exhibits low data rates and lacks features normally associated with a communication channel, such as redundancy, retransmission, or error

Abstract

The reliability of critical infrastructures such as electric power distribution, industrial automation, intelligent traffic control, or telecommunications strongly depends on the authenticity and integrity of the communicated data. Further requirements may relate to the confidentiality of communicated information, but also to monitoring and audit information, which is important to analyze events in the aftermath of an at-tack. Many of the security mechanisms employed rely on time information for synchronization of events or for verifying the security of utilized credentials. This makes the time synchronization information crucial as base for other system security services.

Two main message-based time synchronization protocols are currently in use. The Network Time Protocol (NTP, cf. [1]), provides accuracy in the millisecond range, while the Precision Time Protocol (PTP, IEEE 1588, including domain specific profiles) provides accuracy in the microsecond or even nanosecond range.

NTP started as early as 1992 with protocol inherent security considerations, which have evolved over the years. Network Time Security (NTS, cf. [2]) is the latest solution for managing necessary security parameter for client-server interaction.

PTP supports protocol inherent security means since the 2019 version of IEEE 1588 (cf. [3]). The late introduction of security may relate to the fact that PTP is often use in environments, which are either physically separated or are connected via distinct security protocols. To utilize the security defined in IEEE 1588, a key management is necessary to distribute security parameters and the associated security policy. PTP is special regarding the inherent support and use of multicast communication to distribute the time in-formation. This poses specific requirements to the key management.

In power system automation, communication security is required to protect against threats to this critical infrastructure. Standardization of related security is done in the IEC Technical Committee 57 in Working Group 15 (IEC TC57 WG15). Here security mechanisms for point-to-point communication and multicast communication are profiled or defined if necessary. This also involves the key management for multicast security. In this respect, the group-based key management Group Domain of Interpretation (GDOI, cf. [3]) has been enhanced to accommodate the security parameter provisioning for power system specific multicast protocols and also for PTP in IEC 62351-9 (cf. [5]). Security of PTP and the associated key management is currently also considered in the revision of the PTP power utility automation profile in IEC 61850-9-3 (cf. [6]). IEC 61850-9-3 specifies a PTP profile, which allows compliance with the highest synchronization classes of IEC 61850-5 (Communication requirements) and IEC 61869-9 (substation communication architecture). Since GDOI is a general group key management protocol, the enhancements defined in IEC 62351-9 to distribute PTP security parameters may also be leveraged in other application domains, be-sides the power system automation domain.

The Talk is intended to provide an overview about the standardized technical approach from IEC 62351-9 and show implementations of the chosen solution.

REFERENCES

[1] D. Mills et al., " Network Time Protocol Version 4: Protocol and Algorithms Specification," IETF RFC 5905, June 2010.

[2] D. Franke et al., "Network Time Security for the Network Time Protocol," RFC 8915, IETF RFC 8915, September 2020.