ENGINEERING REPORT

Security in SMPTE ST 2059: Threats, Controls and Mitigation Strategies

SMPTE ER 1009:2023

The home of media professionals, technologists, and engineers.

SMPTE ER 1009:2023

SMPTE ENGINEERING REPORT

Security in SMPTE ST 2059: Threats, Controls and Mitigation Strategies

Table of contents Page

445 Hamilton Ave., White Plains NY 10601, (914) 761-1100
Approved March 24, 2023

1 Introduction

1.1 Overview

This Engineering Report (ER) is pursuant to a request from the Joint Task Force on Networked Media Administration Group.

TC-32NF SG on Security in ST 2059 began its work in December 2018, directed by SMPTE Standards Development leadership to "*investigate issues surrounding PTP security within a facility; and produce a report identifying both theoretical and observed security risks as well as recommendations for potential mitigation. Recommendations should be constrained to the nature of the mitigation (e.g., operational practice, device behavior, new specifications, new standards, etc.) and should not be solutions."*

This current report is a second report from the SG. While the first report focused on describing the threats, this second report specifies the detection and mitigation strategies for the same.

The scope of the SMPTE Study Group on Security in SMPTE ST 2059 can be found in Annex A.

1.2 What do we mean by Information Security?

Formally, Security of information and information systems is assured by the so-called Triad of: Confidentiality, Integrity, and Availability (CIA).

- Confidentiality ensures that information cannot be accessed without authorization.
- Integrity ensures that the information is complete and has not been tampered with.
- Availability ensures that information can be accessed by authorized systems and users in a timely manner.

"Timely manner" takes on special meaning within the context of this report. Nobody notices or cares if a web page loads 20 ms faster or slower, but an essence stream whose framing jittered by this amount would be completely unusable. Indeed, it would fail the Integrity and Availability criteria. PTP, the technology used to ensure accurate and reliable essence timing thus underpins two of the main pillars of Information Security in a production context and securing it is the motivation and focus of this report.

1.3 Threat Dynamics and Attacker Goals

The production industry is undergoing a technology transition as fundamental as the analog-to-digital transition that started in the 1980s. This time, the transition affects how content is moved and processed with special-purpose solutions being supplanted by general-purpose IT. Content increasingly moves as packets on TCP/IP networks and is processed by software running on mass-market operating systems. This means that production operations' threat surface has grown much larger and become more susceptible to attack. For example, there are numerous public examples of content producers being successfully targeted by mission critical attacks in the past five years. The motivation can be financial, or ideological and the attackers are increasingly highly skilled, well-funded, patient, and professional. The correct fiduciary response to the increased level and sophistication of threats is to understand the threats in detail and deploy controls to counter them. This report aims to model such a response for PTP usage within production operations.

Why do we need a whole report about securing PTP? It's because many aspects of broadcast production rely on knowing the correct time to within a few μs. This provides an attack on the sources, distribution, and accuracy of timing, the potential to cause broad-based damage. This report addresses the multiple ways in which an attacker could target PTP, and suggests detection, prevention, and resolution controls for each of them.

1.4 What's Special About Media Networks?

The hardware, operating systems and other components in a media network are the same as you'd find in any other private, enterprise class network. It's the business requirements and the methods used to meet them that accord media networks "special" status and treatment. At a high level, the business requirements are clear pictures and sound, reliable metadata, and accurate conformance to the playout schedule; and their realization in today's state of the art IP production facility relies on:

- Up to thousands of high bandwidth (~3Gb/s) RTP streams comprised of packets that must be presented to the physical layer at precise times. [SOURCE ST 2120-21 Compliance Models]
- Signal processing systems that must synchronize their inputs with upstream devices
- Automation systems that must accurately cue and play essence with frame accuracy by sending control commands over the network

These processes fail without access to accurate and reliable timing – how is it provided?

Before IP-based production, a reference timing signal, "genlock," was distributed to each device via dedicated cabling. Today it is accomplished using the SMPTE ST 2059-1 and ST 2059-2 standards. These standards build on the IEEE 1588 standard for Precision Time Protocol, which distributes timing and synchronization information over the network. Using these standards, each process agrees precisely on each stream element's start time and uses an accurate clock to know when it has occurred.

If the processes listed here fail, the business requirements cannot be met resulting in potentially catastrophic impacts to revenues and reputation.

1.5 What can I do about it?

There are sophisticated threat actors with financial or ideological goals that see disrupting or disabling your IP-based production facility as a way to fulfill them. They know that compromising the timing generation and distribution would have broad-based effects. By reading and acting on this report you can:

- Get a high-level understanding of PTP and the SMPTE ST 2059 standards that define its use in an IP production context
- Understand the threats that are special to PTP
- Learn how to effectively counter those threats

… and reduce the likelihood of the revenue and reputation losses caused by a successful attack.

2 Terms and Definitions

Note that IEEE Std 1588-2008 remains an authoritative reference for interested readers. The updated version, IEEE Std 1588-2019 is referenced in this document in cases where there are material differences between it and the older standard. For the purposes of this document, the terms and definitions given in IEEE Std 1588-2008 and IEEE Std 1588-2019, and the following apply:

2.1
Best Master Clock Algorithm
BMCA

default algorithm defined in IEEE Stds 1588-2008 subclauses 9.3.2, 9.3.3, and 9.3.4 that compares data describing two clocks to determine which data describes the better clock and computes a recommended state for each port involved

2.2
Boundary Clock
BC

clock that has multiple Precision Time Protocol (PTP) ports in a domain and maintains the timescale used in the domain. It can serve as the source of time, i.e., be a leader, and can synchronize to another clock, i.e., be a follower

[SOURCE: IEEE Std 1588-2008, 3.1.3, with modified terminology]

2.3
clock

device that can provide a measurement of the passage of time since a defined epoch

[SOURCE: Approved Draft IEEE Std 1588-2019, 3.1.4]

2.4
Denial of Service
DoS

attack in which one or more machines target a victim and attempt to prevent the victim from doing useful work

[SOURCE: RFC 4732, Introduction]

2.5
epoch

origin of a timescale

[SOURCE: IEEE Std 1588-2019, 3.1.12]

2.6
follower

clock in the context of a Precision Time Protocol (PTP) communication path that synchronizes to a source of time

Note 1 to entry: Referred to as ‘slave’ in IEEE Std 1588-2008.

2.7
Global Navigation Satellite System
GNSS

one or more constellations of satellites providing signals from space that transmit positioning and timing data

2.8
grandmaster
GM

clock within a Precision Time Protocol (PTP) domain that is the ultimate source of time for clock synchronization using the PTP as defined in IEEE Std 1588-2008

2.9
leader

clock in the context of a single Precision Time Protocol (PTP) communication path, that is the source of time to which all other clocks on that path synchronize

Note 1 to entry: Referred to as ‘master’ in IEEE Std 1588-2008.

2.10
management message

PTP message defined for the purpose of configuring and/or monitoring PTP Nodes and PTP Instances

[SOURCE: IEEE Std 1588-2019, 3.1.56]

2.11
Man-in-the-Middle
MITM

form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association

[SOURCE: RFC 4949, 4]

2.12
Ordinary Clock

PTP Instance that has a single PTP Port in its domain and maintains the timescale used in the domain

Note 1 to entry: An Ordinary Clock can serve as a source of time, i.e., contain a Leader Clock, or alternatively, the local PTP Clock of an Ordinary Clock can be synchronized, i.e., be a Follower Clock, to the local PTP Clock of a Boundary Clock or another Ordinary Clock in the domain.

[SOURCE: IEEE Std 1588-2019, 3.1.40, with modified terminology, modified — Note 1 to entry has been added.]

2.13
Precision Time Protocol
PTP

protocol defined by IEEE Std 1588 that provides precise synchronization of clocks in packet-based networked systems

Note 1 to entry: The protocol generates a hierarchical relationship among the PTP Instances in the system. The clocks in all PTP Instances ultimately derive their time from a clock known as the grandmaster.

2.14
primary reference source

GNSS or other atomic clock as a traceable reference for a synchronization and timing system that is considered normative

2.15
Transparent Clock
TC

PTP Instance that measures the time for a PTP event message to transit the PTP Instance, and provides this information to PTP Instances receiving this PTP event message

Note 1 to entry: Peer-to-peer Transparent Clocks also correct for PTP link delay.

[SOURCE: IEEE Std 1588-2019, 3.1.84, modified — Note 1 to entry has been added.]

3 Abbreviated Terms

ACL	Access Control List
BC	Boundary Clock
BMCA	Best Master Clock Algorithm
CIA	Confidentiality, Integrity, and Availability, the three aspects of information and information systems that information security practices protect [SOURCE: NIST Special Publication 1800-25A, December 2020]
COPP	Control Plane Policing
DoS	Denial of Service
DSCP	Differentiated Services Codepoint Priority
GM	Grandmaster
GNSS	Global Navigation Satellite System
MITM	Man-in-the Middle
NTS	Network Time Security
PTP	Precision Time Protocol
QoS	Quality of Service
ST 2059/PTP	The combination of SMPTE ST 2059-1, ST 2059-2, and Precision Time Protocol
SV	Satellite Vehicle, Space Vehicle
TC	Transparent Clock
TLV	Type-Length-Value, Tag-Length-Value

4 Background on PTP and SMPTE 2059

4.1 PTP

IEEE Std 1588 is the “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems”. This standard defines the Precision Time Protocol (hereafter, PTP).

PTP enables precise synchronization of clocks in measurement and control systems implemented with technologies such as network communication, local computing, and distributed objects. The protocol is applicable to systems where devices communicate via networks, including Ethernet. PTP enables heterogeneous systems that include clocks of various inherent precision, resolution, and stability to synchronize to a main or standby grandmaster.

The protocol supports system-wide synchronization accuracy in the sub-microsecond range with minimal network and local clock computing resources. The default behavior of the protocol allows simple systems to be installed and operated without requiring the administrative attention of users. PTP can be transported over both User Datagram Protocol (UDP)/Internet Protocol (IPv4 & IPv6) and directly over layer-2 Ethernet frames. It supports multicast as well as unicast message exchange.

PTP also allows the definition of “profiles” which include the set of allowed PTP features and attribute values applicable for specific use cases.

4.2 SMPTE ST 2059

4.2.1 SMPTE ST 2059-1 Generation and Alignment of Interface Signals to the SMPTE Epoch

ST 2059-1 defines:

1. A point in time, the SMPTE Epoch, which is used for alignment of all real-time signals referenced in the Standard;
2. The alignment of these signals to the SMPTE Epoch;
3. Formulae which specify the ongoing alignment of these signals to time since the SMPTE Epoch;
4. Formulae which specify the calculation of SMPTE ST 12-1 Time Address values and SMPTE ST 309 date values from SMPTE Profile PTP data.

4.2.2 SMPTE ST 2059-2 Profile for Use of IEEE-1588 Precision Time Protocol in Professional Broadcast Applications

SMPTE ST 2059-2 is a PTP profile for use in professional broadcast applications. It specifies:

- Which algorithm to implement to compare clocks to determine the best clock to use as a source of time.
- Which of the configuration management options is to be implemented
- Which of the path delay mechanisms is to be implemented
- The range and default values of all PTP configurable attributes and data set members
- The transport mechanisms required, permitted, or prohibited
- The node types required, permitted, or prohibited
- The options required, permitted, or prohibited

In particular, ST 2059-2:

- Requires the use of UDP over IPv4 or IPv6
- Requires the support of multicast transport, but also allows the use of unicast, and mixed multicast/unicast
- Defines SMPTE Synchronization Metadata regarding items such as frame rate, “daily jam”, and whether “daylight saving” is in effect

4.2.3 Model PTP System Overview Diagram

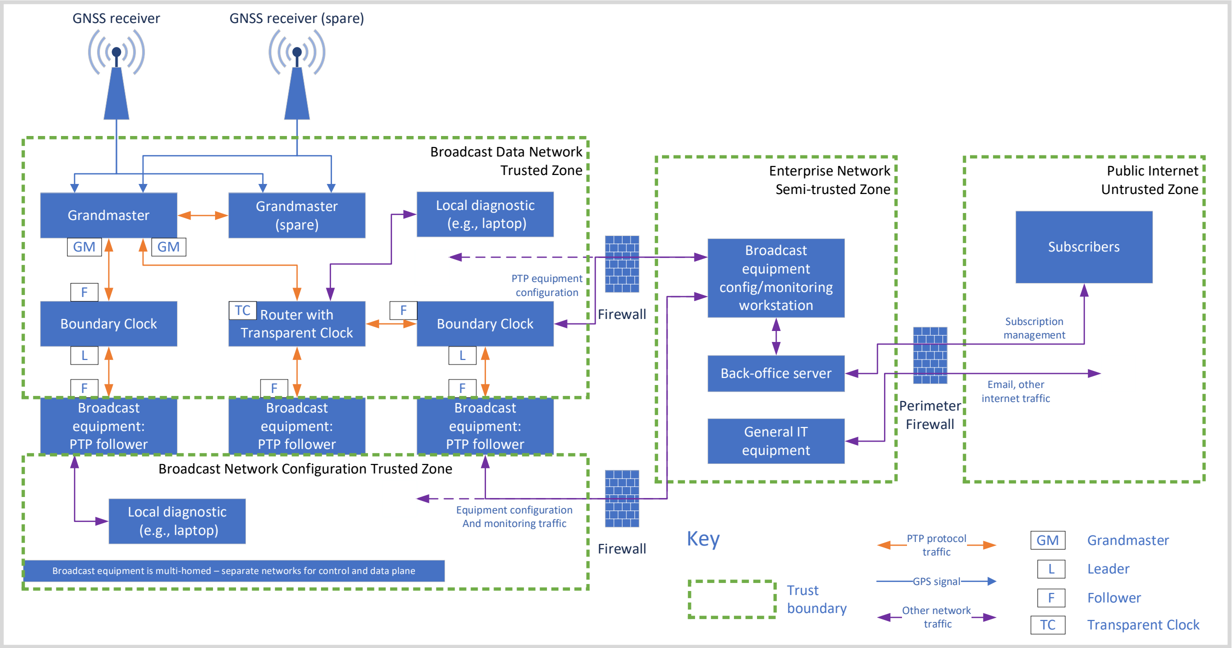


Figure 1 — Model PTP System Overview.

This architecture diagram shown in Figure 1 illustrates the possible composition of a broadcast network, to put into context the security considerations elsewhere in this document. This is but one of many possible architectures, and real users need to consider their specific requirements in network design. For simplicity, this diagram does not show deployment at a realistic scale.

The diagram shows several different network zones. There is a broadcast data network for media traffic. This carries real-time, usually high bitrate traffic between broadcast equipment. It might include compressed and uncompressed media traffic and signaling information to accompany it. In this example architecture, this network also carries PTP protocol traffic. It is also feasible to place the PTP traffic on a separate network from the media traffic, such as the broadcast configuration network, or even a fully isolated network solely for PTP.

A separate broadcast configuration network is typical. This carries configuration traffic to control and monitor the broadcast equipment. This means that broadcast equipment is typically multi-homed, being connected to both the broadcast data network and the broadcast configuration network.

Broadcast equipment seldom exists in an “air gapped” network environment, as used to be the case. Organizations typically want to have supervisory control and monitoring access to the equipment from their enterprise network, which also carries general IT traffic for office functions, and potentially also back-office traffic related to their media business.

The broadcast organization is likely to have access to the public internet for general office IT purposes, and possibly also to allow subscriber access to media services and/or subscription accounts.

The networks can be considered as distinct security “trust zones” The boundaries between trust zones are marked with “trust boundaries”. Each trust zone is assigned a level of trust, depending on the level of risk exposure.

To provide some controlled connectivity between these networks, they are connected via firewalls. These demarcate the security trust zones and will be configured only to allow through traffic with a defined purpose and zone of origination (for example, to allow monitoring of broadcast equipment from the enterprise network).

A PTP network distributes time from a grandmaster to several followers, via a hierarchy of Boundary and Transparent Clocks. This concept, and the different clock types, are explained in SMPTE EG 2059-10:2016.

The architecture diagram is designed to illustrate a variety of PTP Grandmaster, Transparent, Boundary, and Follower Clock connectivity rather than indicating a recommended hierarchy. The design of a PTP network will depend on the scale and distribution of equipment requiring synchronization.

Sometimes diagnostic equipment is connected into the broadcast network for troubleshooting. This is illustrated with a “local diagnostic” connection on both the broadcast data network and broadcast control network.

5 Specific Threats and their Matching Impacts and Controls

5.1 Threat Cards

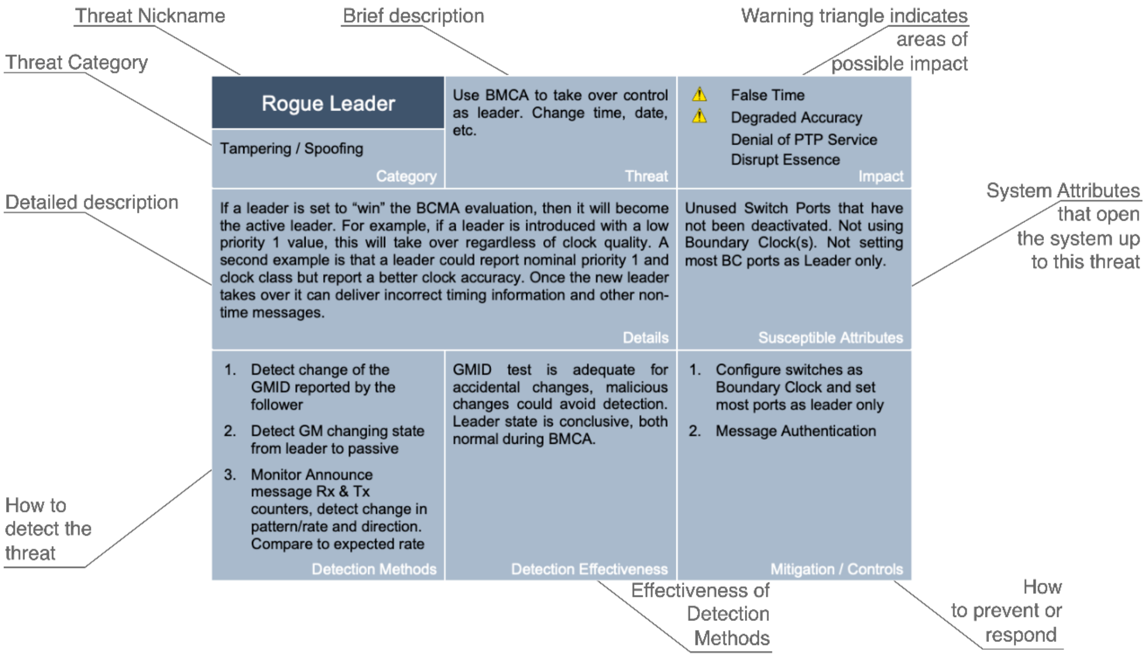
Each specific threat to PTP is summarized as a “Threat Card” to provide a consistent and accessible reference. The card includes information on a detailed description of the threat, methods to detect an attack, methods to prevent or respond to this threat, and the possible impact of the threat. The impact to the time can be:

- False Time - Changes to the system time
- Degrade Accuracy - Disruptions or Degradations in the time distribution
- Denial of PTP Service - Interruptions of the time distribution

… any of which could ultimately cause:

- Disruption of the Essence.

Figure 2 shows an example of a Threat Card.



Threat Nickname
Brief description
Warning triangle indicates areas of possible impact
Threat Category
Detailed description
System Attributes that open the system up to this threat
How to detect the threat
Effectiveness of Detection Methods
How to prevent or respond

Rogue Leader

Tampering / Spoofing

Category

Use BMCA to take over control as leader. Change time, date, etc.

Threat

⚠ False Time
⚠ Degraded Accuracy
Denial of PTP Service
Disrupt Essence

Impact

If a leader is set to “win” the BCMA evaluation, then it will become the active leader. For example, if a leader is introduced with a low priority 1 value, this will take over regardless of clock quality. A second example is that a leader could report nominal priority 1 and clock class but report a better clock accuracy. Once the new leader takes over it can deliver incorrect timing information and other non-time messages.

Details

Unused Switch Ports that have not been deactivated. Not using Boundary Clock(s). Not setting most BC ports as Leader only.

Susceptible Attributes

1. Detect change of the GMID reported by the follower
2. Detect GM changing state from leader to passive
3. Monitor Announce message Rx & Tx counters, detect change in pattern/rate and direction. Compare to expected rate

Detection Methods

GMID test is adequate for accidental changes, malicious changes could avoid detection. Leader state is conclusive, both normal during BMCA.

Detection Effectiveness

1. Configure switches as Boundary Clock and set most ports as leader only
2. Message Authentication

Mitigation / Controls

Figure 2 — Threat Card Explainer.

5.2 through 5.18 describe specific threats, impacts, and controls.

5.2 Rogue Leader

<table>
<tr><td>Rogue Leader
Tampering / Spoofing
Category</td><td>Use BMCA to take over control as leader. Change time, date, etc.
Threat</td><td>⚠ False Time
⚠ Degraded Accuracy
Denial of PTP Service
Disrupt Essence
Impact</td></tr>
<tr><td colspan="2">If a leader is set to “win” the BCMA evaluation, then it will become the active leader. For example, if a leader is introduced with a low priority 1 value, this will take over regardless of clock quality. A second example is that a leader could report nominal priority 1 and clock class but report a better clock accuracy. Once the new leader takes over it can deliver incorrect timing information and other non-time messages.
Details</td><td>Unused Switch Ports that have not been deactivated. Not using Boundary Clock(s). Not setting most BC ports as Leader Only.
Susceptible Attributes</td></tr>
<tr><td>1. Detect change of the GMID reported by the follower
2. Detect GM changing state from leader to passive
3. Monitor Announce message Rx & Tx counters, detect change in pattern/rate and direction. Compare to expected rate
Detection Methods</td><td>GMID test is adequate for accidental changes, malicious changes could avoid detection. Leader state is conclusive, both normal during BMCA.
Detection Effectiveness</td><td>1. Configure switches as Boundary Clock and set most ports as Leader Only
2. Message Authentication
Mitigation / Controls</td></tr>
</table>

5.3 GNSS Spoofing

GNSS Spoofing Tampering / Spoofing Category	Spoof the GNSS to which the GM is locked – change time, date, location, etc. Threat	⚠ False Time ⚠ Degraded Accuracy Denial of PTP Service Disrupt Essence Impact
GNSS signals are weak, and the technology is readily available to either jam the signal so that a receiver cannot get the correct time, or to spoof the received signal [Psiaki, M.L., & Humphreys, T.E.] such that the receiver gets an incorrect time or location. On a regular basis there are reported cases where GNSS signals are interrupted. Details		Antenna near public areas Single constellation and band Susceptible Attributes
1. Monitor Satellite Signal levels – detect sudden increase or too steady over time 2. Monitor GPS location – note if changes 3. Detect SV which should not be present at the current time 4. Compare information from different GNSS constellations Detection Methods	May be able to detect intrusion depending on its sophistication Detection Effectiveness	1. Locate Antenna on top of building away from public streets 2. Use jamming rejection antenna 3. Use anti-spoofing receiver 4. Use multi-band system Mitigation / Controls

5.4 Bad Sync Messages

<table>
<tr><td>Bad Sync Messages
Tampering / Spoofing
Category</td><td>Send extra sync messages with erroneous information
Threat</td><td>⚠ False Time
⚠ Degraded Accuracy
Denial of PTP Service
Disrupt Essence
Impact</td></tr>
<tr><td colspan="2">The PTP sync messages are typically multicast, so if a bad actor injects additional messages which appear to come from the active leader, then the clients may use the timing from both the legitimate and the illegitimate messages. By shifting the time on the injected messages, the bad actor could shift the time derived at the receiver.
Details</td><td>Using switches in non-Boundary Clock mode
Susceptible Attributes</td></tr>
<tr><td>1. Monitor Sync byte rate compared to expected and history. Detect if it does not match the log message period in the messages
2. Monitor for significant time shifts – use Mean Path delay or individual path delays
3. Monitor phase offset
Detection Methods</td><td>Conclusive, good coverage unless masking occurs
Detection Effectiveness</td><td>1. Configure switches to use Boundary Clock mode
2. Implement allow-list to identify valid leaders
3. Message Authentication
Mitigation / Controls</td></tr>
</table>

5.5 Mask Sync Messages

Mask Sync Messages Tampering / Spoofing Category	Send extra sync messages timed to mask the legitimate messages Threat	⚠ False Time ⚠ Degraded Accuracy Denial of PTP Service Disrupt Essence Impact
If a bad actor injects extra sync messages just before the legitimate ones, then some clients may use the injected messages and ignore the legitimate ones. This allows the bad actor better control of the time derived at the client. Details		Using switches in non-Boundary Clock mode Susceptible Attributes
1. Monitor Sync byte rate compared to expected and history. Detect if it does not match the log message period in the messages 2. Monitor for significant time shifts – use Mean Path delay or individual path delays 3. Monitor Phase offset Detection Methods	Test followers to see if masking effect can be induced, if not then conclusive Detection Effectiveness	1. Configure switches to use Boundary Clock mode 2. Implement allow-list to identify valid leaders 3. Message Authentication Mitigation / Controls

5.6 Denial of Service: Leader

DoS Leader Denial of Service Category	Create excess traffic to overpower the ability of the leader to process messages Threat	False Time ⚠ Degraded Accuracy ⚠ Denial of PTP Service Disrupt Essence Impact
A leader must both parse and respond appropriately to PTP messages. If there are too many followers, then a leader might not be able to support them all. Similarly, if a bad actor injects extra delay request messages as if there were many more followers on the network, then the leader might not be able to process all the messages. These overloads can cause the leader to not respond to some legitimate messages. Details		Using switches in non-Boundary Clock mode Susceptible Attributes
1. Monitor the number of missing delay response messages Detection Methods	Seems pretty definitive Detection Effectiveness	1. Use Boundary Clock to limit traffic to the leader Mitigation / Controls

5.7 Denial of Service: Follower

<table>
<tr><td>DoS Follower
Denial of Service
Category</td><td>Create excess traffic to overpower the ability of the follower to parse the messages
Threat</td><td>False Time
⚠ Degraded Accuracy
⚠ Denial of PTP Service
Disrupt Essence
Impact</td></tr>
<tr><td colspan="2">PTP ports must parse all of the received PTP messages to decode the pertinent information. If too many messages are present, then the client may not be able to process all of them. This effect had been observed on nodes with a moderate number of messages per second. This condition can happen accidentally if more followers are added to a network. Alternatively, a bad actor could send enough protocol messages to a follower (such as delay request, delay response, sync) to cause a DoS of the follower stack. Another attack would be spoofed delay requests that cause the leader to send additional delay response messages to the follower, overwhelming it. Monitoring for this attack can be challenging since if the messages were not intended for the device on that port, it would not report the extra messages.
Details</td><td>Using switches in non-Boundary Clock mode
Susceptible Attributes</td></tr>
<tr><td>1. Monitor total PTP message rate from follower
2. Monitor total PTP message rate from GM
3. Monitor total PTP message rate from Switch port
Detection Methods</td><td>Follower may only report messages intended for itself. Switch traffic report seems conclusive.
Detection Effectiveness</td><td>1. Use Boundary Clock to limit traffic to the leader
Mitigation / Controls</td></tr>
</table>

5.8 Message Looping

Message Looping Denial of Service Category	Provoke message looping to overload network devices Threat	False Time ⚠ Degraded Accuracy ⚠ Denial of PTP Service ⚠ Disrupt Essence Impact
Some cases have been observed where PTP traffic is looped back and forth between a spine and a leaf. This seems to occur during some types of network re-convergence possibly linked to PTP port state changeover. The looping of such messages, and specifically SMPTE management messages may overload a device attempting to process these. Details		Devices which do not fully support ST2059-2 Unpatched PTP4L Susceptible Attributes
1. Monitor the rate of the management messages, compare to expected and history 2. Monitor Switch and Device CPU load Detection Methods	Knowing management message rate will detect the condition, but the CPU load is also needed to know if it’s causing a problem Detection Effectiveness	1. Test during commissioning and modify system parameters and/or switch configuration as needed 2. Use COPP to limit the volume of messages 3. Block multicast management messages from media nodes into the network Mitigation / Controls

5.9 Excess Traffic

<table>
<tr><td>Excess Traffic
Denial of Service
Category</td><td>Use management messages to trigger excess traffic
Threat</td><td>False Time
⚠ Degraded Accuracy
⚠ Denial of PTP Service
⚠ Disrupt Essence
Impact</td></tr>
<tr><td colspan="2">Management messages are propagated throughout a BC network and will often cause devices to send a message in response. If the messages and the responses are multicast, this can generate excess traffic which might overload some devices. If the messages are malformed or unsupported, an error response will be triggered. Devices should not respond to the responses, but it is possible that this might occur in flawed implementations. If it did occur, a message storm could result.
Details</td><td>Unrestricted management message support
Susceptible Attributes</td></tr>
<tr><td>1. Monitor the rate of the management messages, compare to expected and history
2. Monitor Switch and Device CPU load
Detection Methods</td><td>Knowing management message rate will detect the condition, but the CPU load is also needed to know if it’s causing a problem
Detection Effectiveness</td><td>1. Test during commissioning and modify system parameters and/or switch configuration as needed
2. Use COPP to limit the volume of messages
3. Block multicast management messages from media nodes into the network.
Mitigation / Controls</td></tr>
</table>

5.10 Rejection Failure

Rejection Failure Denial of Service Category	Exploit followers which cannot reject delay response messages intended for a different follower Threat	False Time ⚠ Degraded Accuracy ⚠ Denial of PTP Service Disrupt Essence Impact
Some followers have been noted to have a bug where they process delay response messages that were triggered by a different follower. This can disrupt the lock on the target follower. This is sometimes manifested as a follower which will only lock to a Boundary Clock. If connected to a leader with other devices, then the follower cannot lock. Details		Using switches in non-Boundary Clock mode Susceptible Attributes
1. Monitor total PTP message rate from follower 2. Monitor total PTP message rate from Switch port 3. For both, detect if different than expected or history Detection Methods	Follower may only report messages intended for itself. Switch reporting seems conclusive. Detection Effectiveness	1. Manage supply. Require vendors to assure that their equipment does not have this bug 2. Configure switches in Boundary Clock mode Mitigation / Controls

5.11 BMCA Thrashing

BMCA Thrashing Denial of Service Category	Cause continuous BCMA cycles to prevent all clients from locking to a leader Threat	False Time Degraded Accuracy ⚠ Denial of PTP Service Disrupt Essence Impact
If a bad actor sends announce messages with better clock quality, then the current grandmaster will back off and stop sending PTP messages. To be more sophisticated, the bad actor could cycle through several dummy Leader Clock IDs on the announce messages, so it would appear as though several leaders were trying to assert their right to be the active leader. This continual BMCA process would prevent all of the clients from getting the correct time. Details		Using switches in non-Boundary Clock mode Susceptible Attributes
1. Monitor lock status on all followers. Report if not locked. 2. Monitor GMID reported by followers – in this case they will be changing often. Detection Methods	Conclusive to detect a problem, may not identify the source Detection Effectiveness	1. Configure switches as Boundary Clock and set most ports as Leader Only 2. Use allow list to identify valid leaders Mitigation / Controls

5.12 Delay / Replay

Delay / Replay Delay / Replay Category	Record messages from a grandmaster and replay them later to skew the time in the followers Threat	⚠ False Time ⚠ Degraded Accuracy Denial of PTP Service Disrupt Essence Impact
Record messages from a grandmaster and replay them later to skew the time in the followers. Details		Unused switch ports that have not been deactivated Not using Boundary Clock mode Not setting most BC ports as Leader Only Running PTP outside protected plant such as over public networks or WAN Susceptible Attributes
1. Monitor lock status on all followers – will see unlock 2. Monitor phase offset – will see time shift Detection Methods	Any significant abrupt shift should be detected Detection Effectiveness	1. Configure switches in Boundary Clock mode and set most ports as Leader Only Mitigation / Controls

5.13 Man-in-the-Middle

MITM Man-in-the-Middle attacks Category	Intercept and modify PTP messages to modify time, date, BMCA parameters, domain, etc. Threat	⚠ False Time ⚠ Degraded Accuracy Denial of PTP Service Disrupt Essence Impact
This could happen at a switch, BC, etc. Details		PTP outside protected plant such as over public network or WAN Susceptible Attributes
1. Monitor for significant time shifts 2. Monitor for changes in Mean Path Delay Detection Methods	Either approach may cover this – depends on the attack. It's hard to detect slow shifts in timing. Detection Effectiveness	1. Message Authentication Mitigation / Controls

5.14 Change Leader Priority

Change Leader Priority

Management Messages

Category

Use management messages to change priority on a leader

Threat

⚠ False Time
Degraded Accuracy
Denial of PTP Service
Disrupt Essence

Impact

A management message TLV can set the values of priority1, priority2, and clockAccuracy in such a way as to cause an undesired device to be chosen as grandmaster by the BMCA. Note that not all PTP devices allow management messages to change their data sets.

Details

Devices which support management message configuration

Unrestricted management message support

Susceptible Attributes

1. Monitor Priority 1 & 2 reported by the followers
2. Detect change of GMID reported by follower
3. Detect GM changes state from active to passive

Detection Methods

All three should detect this. Several priority levels are normal in most systems so that can be less definitive.

Detection Effectiveness

1. Disable changing dataset with management messages or block these messages

Mitigation / Controls

5.15 Privilege Elevation

Privilege Elevation

Management Messages

Category

Use management messages to change a device from Follower Only to Ordinary Clock

Threat

⚠ False Time
Degraded Accuracy
Denial of PTP Service
Disrupt Essence

Impact

A management message TLV can change the value of defaultDS.slaveOnly to allow an undesired PTP device to become leader.

Details

Devices which support management message configuration

Unrestricted management message support

Susceptible Attributes

1. Monitor the Follow Only state on all followers
2. Monitor Priority reported by followers
3. Detect change of GMID reported by follower
4. Detect GM changes state from active to passive

Detection Methods

All four should detect this. Several priority levels are normal in most systems so that can be less definitive

Detection Effectiveness

1. Configure switches as Boundary Clock and set most ports as Leader Only
2. Disable changing dataset with management messages

Mitigation / Controls

5.16 Misconfigured QoS

Misconfigured QoS

Management Messages

Category

Excess traffic can cause PTP message loss

Threat

False Time
Degraded Accuracy
⚠ Denial of PTP Service
Disrupt Essence

Impact

In non-Boundary Clock switches, PTP traffic should always be the highest priority traffic in the network. If other traffic is not correctly prioritized lower than PTP then the PTP traffic will be delayed.

Details

Overloaded systems not set up with QoS to prioritize PTP over other traffic

Not using switches in Boundary Clock mode

Susceptible Attributes

1. Monitor the message rates, detect if not as expected, if they change over time, or if they do not agree with the rate stated in the messages

Detection Methods

If a significant percentage of messages is lost, then this should detect it

Detection Effectiveness

1. Configure switches in Boundary Clock mode to isolate timing traffic
2. Monitor traffic in network
3. Use DSCP and QoS to prioritize PTP traffic

Mitigation / Controls

5.17 Misconfigured Switch

Misconfigured Switch

Management Messages

Category

Change the configuration on the switch to disrupt PTP

Threat

False Time
⚠ Degraded Accuracy
⚠ Denial of PTP Service
Disrupt Essence

Impact

Any switch configuration that can impact PTP, for example, applying an ACL, or changing domain can cause disruption in the PTP traffic.

Details

Systems which do not protect switch configuration

Susceptible Attributes

1. Monitor message rates in devices
2. Monitor lock status of devices

Detection Methods

The effectiveness of these detection methods depend on what switch setting was changed

Detection Effectiveness

1. Control and monitor access to the switch

Mitigation / Controls

5.18 Media Node

Media Node	Change the configuration on the Media Node to disrupt PTP Threat	⚠ False Time Degraded Accuracy Denial of PTP Service Disrupt Essence Impact
Management Messages Category		
One example of a configuration change is changing a media node's PTP domain which will cause it to unlock from the intended PTP leader. Details		Systems which do not protect switch configuration Susceptible Attributes
1. Monitor messages rates in devices 2. Monitor lock status of devices Detection Methods	The effectiveness of these detection methods depends on what media node settings were changed Detection Effectiveness	1. Control and monitor access to media node Mitigation / Controls

6 Vulnerabilities that can Compromise Networks

6.1 Overview

While PTP systems can be designed and configured securely, some operational practices and network configurations have the potential to undermine a previously secure setup.

The model system in Figure 1 — Model PTP System Overview shows an isolated network which is the ideal configuration from an information security perspective. However, in practice this may not always be possible, and isolated networks may become coupled to others by malicious action or by accident, or allow covert data transfer. Following in 6.2, 6.3, 6.4, and 6.5, are four specific mechanisms by which this can happen.

6.2 Network Bridging

Network Bridging	Plug in a Wi-Fi enabled laptop thereby bridging the PTP and other networks Likely accidental rather than malicious Access Pathway
Private Network Breaches Category	
If a user connects a device such as a laptop to the trusted network, and that device also has Wi-Fi enabled, then potentially that could bridge the two networks and provide access for attacks from the less secure network. Details	

6.3 Device Control Misuse

Device Control Misuse	Attack a device via the control port and gain access / control on the PTP port Access Pathway
Private Network Breaches Category	
Many devices have connections to both the data and control networks. Potentially an attack could be made from the control side and gain access to the data network. Details	

6.4 Connect Insecure System

Connect Insecure System	Connect the trusted PTP network to another system such as an OB van Access Pathway
Private Network Breaches Category	
In some operational situations a trusted network must be connected to outside systems. An example is an OB van needing access to the PTP/Data network. This can be a possible source of access if the outside system is not secure. Details	

6.5 PTP as Exfiltration Vector

PTP as Exfiltration Vector	PTP can be used as a covert data channel which, although not high in bandwidth, could be used to exfiltrate valuable data such as passwords, SSH keys etc. Access Pathway
Confidentiality Category	
The PTP packet header can be used as a covert communication channel, e.g., using the correction field. This communication can be bidirectional, e.g., using delay_request and delay_response messages. Detection of the covert communication channel can be accomplished by careful detailed analysis of the PTP packet header fields; however, this has limited effectiveness and is not practical in most applications. The covert communication channel can be mitigated by using Boundary Clock switches. Details	

7 Best Current Practices

While each threat in Clause 6 needs to be considered within the context of your system, the best current practices in this clause apply to most systems and provide a good starting point in securing yours.

All equipment in a network should be protected with strong password authentication at a minimum, and, ideally multi-factor authentication, to prevent malicious/inadvertent configuration changes. This includes both the GUI and API interfaces. The GM and switches are the most critical to protect since they have the greatest impact. All switch accesses as well as configuration changes must be logged and preserved. This recommendation is one of the most important in securing a PTP system.

Using switches in PTP Boundary Clock mode is the preferred implementation of PTP in an IP fabric. This provides a fair amount of isolation between the media nodes or GM and also distributes the overall load across all the network switches.

Boundary Clock interfaces that are not designed to have GM connected to them, either directly or via other switches, should be set to “Leader/Master Only” mode. This feature blocks an interface being used in the BMCA selection. While this feature was introduced in IEEE 1588:2019, it is available in most IEEE 1588:2008 switches. This recommendation is one of the most important in securing a PTP system.

PTP management messages should be restricted to only the features that are required by your system, e.g., prevent management messages that change device’s dataset parameters. Restrict the use and distribution of multicast management messages to only the paths that require them. All multicast management response messages should be blocked.

If GNSS is used by the GMs for the time source, the antennas should be protected against jamming and spoofing attacks. You should use two antennas, with each connected to just one of the dual redundant data networks per ST 2022-7. You should use dual band receivers that can receive multiple constellations. You should use antennas with anti-jamming and spoofing features.

In a multi-site deployment, sometimes there is a requirement to extend PTP across sites. The external interfaces need to be protected. The most secure is to block external PTP packets from entering a site and use a separate GM at each site.

It is recommended to have a PTP monitoring system because this should detect changes to the system time, disruptions or degradations in the time distributions or interruptions of the time distribution. SMPTE RP 2059-15, which is under development at time of writing, standardizes the parameters to monitor.

One must configure only the switch interfaces that are in use, and spare interfaces must be disabled. All switch configurations should be deliberate, and any default configuration should be avoided/cross checked.

Switches should be configured with “allow list” host access policies, so that by default all traffic is denied through the switch and only the allowed set of endpoints can send/receive through the network.

8 A Peek into the Future of PTP Security

8.1 Overview

Like most network standards, PTP and network security is always evolving. Let’s take a look at how in closing this report.

8.2 Secure by Design, Secure by Default, IEEE 802.1X (RADIUS) Networking

This mature technology addresses the problem that devices can receive and transmit data as soon as they are physically connected to the network. This means that they can attack the network too. The RFC adds defense in depth by defining a mechanism to control physical access to a network port. It defines three network access control entities:

- Supplicant: A device connected to a network port (wired or wireless) that seeks to be authenticated by a network Authenticator.

- Authenticator: An entity that facilitates the authentication process. This is often the network equipment (e.g., the switch) that is connected to Supplicant directly.

- Authentication Server (AS): An entity that provides an authentication service to an Authenticator. This service determines, from the credentials provided by the Supplicant, whether the Supplicant is authorized to access the services provided by the system in which the Authenticator resides. The Authentication Server function can be co-located with an Authenticator, or it can be accessed remotely via a network to which the Authenticator has access.

Switch ports are in a “blocked” state by default, which disables any data path between it and a newly connected device, which is effectively isolated. Once authenticated the port opens and the device is admitted to the network.

IEEE 802.1X is supported by all major enterprise switch vendors and operating systems in widespread use. However, the complexity of managing the certificates has limited its adoption.

If you want to control against untrusted devices being connected to your network, IEEE 802.1X could be a very effective tool if supported by media nodes.

8.3 IEEE 1588 Recommendations

IEEE1588:2019 annex P has four main “prongs,” A to D, of possible security improvements for PTP:

A. Message Authentication TLV and associated Key management system.
B. External Transport Message Security, e.g., MACsec and IPsec.
C. Network enhancements like redundant Leaders and segmented networks
D. Monitoring and Management

Prong A is actively being developed by IEEE, IETF and other groups with progress being reported via papers at recent conferences. Much of the work is focused on extensions to RFC8915, which is “NTS”, the key-based security for NTP, and defining the Key authentication mechanisms.

Prong B (MACsec and IPsec) may make sense in some profiles, but does not seem to be gaining traction in the broadcast industry.

Prong C utilizes some new optional features in IEEE1588:2019, specifically for redundancy. Since video networks already use some forms of redundancy this may be attractive if devices start to support the additional features from the 2019 version. Currently the SMPTE PTP profile does not specify any of the new optional features.

Prong D. Monitoring and Management. One advance in this area is the ongoing development of SMPTE RP 2059-15 which is a YANG model to standardize reporting of PTP and device related information. The intent is to make it easier to monitor all the PTP connected devices in a network by creating a common data structure. As pointed out in IEEE1588:2019 annex P and the Threat Cards in this report, monitoring aspects of the PTP system can detect many forms of intrusion and facilitate corrective measures.

Annex A Scope of the SMPTE Study Group on Security in SMPTE ST 2059

A request from the Joint Task Force on Networked Media Admin group was received on 2018-08-10 as follows:

The following areas may require attention from JT-NM Coordination Group members in order to improve security around PTP. It may be appropriate for the JT-NM to call on these bodies to create appropriate technical documents within their respective scopes in order to improve the security and reliability of PTP, which is critical to IP-based media facilities. Areas of investigation:

- Ways to harden PTP infrastructure against the assumption of the role of PTP grandmaster by a rogue device
- Ways to harden the network against PTP attacks generally (e.g., rogue management TLV messages or other intentional attacks, changing PTP time)
- Ways to improve recovery time when power is restored to a facility with a large number of PTP devices and whether this scenario causes a particular issue for PTP devices
- Appropriate best practices regarding the design of PTP networks to reduce the likelihood of an attack against critical PTP infrastructure
- Appropriate test methods to ensure devices implement recommendations from the various Coordination Group members
- Methods for detecting that attacks are occurring

The Study Group should investigate issues surrounding PTP security within a facility. The SG should produce a report identifying both theoretical and observed security risks as well as recommendations for potential mitigation. Recommendations should be constrained to the nature of the mitigation (e.g., operational practice, device behavior, new specifications, new standards, etc.) and should not be solutions.

References and Bibliography

IEEE 802.1X:2020. “IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control”

IEEE, IEEE Std 1588-2008. “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems”

IEEE, IEEE 1588-2019. “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems”

IETF RFC 7384. “Security Requirements of Time Protocols in Packet Switched Networks”

Itkin, E. and Wool, A. “A Security Analysis and Revised Security Extension for the Precision Time Protocol,” IEEE Transactions on Dependable and Secure Computing. doi: 10.1109/TDSC.2017.2748583

Jacobs L., DeCusatis C., Wojciak P., Kaiser C., & Guendert S. “Covert Message Channels and Attack Vectors for IEEE Precision Time Protocol,” IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS), 2022 https://ieeexplore.ieee.org/document/9918524

NIST “Special Publication 1800-25A,” December 2020

Psiaki, M.L., & Humphreys, T.E. (2016). “GNSS Spoofing and Detection. Proceedings of the IEEE,” 104, 1258-1270.

SMPTE, ST 2059-1:2020 “Generation and Alignment of Interface Signals to the SMPTE Epoch”

SMPTE, ST 2059-2:2020 “SMPTE Profile for Use of IEEE-1588 Precision Time Protocol in Professional Broadcast Applications”

SMPTE, EG 2059-10:2016, “SMPTE Engineering Guideline - Introduction to the New Synchronization System”

SMPTE, RP 2059-15:2023 Public CD “YANG Data Model for ST 2059-2 PTP Device Monitoring in Professional Broadcast Applications,” retrieved from https://github.com/SMPTE/rp2059-15

SMPTE, ST 2110-21 “Professional Media Over Managed IP Networks: Traffic Shaping and Delivery Timing for Video”

Treytl, A., and Hirschler, B. “Security flaws and workarounds for IEEE 1588 (transparent) clocks,” 2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication, Brescia, 2009, pp. 1-6.

Treytl, A, Gaderer, G., Hirschler, B., and Cohen, R. “Traps and pitfalls in secure clock synchronization,” 2007 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication, Vienna, 2007, pp. 18-24.