SMPTE ENGINEERING REPORT

Report of the Study Group On Security in SMPTE ST 2059 – Threat Landscape

SMPTE ER 1005:2021

The home of media professionals, technologists, and engineers.

SMPTE Engineering Report

Report of the Study Group On Security in SMPTE ST 2059 - Threat Landscape

Table of Contents **Page**

Approved **October 13, 2020**

1 Introduction

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."*

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

1.1 What do we mean by Security?

In general, IT security is a set of strategies that prevent unauthorized access to organizational assets such as computers, networks, and data. Security also maintains the integrity and confidentiality of sensitive or valuable information. Security, as used in this document, is envisioned in two distinct parts: data or information, such as PTP timing reference signals, and any network used to distribute, switch and transport them. Succinctly put, *Data Security* and *Network Protection.*

1.2 Why is it Becoming More Threatening?

Data security and network protection issues and concerns in today's enterprise business IT environment are generally perceived as becoming more threatening. In reality, it is not so much simply due to an increase in some number of threats as it is the enormity of breaches, or of the amount or the value of the information at risk. Contemporary issues and concerns seem to arise from these forces of change:

- Trend toward 'digital transformation' impact on enterprise business operations
- Growth in data; big data, growth in requirements for basic components, Storage, processing, network bandwidth
- Increase in the number of potential bad actors as the IT industry expands
- More attacks on the surface; more unauthorized access attempts, penetrations, etc.
- Tendency for attacks/attempts to occur anytime - 7x24x365 (real time)

1.3 What's special about media networks?

Media networks are built upon the same network elements as traditional IT networks, and thus are potentially vulnerable to a range of traditional IT security attacks.

However, media networks are different from traditional enterprise IT networking because of their specialized business requirements. Media networks typically involve high bit rate multicast UDP flows not typically found in traditional IT networks. High-accuracy PTP timing is also at the core of media networks' business. And there is a potential massive loss of revenue if attacks impinge on the quality of a widely-viewed broadcast event, even due to fairly slight network degradations.

SMPTE ST 2059/PTP Security has its own set of characteristics, concerns and challenges. It is special because synchronization and timing in a facility are critical. Disruption of either can result in unacceptable impacts on picture, sound clarity, and quality no matter the source. Disruption of ST 2059/PTP reference signals can cause chaos and incoherence across an entire facility.

ST 2059/PTP security and network protection is one of the most important functions in a modern IP-based television plant. Broadcast Industry sync and timing is one of several industrial models found across peer industry market segments (such as Telecom, Finance, and Factory Automation industrial control systems.) ST 2059-1 relies on the PTP for high accuracy in timing; ST 2059-2 is a unique, custom PTP profile for accurate, precise, stable synchronization reference and broadcast facility synchronization (what has been traditionally known as "genlock").

Media networks are assumed to be private networks. The protocols and standards which are used on media networks were in many cases developed under the assumption that they are for deployment solely on private networks.

Whilst private networks cannot be assumed to be immune to security considerations, the security stance for public and private networks is somewhat different, as public networks are subject to a larger range of threats.

This report should therefore be considered to be applicable to private networks only, to reflect the intended use of ST 2059.

1.4 Mitigation Strategies and Techniques

The nature and characteristics of threats, both observed and theoretical is the purview of vendors and their individual customer entities. Mitigation begins in planning and design; it continues through equipment and system configuration, extending into daily business and technical operations.

Effective mitigation measures encompass multiple defensive and offensive endeavors. From initial employee security training, through continuing communications that create and maintain awareness of threats to security of physical and virtual assets, and on to monitoring and testing of well thought-out 7x24x365 security and network protection “solutions”.

Key elements of these mitigation strategies and techniques are:

- Effective mitigation manifests in a mindset of product and service architecture and design
- Creation, design of policy, and continuing communications awareness programs
- Applications design, development, and deployment with embedded and external security as a top priority
- Internal and vendor services should be specified, designed, and deployed with security embedded as a basic property, extended across the premise’s service demarcation physical interface
- Creation and instantiation of operations procedures and protocols with security as a first and continuing requirement
- Local clocks capable of maintaining lock independent of a lost PTP network for a significant period of time

2 Terms and Definitions

BMCA
The default algorithm defined in IEEE Std 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

boundary clock
a clock that has multiple Precision Time Protocol (PTP) ports in a domain and maintains the timescale used in the domain. It may serve as the source of time, i.e., be a leader clock, and may synchronize to another clock, i.e., be a follower clock
[SOURCE: IEEE Std 1588-2008, 3.1.3, with modified terminology]

clock
a 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]

denial of service
an attack in which one or more machines target a victim and attempt to prevent the victim from doing useful work
[SOURCE: RFC 4732, Introduction]

epoch
the origin of a timescale
[SOURCE: Approved Draft IEEE Std 1588-2019, 3.1.12]

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.

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

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

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.

management message
a PTP message defined for the purpose of configuring and/or monitoring PTP Nodes and PTP Instances
[SOURCE: Approved Draft IEEE Std 1588-2019, 3.1.56]

man-in-the-middle
a 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]

master clock
in the context of a single PTP communication path, the local PTP clock of an ordinary clock or boundary clock that is the source of time to which all other local PTP clocks on that PTP communication path synchronize
[SOURCE: Approved Draft IEEE Std 1588-2019, 3.1.31]

ordinary clock
a PTP Instance that has a single PTP Port in its domain and maintains the timescale used in the domain. 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: Approved Draft IEEE Std 1588-2019, 3.1.40, with modified terminology]

peer-to-peer
time synchronization mechanism where each device on the network exchanges peer-delay measurement messages

peer-to-peer transparent Clock
a transparent clock that, in addition to providing PTP event transit time information, also corrects for the propagation delay of the PTP link connected to the PTP Port receiving the sync message. In the presence of peer-to-peer transparent clocks, delay measurements between follower clocks and the leader clock are performed using the peer-to-peer delay mechanism.
[SOURCE: Approved Draft IEEE Std 1588-2019, 3.1.43, with modified terminology]

Precision Time Protocol
IEEE Std 1588 defines a protocol that provides precise synchronization of clocks in packet-based networked systems. 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.

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

transparent clock
a 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. Peer-to-peer transparent clocks also correct for PTP link delay
[SOURCE: Approved Draft IEEE Std 1588-2019, 3.1.84]

3 Abbreviated Terms

ST 2059/PTP – The combination of SMPTE ST 2059-1, ST 2059-2, and Precision Time Protocol

BC – boundary clock

DoS – denial of service

GNSS - Global Navigation Satellite System

P2P – peer-to-peer

PTP – Precision Time Protocol

TC – transparent clock

4 Background on PTP and SMPTE ST 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 clock.

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.

Annex B describes a real-world PTP distribution system at the Canadian Broadcasting Corporation.

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

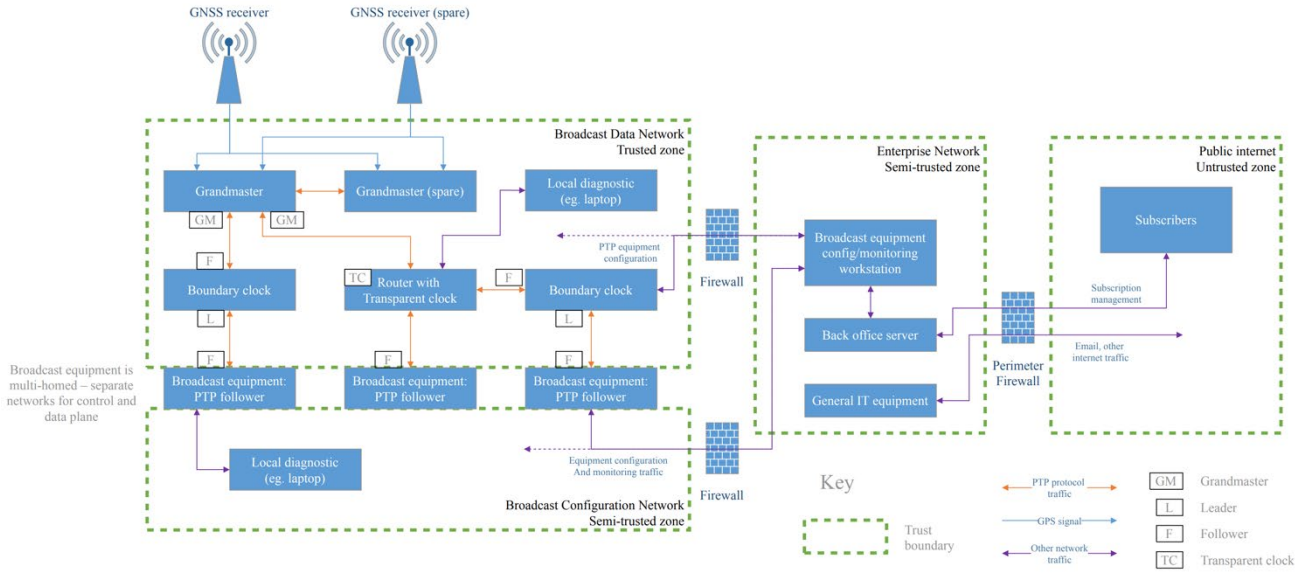
SMPTE ST 2059-2 is a PTP profile for use in professional broadcast applications. It specifies:

- 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 use of multicast transport, but also allows the use of unicast
- Requires delay request-response for default path delay measurement, but also allows peer delay to be used
- Defines SMPTE Synchronization Metadata regarding items such as frame rate, “daily jam”, and whether “daylight savings” is in effect

4.3 PTP System Overview Diagram



This architecture diagram 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.

In order 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 a number of 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 commended 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.

4.4 IEEE Std 1588-2008 Annex K Security

Informative Annex K of IEEE Std 1588-2008 defines an experimental security extension to PTP. The security mechanisms as defined in Annex K are deprecated since investigations revealed vulnerabilities in the proposed integrity check value (ICV) calculation scheme [Treytl, et al.]. Furthermore, there has been no known commercial deployment of Annex K by any PTP vendor.

5 Possible Threat Methods to disrupt PTP systems

5.1 Tampering / Spoofing

5.1.1 Use BMCA to take over control as leader (“rogue leader”) – change time, date, etc.

If a leader is set to “win” the BMCA 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.

5.1.2 Spoof the GNSS to which the GM is locked – change time, date, location, etc.

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.

5.1.3 Send extra sync messages with erroneous information

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 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.

5.1.4 Send extra sync messages timed to mask the legitimate messages

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.

5.2 Denial Of Service (DoS)

5.2.1 Create excess traffic to overpower the ability of the follower to parse the messages

PTP ports must parse all 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, etc.) to cause a DoS of the follower stack. Another attack would be a 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 then it would not report the extra messages.

5.2.2 Create excess traffic to overpower the ability of the leader to process messages

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 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.

5.2.3 Provoke message looping to overload network devices

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.

5.2.4 Use management messages to trigger excess traffic

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.

5.2.5 Exploit followers which cannot reject delay response messages intended for a different follower

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.

5.2.6 Cause continuous BMCA cycles to prevent all clients from locking to a leader

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 the clients from getting the correct time.

5.3 Delay and Replay attacks

Record messages from a grandmaster and re-play it at a later time to skew the time in the followers.

5.4 Man-in-the-Middle attacks

Modify PTP messages to modify time, date, BMCA parameters, domain, etc. This could happen at switch, BC, etc.

5.5 Management messages

5.5.1 Use management messages to change priority on a leader.

A management message TLV can set 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.

5.5.2 Use management messages to change a device from follower only to ordinary clock (elevation of privilege)

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

5.6 Private network breaches

5.6.1 Plug in a laptop which has WiFi enabled – bridge the PTP and other networks. The path so established might provide access for attacks from the other networks.

5.6.2 Attack a device via the control port and gain access / control on the PTP port.

5.6.3 Connect the trusted PTP network to another system such as an OB van

6 Attack/Impact Table

Some of the threats in this table should only happen as a result of intentional and presumably malicious action, for example a "man-in-the-middle" attack requires some sophisticated effort. However other threats in this table may happen maliciously or accidentally. An example of that is using the BMCA to take over as leader. This could easily happen if a device has a default configuration with follower only mode disabled and a low priority 1. If that device is added to the network it can take over as grandmaster. Users and vendors are encouraged to consider that these threats may occur as a result of both accidental and malicious action.

The table below is a collection of possible attacks, along with their impact. (Table inspired by IETF RFC 7384).

		Impact			
Section	**Attack**	**False Time**	**Accuracy Degraded**	**DoS for PTP**	**Disrupt Essence**
5.1.1	Use BMCA to take over control as leader	x	x		
5.1.2	Spoof the GPS to which the GM is locked	x	x		
5.1.3	Send extra sync messages with erroneous information	x	x		
5.1.4	Send extra sync messages timed to mask the legitimate ones	x	x		
5.2.1	Create excess traffic to overpower the ability of the follower to parse the messages		x	x	
5.2.2	Create excess traffic to overpower the ability of the leader to process messages		x	x	
5.2.3	Provoke message looping to overload network devices		x	x	x
5.2.4	Use management messages to trigger excess traffic		x	x	x

5.2.5	Exploit followers which cannot reject delay response messages intended for a different follower		x	x	
5.2.6	Cause continuous BMCA cycles to prevent all clients from locking to a leader			x	
5.3	Delay and Replay attacks	x	x		
5.4	Man-in-the-middle attacks	x	x		
5.5.1	Use management message to change priority on a leader		x		
5.5.2	Use management messages to change a device from follower only to ordinary		x		

7 External Attack Vectors

External attack vectors are those from networks that are not expected to be part of the PTP system.

Section	Attack Vector	Accidental / Malicious
5.6.1	Plug in a laptop which has WiFi enabled – bridging the PTP and control networks	Accidental
5.6.2	Attack a device via the control port and gain access / control on the PTP port	Malicious
5.6.3	Connect the trusted PTP network to another system such as an OB van	Accidental

8 References and Bibliography

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

IEEE Std 1588-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems[1]

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

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

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.

[1] IEEE-Std 1588 is a registered trademark of the Institute of Electrical and Electronics Engineers, Inc.

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:

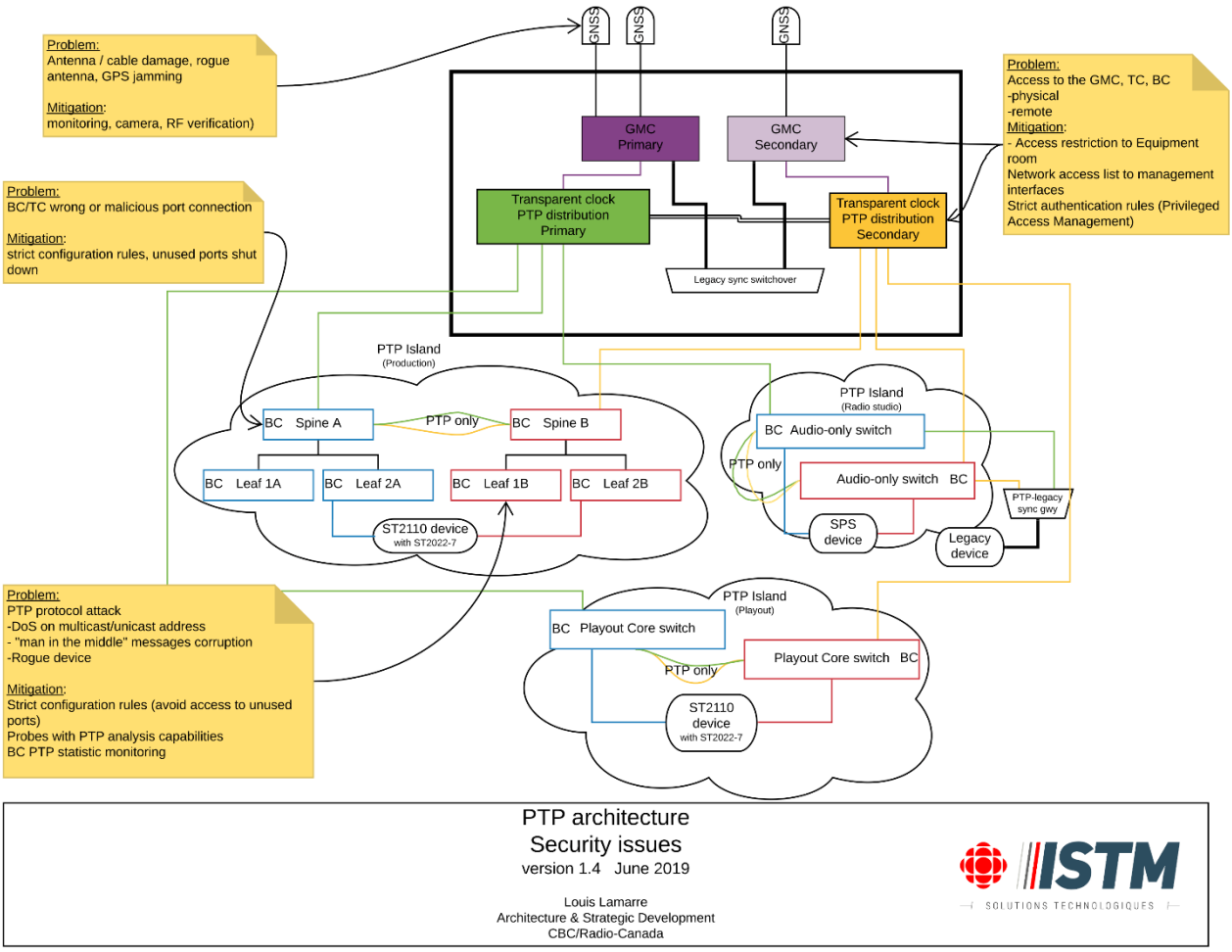
The following areas may require attention from JT-NM Coordination Group members in order to improve security around PTP. It may be appropriate for the JT-NM to call on these bodies to create appropriate technical documents within their respective scopes in order to improve the security and reliability 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.

Annex B: Solution Example - CBC

1. CBC PTP Architecture



2 CBC PTP Architecture Description

2.1.1 General

- The distribution network is a VLAN hosted on two PTP-capable switches in TC mode and linked with a dual link port channel. This VLAN is only for PTP and is not configured as the default VLAN for all ports.
- Each top-layer element of a media environment (Spine blue or red, Playout core, etc.) is connected to the PTP distribution VLAN. For longer travel, fiber links with high speed must be used to reduce the transmission delay.
- In overlay installation (existing site) legacy synchronization (NTSC black burst, Tri-Level, DARS, etc.) must be maintained. To ensure video and audio clean interworking between legacy and IP sources those legacy synchronization signals have to be sourced and referenced from a PTP clock, preferably the grandmaster itself. As per ST 2059-1, all video and audio signals must use the same phase and as such, must share the same “epoch”. The grandmaster must replace the legacy main and backup leader clocks and be used as the primary reference source for the changeover unit in place. Downstream of the C/O unit, the DAs and other configuration is unchanged.

2.1.2 PTP Service Elements

2.1.2.1 Grandmaster Clock

A main and backup grandmaster is the ultimate reference for the entire clock of the PTP domain hierarchy. The best practice is to use specialized hardware platform with a controlled temperature crystal oscillator and GPS external time and frequency source.

At each site, a main and backup grandmaster pair must be provided and each of them should have at least one GPS antenna to synchronize its internal clock. For a major presentation site, an addition layer of robustness is required for the primary clock which will host two GPS cards with a failover module to switch between them transparently to the PTP clock. This is important to avoid any PTP grandmaster change related to a GPS cable antenna or cable issue.

Since PTP service and grandmaster, like most modern broadcast platform, rely on software and are hence potentially affected by code errors, firmware updates, redundancy principle also ask for diversity. The solution is to install two grandmasters from different vendors.

In addition, special care must be given to GPS cables to protect them and make sure that different cable are transported on different conduits, again to avoid a single point of failure. The grandmaster hardware must be protected from electric discharge (caused by lightning or other electric hazard) by using a protection circuit, usually provided with the antenna package.

2.1.2.2 PTP distribution - Transparent clock (TC)

Many different media environments may need a connection to the PTP clock distribution. Hence, there will be a PTP distribution network which role will be to give direct access to the redundant grandmasters for all media networks that need PTP. This network is based on 1Gbit/s ports and for longer reach, fiber links and SFPs should be used to minimize the transmission delay.

To add robustness, the distribution network consists of two switches in transparent clock configuration, linked with a port channel of two 1 Gbit/s ports expanding the PTP traffic VLAN between them. Each grandmaster is connected to a single switch but is visible from both. Hence, not only all BC switches can see both grandmasters for redundancy purposes, but the grandmasters also see each other directly and the secondary Grandmaster Clock can act quickly in case of failure of the primary.

2.1.2.3 Spines, Leaves, Aggregators: Boundary Clocks (BC)

Spines (SP), leaves (LF) and Aggregators (AG) will all be configured as BC. They receive PTP from an upstream link and take the role of a leader for all downstream devices or other BC downstream.

As an example, in normal and stable operation:

- Spines switches have their follower port connected to the main PTP distribution network.
- Leaves have their follower port connected to their main upstream port to the spine.
- Redundant port between spines are in “passive mode”.
- All ports connected to endpoints are hence in LEAD state.

2.1.3 Rules for implementation

2.1.3.1 Every site has a both a main and a standby grandmaster

In theory, it could be possible to have a single Grandmaster Clock for the whole network and transport PTP over WAN. However, because the current transmission time, and more importantly, to respect the robustness objective, every site which needs PTP would have at least one designated grandmaster, preferably with GPS, as is done for legacy sync generator clocks.

2.1.3.2 Production IP broadcast network

PTP distribution will be restricted to media network, in all sites where AES67 and ST 2110 networked equipment would be deployed. Hence, PTP will not be available on corporate network, management network and won’t be transported over WAN.

2.1.3.3 PTP service redundancy

Given the direct impact in production of any PTP failure or service degradation, the robustness and resilience expected will be very high. To get there, all main components will be redundant and no single point of failure should be exposed.

2.1.3.4 GNSS (GPS) reference source

The obvious external synchronization source is the satellite system. All grandmaster candidates must be provisioned with a multi service (GNSS) antenna and receptor. This will provide a redundant system able to use all available satellite systems (GPS, Galileo, GLONASS, and BeiDou) to avoid a single system dependency.

2.1.3.5 Specialized IP network for PTP transport

The main elements from PTP service will be connected together only with PTP-capable network switches, using TC or BC configuration. Exception can be made to synchronize an isolated non-critical device located in a remote network zone. PTP traffic would then be using unicast sessions, or will need a V(X)LAN designed to carry only PTP and isolated to protect higher PTP layers.

2.1.3.6 VLAN and QoS

PTP traffic between the BCs and grandmaster of the higher layers of the network (distribution, spines, leaves) and when mixed with other media or management traffic, will be configured with highest QoS (EF) using DSCP tagging and associated queue management. However, since PTP needs very small bandwidth, this highest priority traffic should be limited in those interfaces with a traffic policer and class overflow traffic in best effort (BE). Given the large size of those links, a recommended BW of 100 Mbit/s should be enforced for EF traffic.

2.1.3.7 Primary external reference source and internal oscillator

Every grandmaster must have at least one GNSS antenna directly connected to the unit. The grandmaster must also host a very precise and autonomous oscillator (for example, an Oven Controlled Crystal Oscillator) able to keep a 0.1 ms precision in holdover mode for at least an hour. This will give a few hours to find and repair the cable or the GPS antenna without any production impact, even in a site where no grandmaster redundancy exists. But, in major sites, it’s recommended to opt for a dual GPS antenna configuration, with a change-over card that offers a transparent redundant GPS connection to the PTP card.