Security Threats and Mitigation in PTP Networks

Doug Arnold
Principal Tecnologist
MEINBERG

Tim Frost
Strategic Technology Manager
Calnex
Insight and Innovation

WSTS 2016 San Jose

Timing Network Security Landscape

- The Great Wall
  - Firewalls
  - VLANs
  - What happens if they are breached?
- Device management security
  - Secure management interfaces
  - Passwords
  - Management only ports
  - Alarm when configuration changed
  - Intrusion detection

Threat: Simple BMCA Attack

1. Gain access to the network with multicast PTP
2. Send Announce message with best possible credentials
3. Send wrong time to slave ports
    - Different time to each slave via Delay Response messages
    - Wrong frequency

Mitigation: Slave heuristics

- Different masters should have similar time
- Time from same master should not contain large jumps
- Time should not go backwards
- May be malicious or just a device failure

Raise alarm and go into holdover!

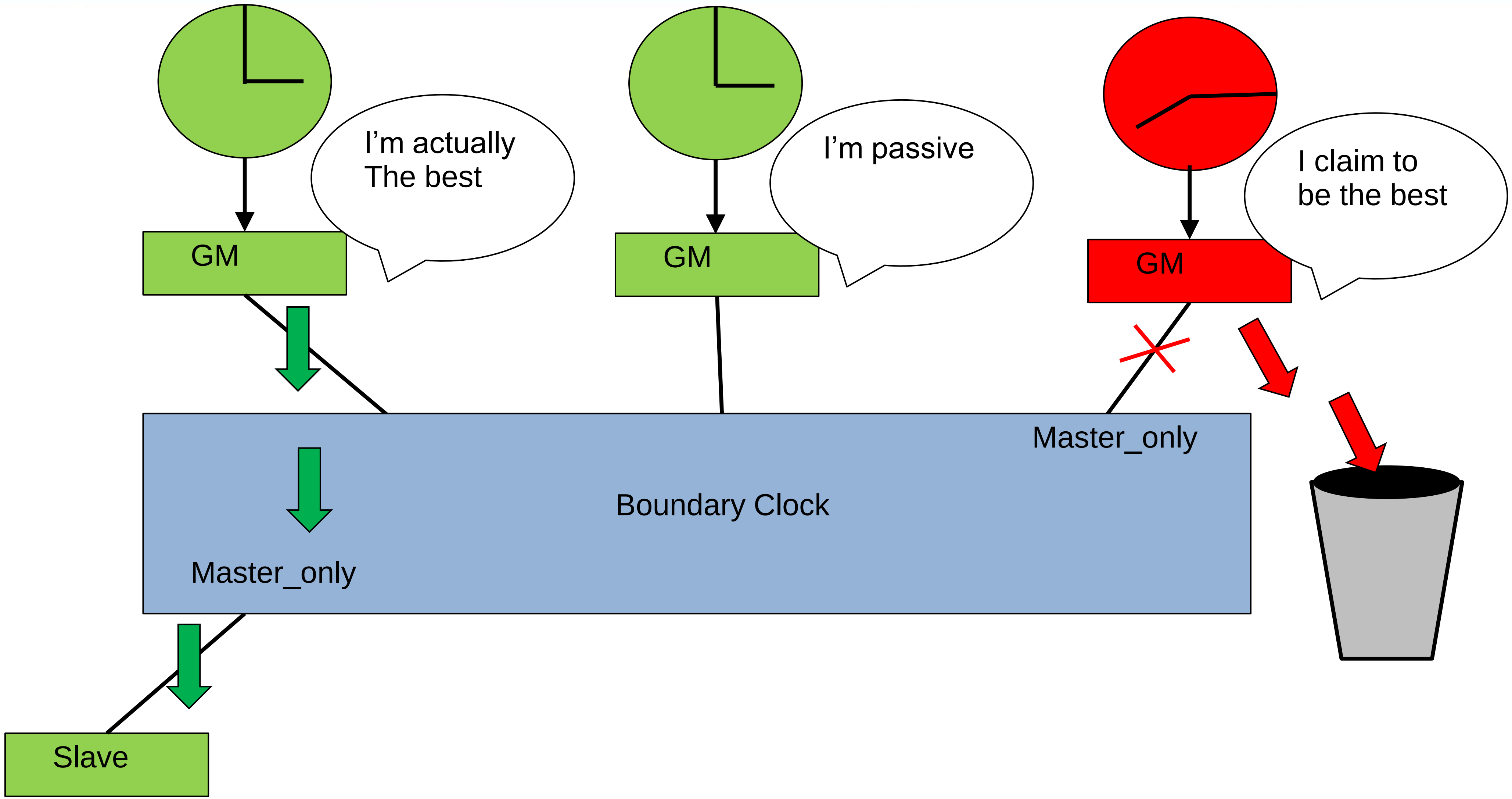
Threat: Smarter BMCA attack

1. Gain access to the network with multicast PTP
2. Synchronize to the master
3. Take over as best master
4. Send time with small rate error
    - Avoid easy slave heuristic detection
    - Wrong frequency
    - Gradually wrong time

Mitigation Techniques

- Assisted GNSS
    - Works for slave port on BC with GNSS
- Unicast PTP
    - On path support?
- Acceptable Master Table
    - BCs would not set port to slave state with rogue master input
    - Option in IEEE 1588-2008
    - Slaves, BCs need to be updated when new GM, BC added to network

Mitigation: Master_only Port



I’m actually
The best

GM

I’m passive

GM

I claim to
be the best

GM

Master_only

Boundary Clock

Master_only

Slave

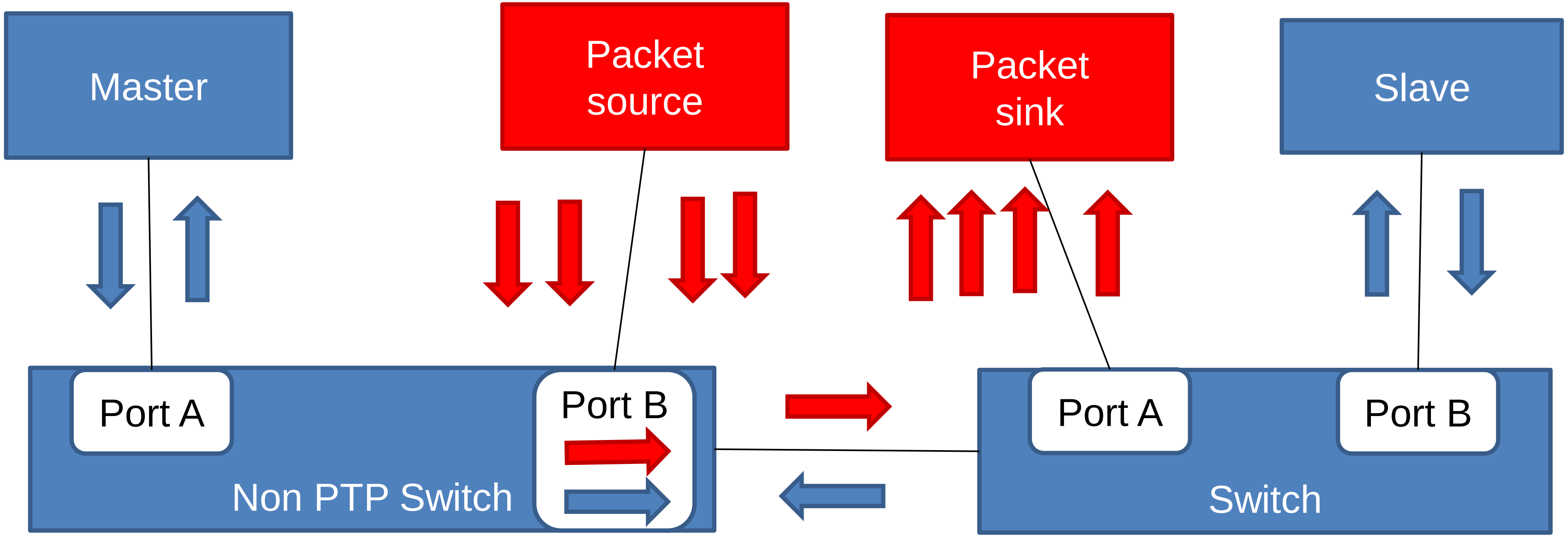
Threat: Master clock impersonation

1. Gain access to the network with multicast or unicast PTP
2. Send Sync and Delay Response with clock ID and source address of current master
3. Slaves receive both true and forged messages

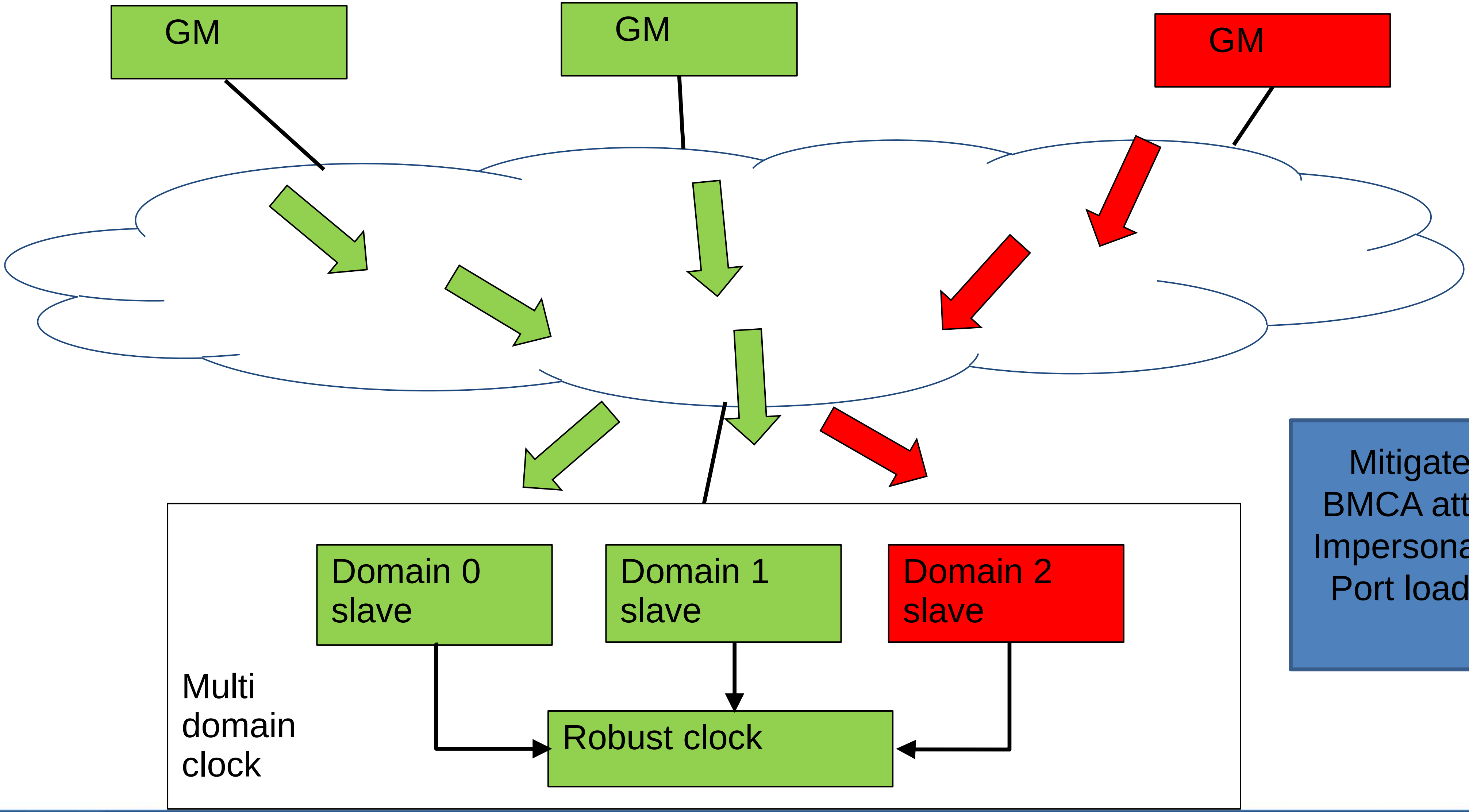
Mitigation Techniques

1. Master_only ports
2. Slave port packet selection:
   - Ignore outliers
   - Look for changes in apparent delay (t2-t1) and/or one-way delay
   - Sudden changes or inconsistent delays are warning signs!!
3. Filter out rogue values according to consistency criteria
4. If still confused, raise alarm and go into holdover

Threat: Port loading delay attack



Mitigation: Multimaster PTP



Mitigates:
BMCA attack
Impersonation
Port loading

Threat: Multidomain Attack

1. Gain access to the network with multicast or unicast PTP
2. Become best master or impersonate masters in all active domains
3. Defeats multi-master scheme

- Similar effect by impersonating all masters in network

Mitigation: Cryptography

- Authenticate master
  - e.g. using digital certificates
- Check integrity of messages
  - Challenge: TCs change messages then retransmit
- Also helps with
  - BMCA attacks
  - master impersonation attack
- Does not help with delay attacks

Some encryption Options

- MACsec
  - Good for layer 2 PTP
- IPsec
  - Good for layer 3 PTP
- Proposed PTP security TLV
  - Expected with 1588 revision
  - Includes hash code to authenticate message
  - Compatible with GDOI (group symmetric key)
  - Compatible with NTS (Tesla based security)

For further discussion

- What happens if they gain control of a device?
  - GM
  - BC
  - TC
  - Switch or router (Delay attack)
- Is attacking PTP the biggest concern at this point?

Summary

- *PTP can be attacked simply gaining access to network*
  - *No need to take over a device on the network*
  - *Multicast PTP vulnerable to more attacks than Unicast PTP*
- *Mitigation techniques*
  - *Smart slave algorithms*
  - *Acceptable master table*
  - *Master_only ports on BCs*
  - *Multi-master PTP*
  - *Cryptography*
- *No one technique stops all attacks: <u>use multiple techniques</u>*

MEINBERG

Thank you for your attention!

Doug Arnold
doug.arnold@meinberg-usa.com

Tim Frost
tim.frost@calnexsol.com

www.meinbergglobal.com