A Security Analysis of the Precise Time Protocol

Jeanette Tsang & Konstantin Beznosov

December 5, 2006

Laboratory for Education and Research in Secure Systems Engineering (LERSSE)

University of British Columbia

Outline

1. Work objectives
2. Assumptions
3. Discussion of Best Master Clock (BMC) attack
4. Results summary
5. Conclusion

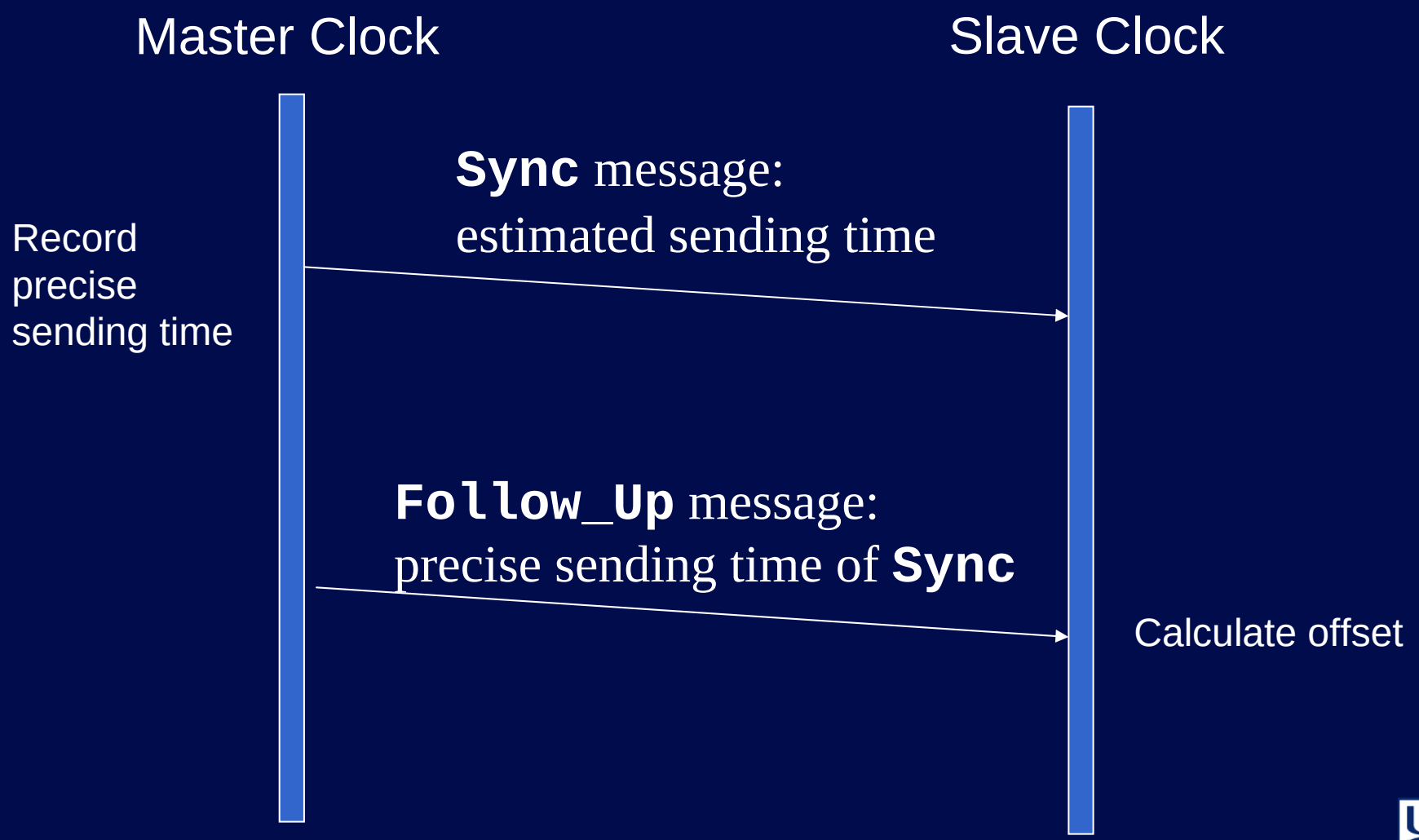
Work Objectives

1. Identify generic security vulnerabilities
2. Identify PTP-specific vulnerabilities
3. Suggest countermeasures

Assumptions

1. Closed network
   - i.e., no direct or indirect connections with the Internet
2. Insiders can mount passive & active attacks
   - i.e., remove, modify, and inject messages
3. No IP-level data protection
   - e.g., IPSec

Sample Run of the PTP Protocol



Attacks

Types of Attacks Identified

1. Modification
2. Masquerading
3. Delay
4. Replay
5. Denial of service

Attack 1: How to Masquerade as the Master Clock

Two ways:

1) Impersonate Current Master Clock
   - "Steal" current master clock identity

2) Switch the slave clock to the rogue master clock
   - Win the Best Master Clock (BMC) election

How to Win Best Master Clock (BMC) Election (1/4)

Sync message

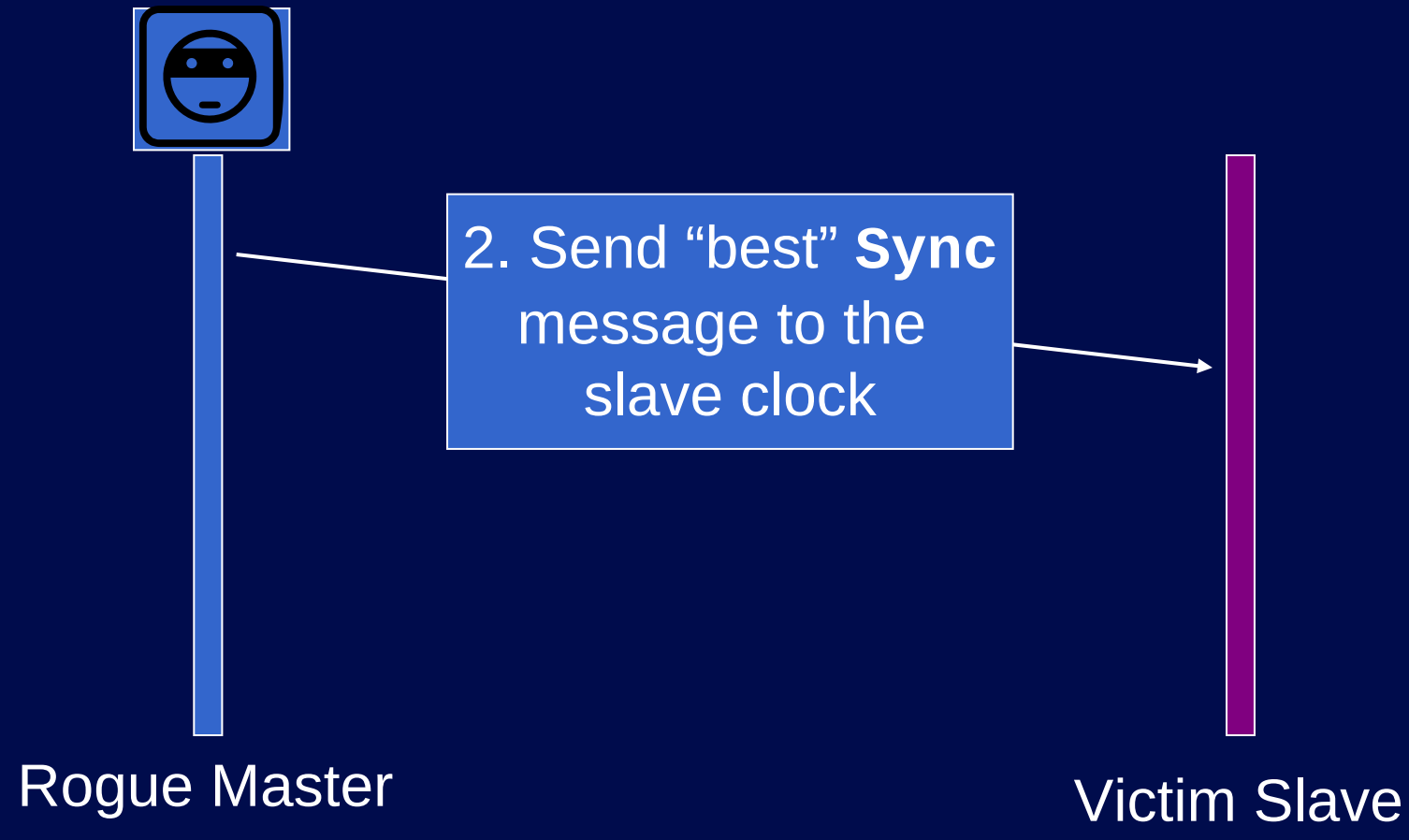
1. Snoop
- Grandmaster clock information
- sequenceId
- Uuid, etc.

Rogue Master

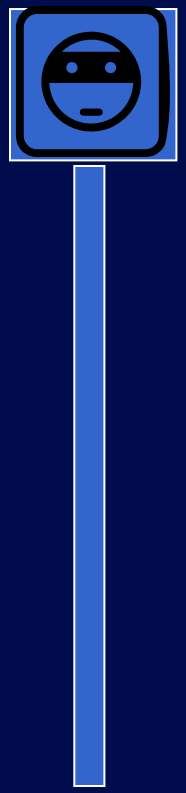
Legitimate Master

Victim Slave

How to Win BMC Election (2/4)



How to Win BMC Election (3/4)

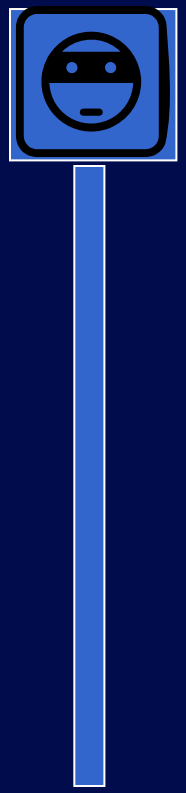


Rogue Master

Victim Slave

3. Victim slave clock runs BMC and picks the rogue master

How to Win BMC Election (4/4)

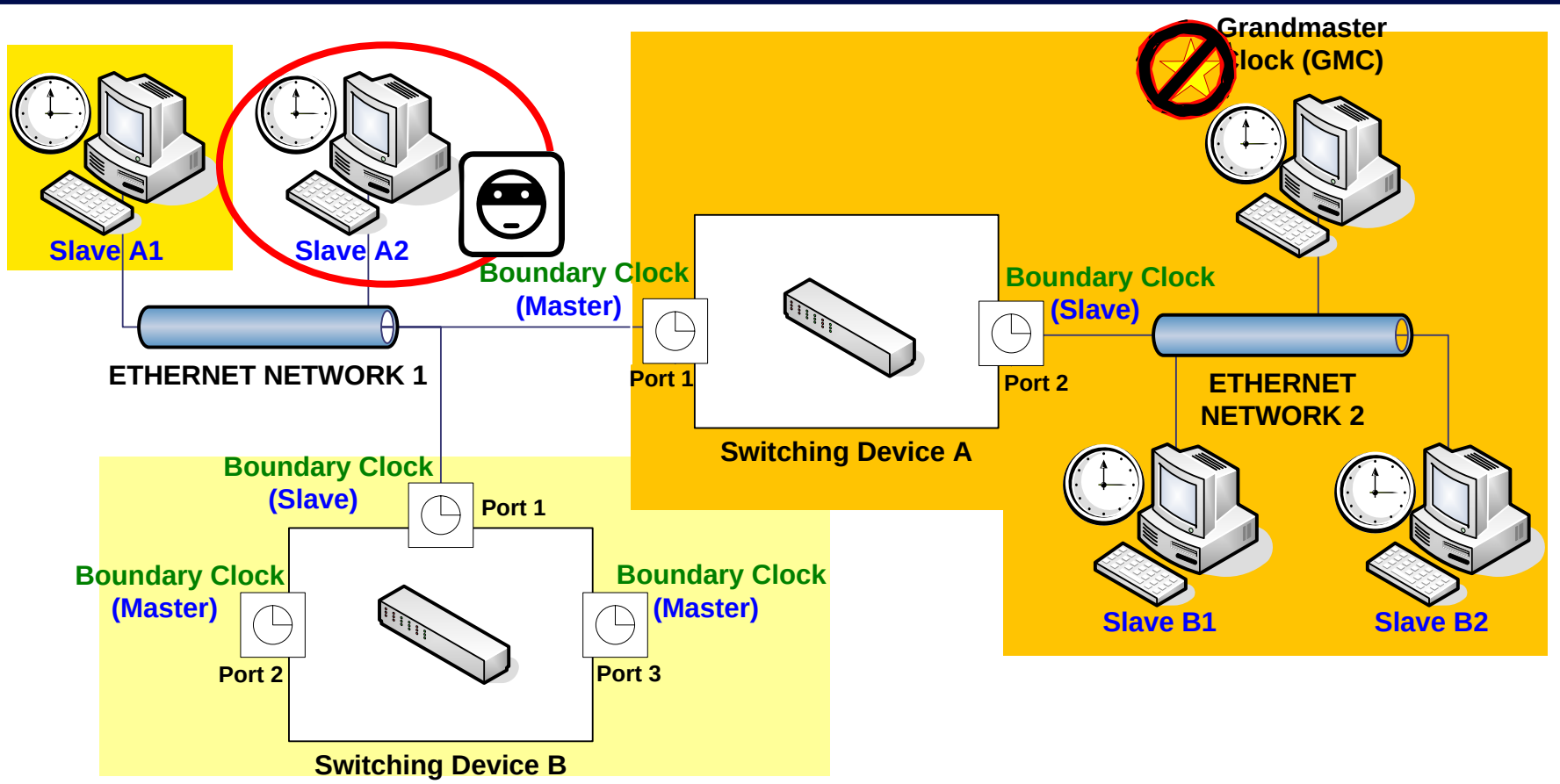


Rogue Master

Victim Slave

4. Victim slave “switches” to the Rogue Master

Sample PTP Network

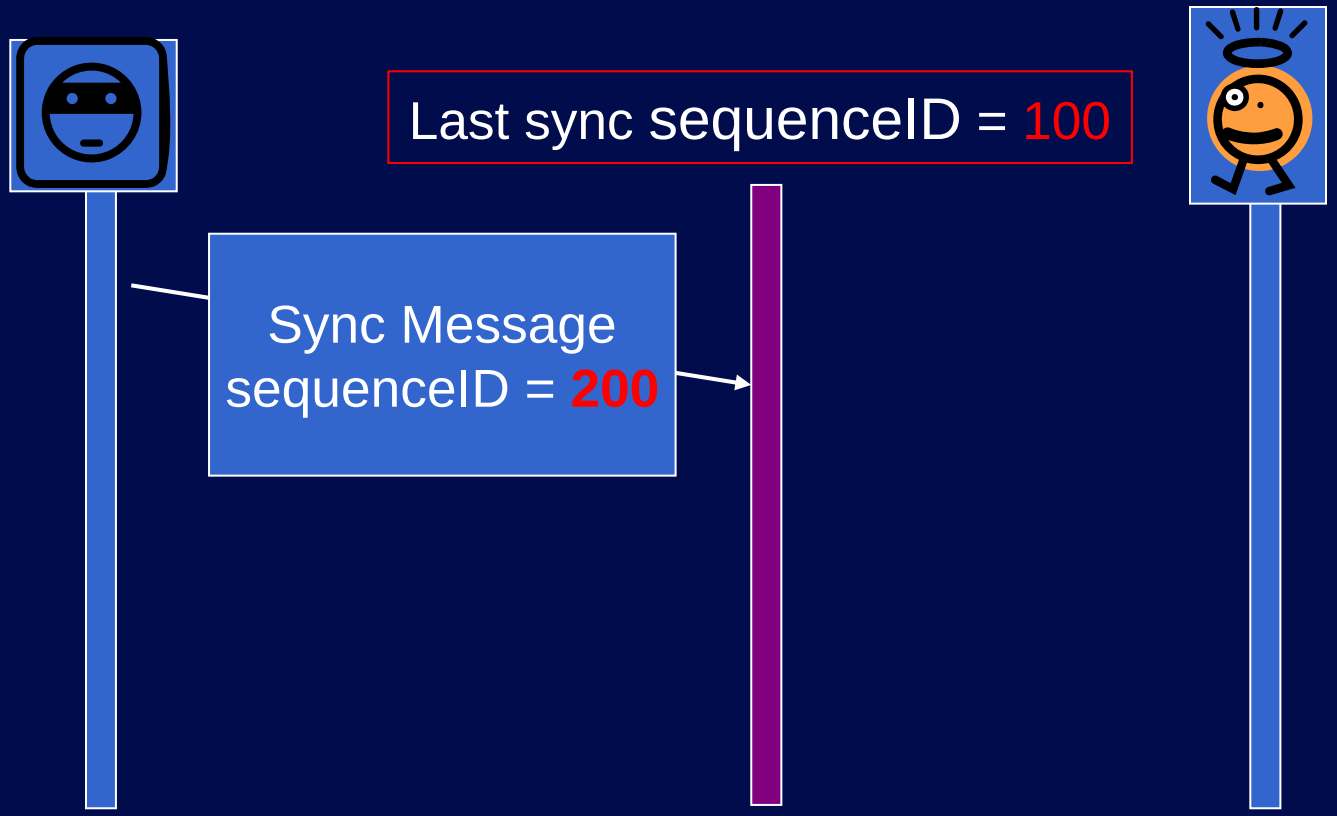


Attack 2: Depriving slave from synchronization

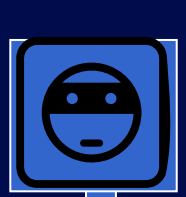
Ways to attack:

1. Block *sync* messages
   - Congestion
   - Removal
2. Make victim slave to discard good sync messages
   - *Sync* message modification
   - Illegal update of *sequenceId*

Attack 2: Illegal update of sequenceId (1/4)



Attack 2: Illegal update of sequenceId (2/4)



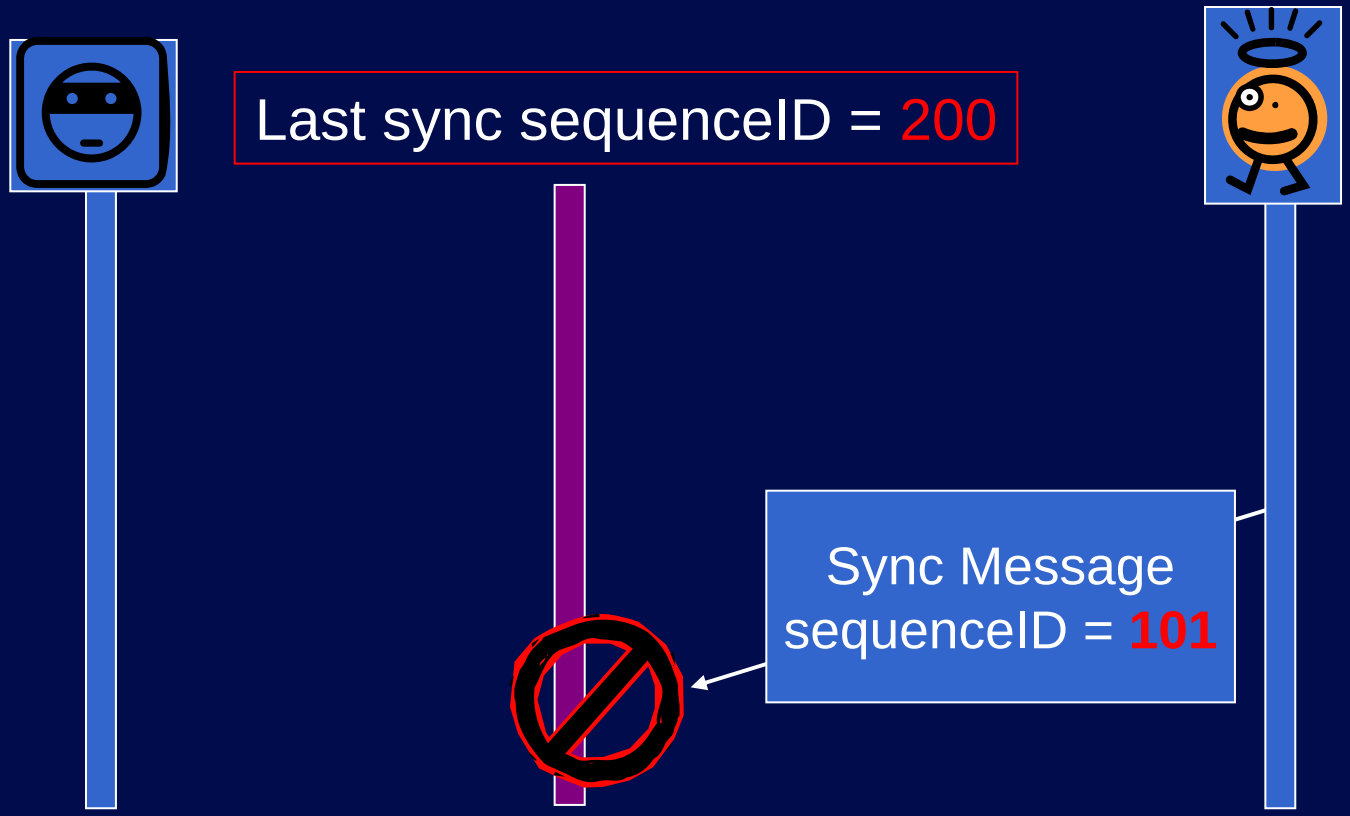
Update last sync sequenceID → 200

Rogue Master

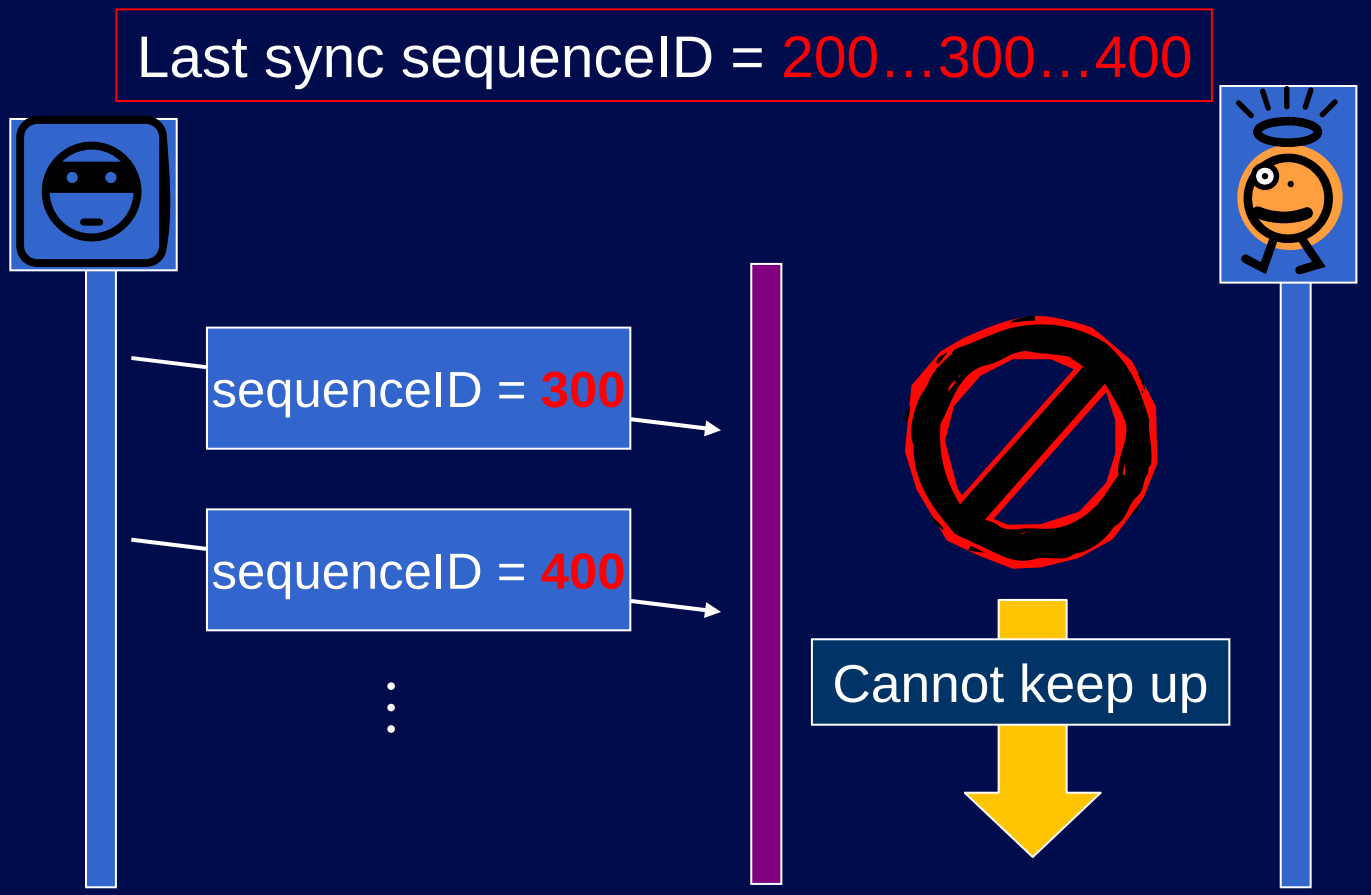
Victim Slave

Current Master

Attack 2: Illegal update of sequenceId (3/4)



Attack 2: Illegal update of sequenceId (4/4)



Attack Type	Effects	Countermeasures	Would IPsec help to counter this attack type?
Modification	•Denial of Service •Incorrect resynchronization •**Changing clock hierarchy**	•Cryptographic integrity protection	Yes
Masquerading	•**resynchronization**	•Centralized or chained authentication mechanism	No
Delay	•Delay in timing messages •Timeout of synchronization process •Increase in offset calculation	•Algorithm to detect abnormal timestamp •Back up plan using previous timing records	Yes
Replay	•Disturbance of message sequence •Saturate process queue •Congest network paths	•Authentication mechanism •Tunneled connection	Yes
Denial of Service	•Small-scaled: Affect accuracy of synchronization •Big-scaled: Put halt on the whole PTP system	•Physical protection •Pay precautions to other malicious attacks •Monitor traffic	No

Conclusions

- Could not ensure integrity of messages and authenticity of sender
- Analyzed five types of attacks
  - Incorrectly resynchronize clocks
  - Rearrange or disrupt hierarchy
  - Bring protocol participants into an inconsistent state
  - Deprive victim slave clocks from synchronization in ways undetectable by generic network intrusion detection systems
- Proposed countermeasures for the identified attacks

More information available on

lersse.ece.ubc.ca