A Security Analysis of the IEEE 1588 Standard

Jeanette Tsang & Konstantin Beznosov

October 12, 2005

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

University of British Columbia

What will happen if...

Photo from:
:http://www.edwards.af.mil/articles98/docs_html/splash/jan98/cover/page_5.html

And what if...

Photo from: www.aandbfoundry.com/ products.html

How do you know PTP is “secure”?

- No security analysis has been done

- Confidentiality
- Integrity
- Availability

Outline

1. Objectives
2. Assumptions
3. Discussion of possible attacks
4. Results summary
5. Conclusion

Our Objectives

1. Identify PTP security vulnerabilities for generic attacks
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 active attacks
   - i.e., remove, modify, and inject messages
3. No IP-level data protection
   - e.g., IPSec

Attacks

Attacks Identified

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

Attack I: 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

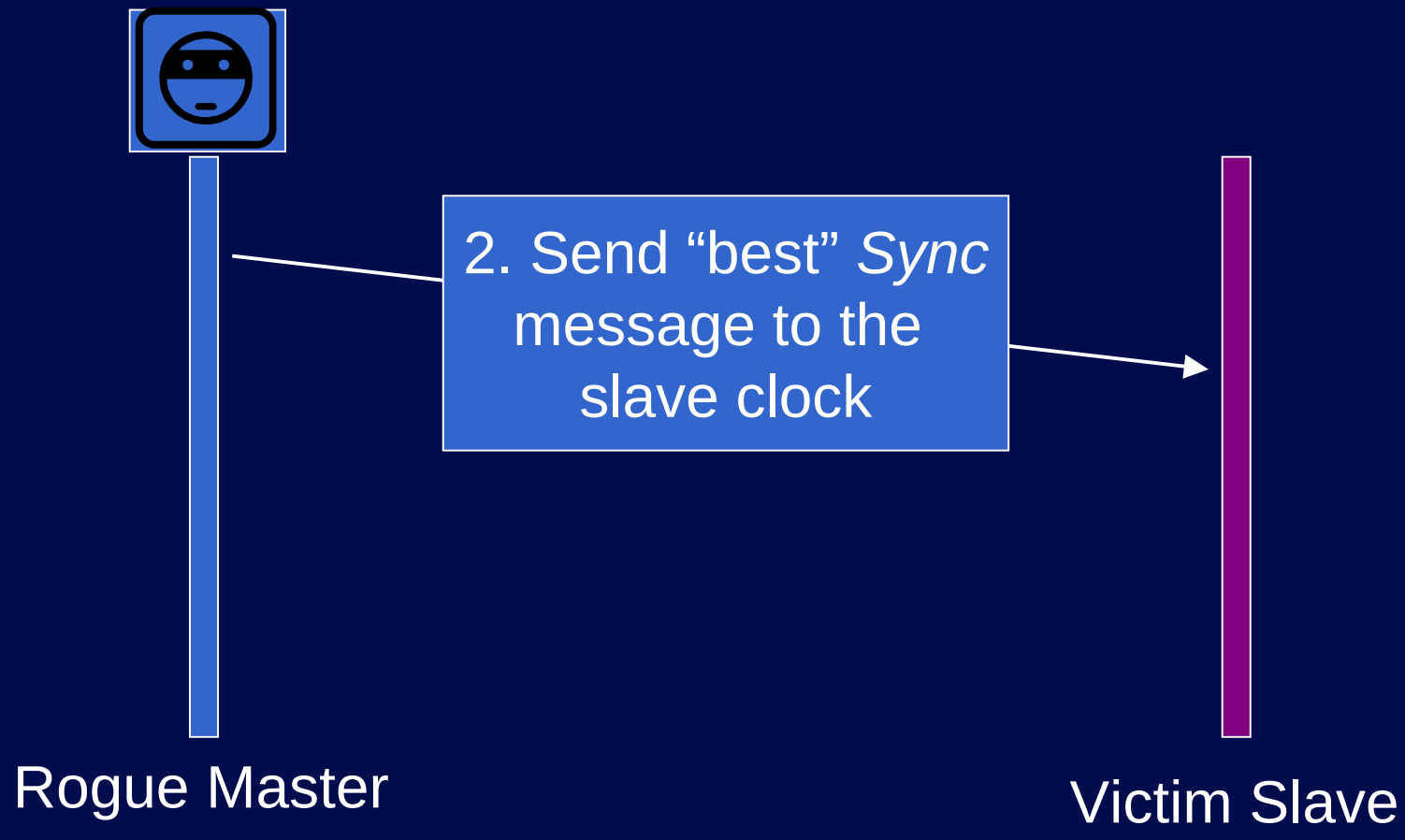
How to Win BMC Election (1/4)

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

Rogue Master

Victim Slave

How to Win BMC Election (2/4)



How to Win BMC Election (3/4)

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

Rogue Master

Victim Slave

How to Win BMC Election (4/4)

4. Victim slave "switches" to the Rogue Master

Rogue Master

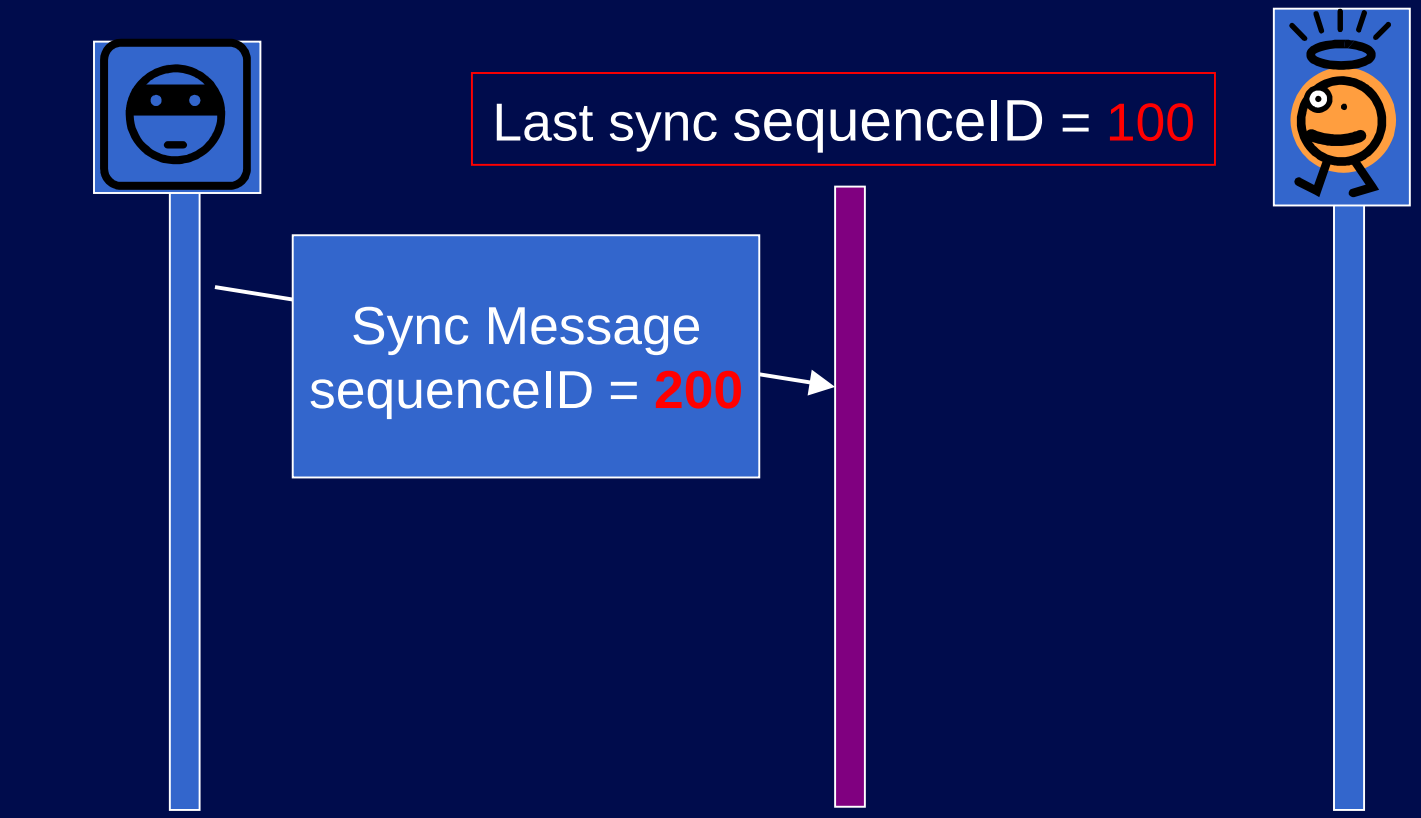
Victim Slave

Attack 2: Depriving slave from synchronization

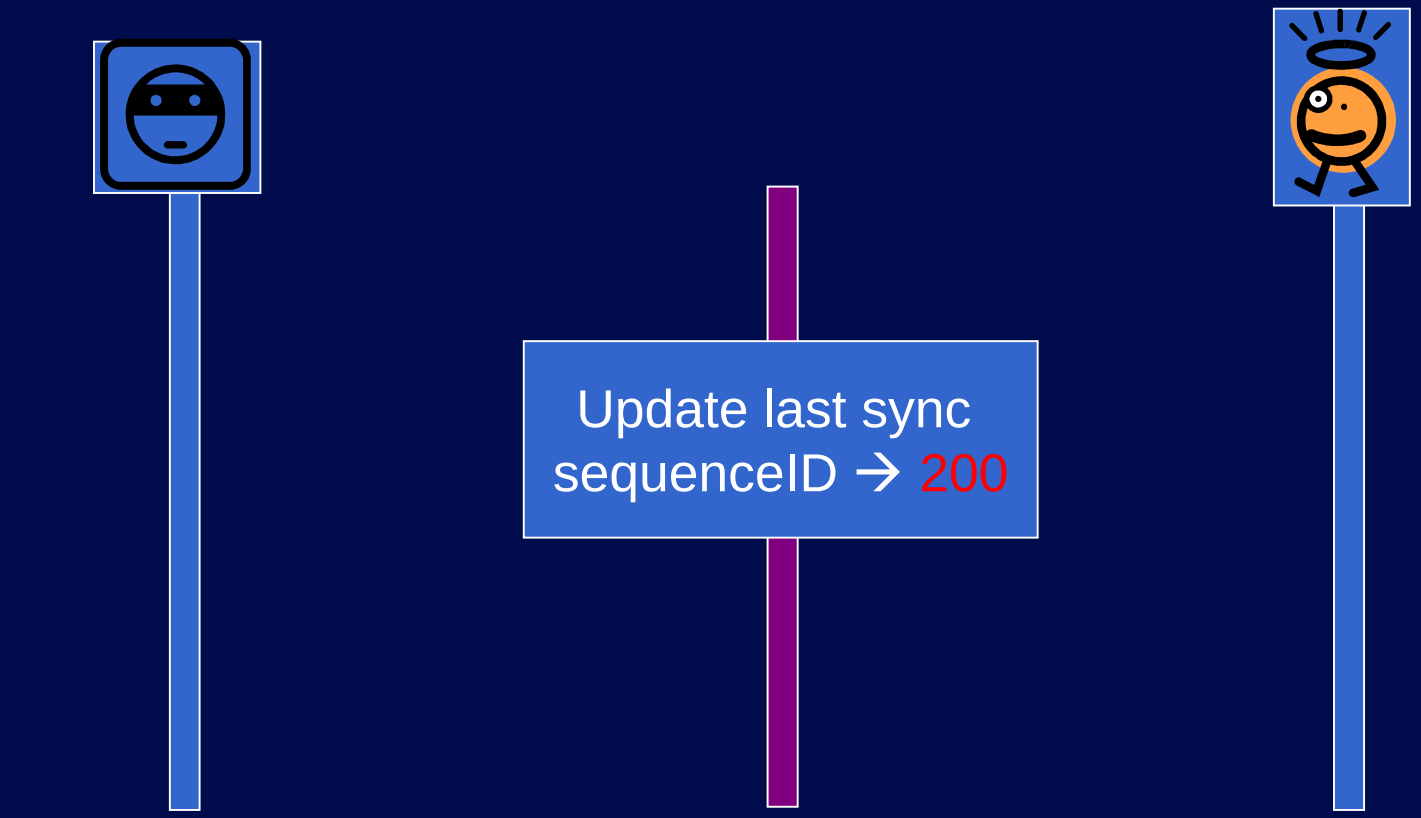
Ways to attack:

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

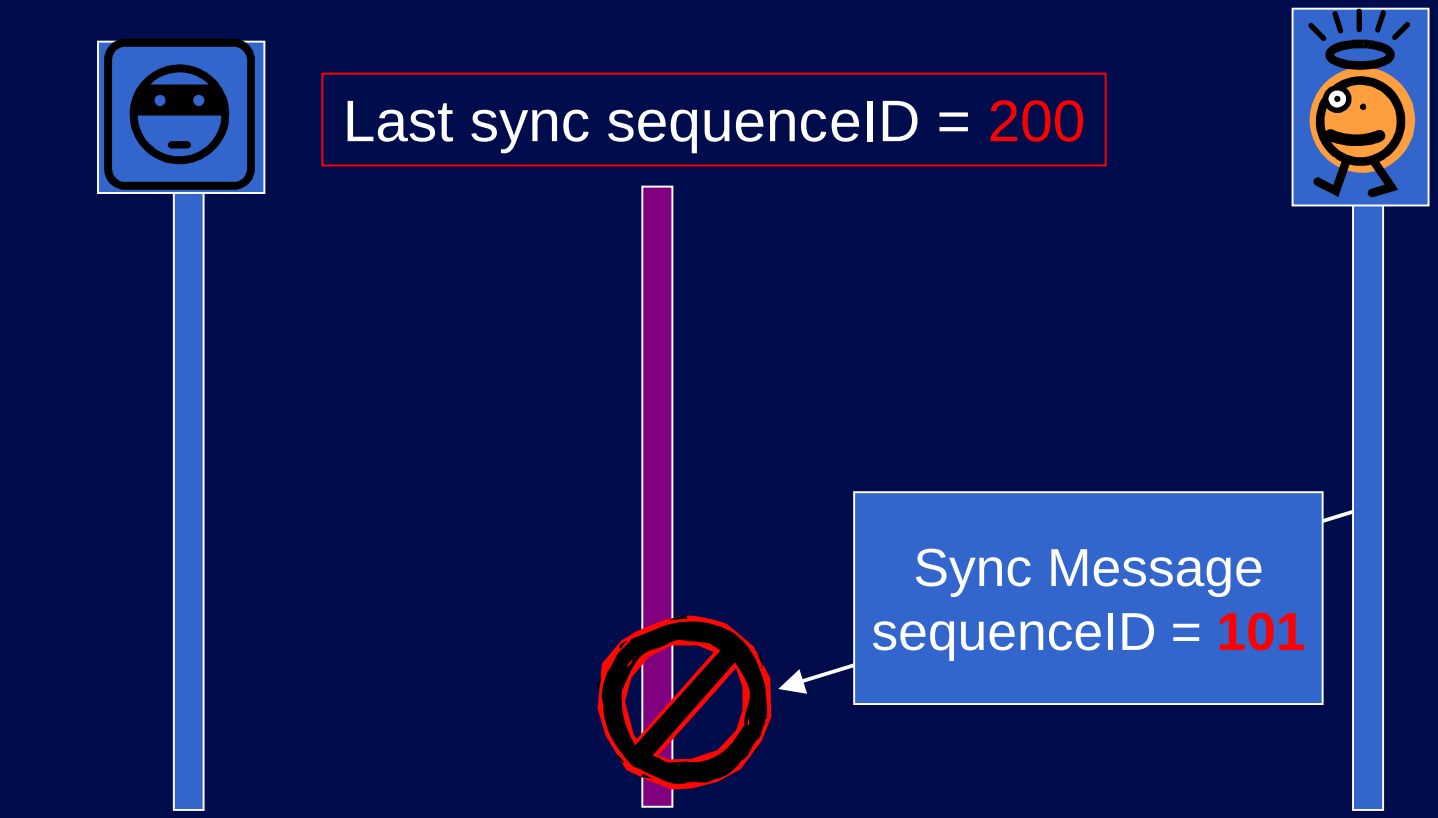
Attack 2: Illegal update of sequenceId (1/4)



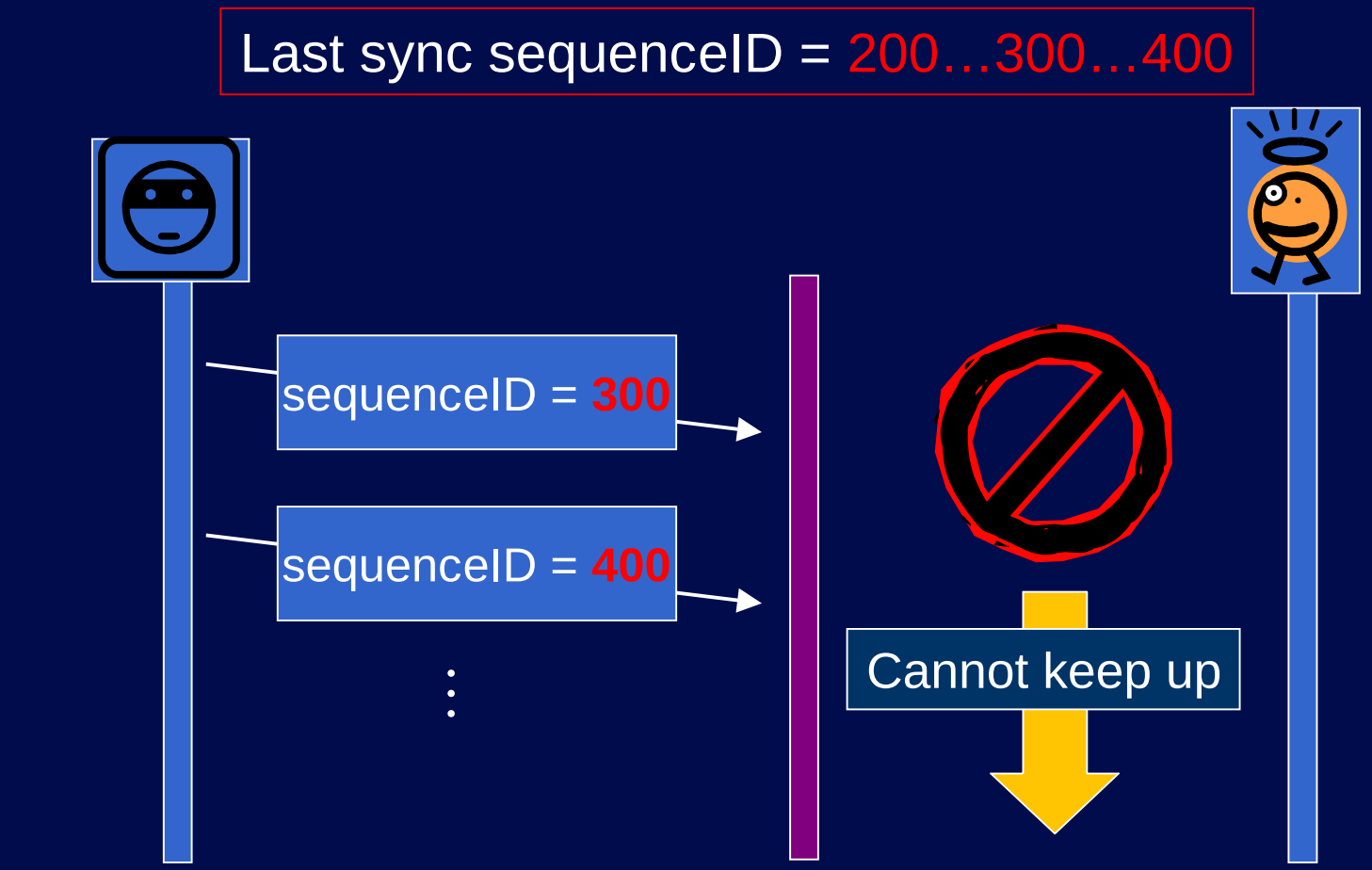
Attack II: Illegal update of sequenceId (2/4)



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



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



Results Summary

Attack	Effects	Countermeasures	IPsec?
Modification	•Denial of Service •Incorrect resynchronization •Changing clock hierarchy	•Cryptographic integrity protection	Yes
Masquerading	•resynchronization	•Centralized or chained authentication mechanism	Yes
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	No

Results Summary

Attack	Effects	Countermeasures	IPsec?
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

- Presented two attacks:
  - Masquerading
  - Depriving slave from synchronization
- Countermeasures:
  - Integrity protection
  - Authentication mechanism
  - Tunnelled connection
  - Monitor network traffic
  - Detect abnormal timestamp

More information

lersse.ece.ubc.ca