

# Formal Methods in Networking Protocols

Joshua Hulst  
Dec. 14, 2009  
CSE 814

# What's so Important about Network Protocols?

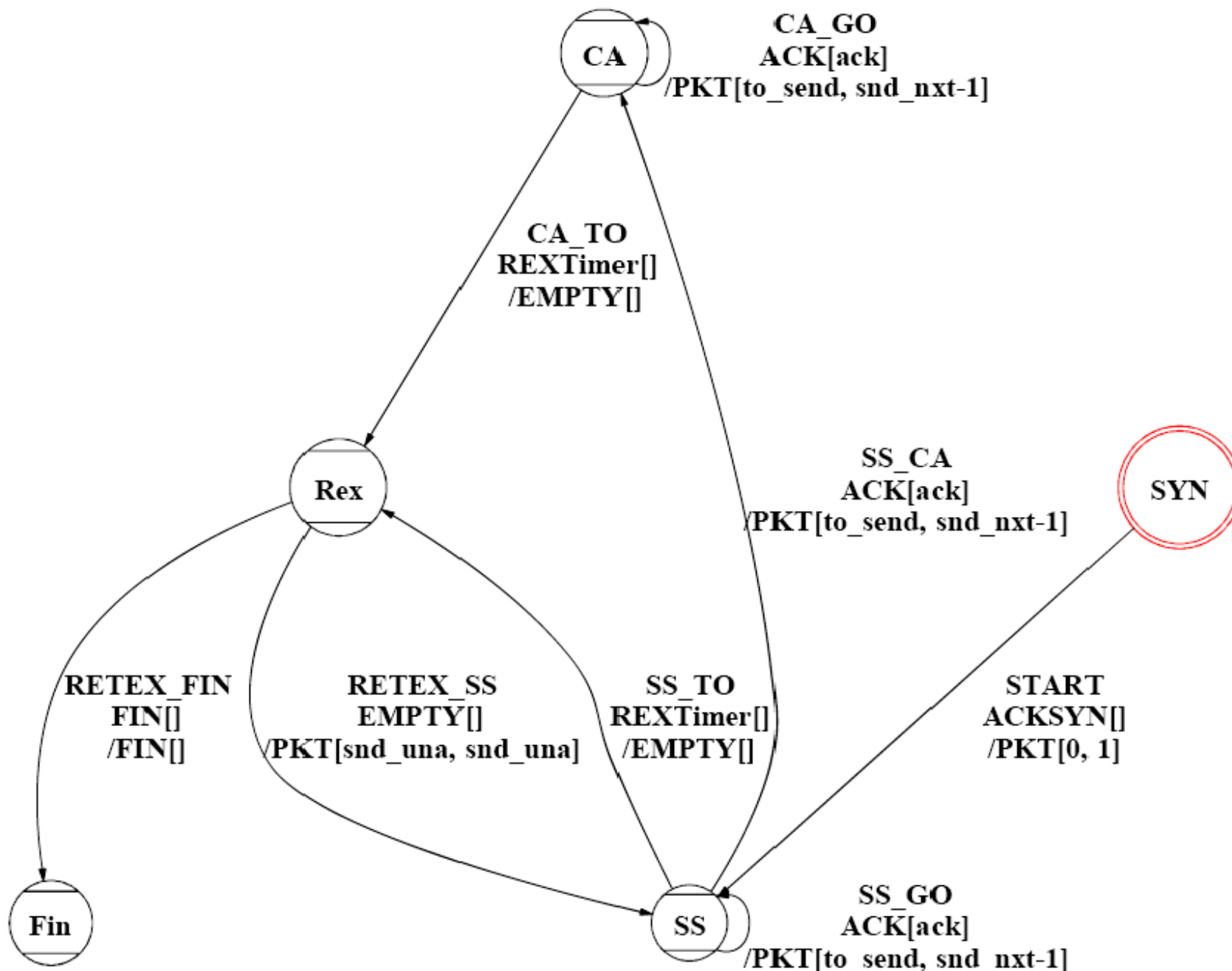
- Backbone of Networking
- Many Implementations
- SSL
  - `https://msu.edu\0.evil.com` = `https://msu.edu`
- Security and Stability are always important

# What is a Network Protocol?

- Rules for Communication
  - Setup/Teardown
  - Data Transfer
  - Control
- Examples
  - SSH
  - HTTP
  - SSL
  - TCP/IP

# Where do Formal Methods Fit?

- Usually defined in Non-Machine readable language
- Fuzzy and incomplete specifications
- Finite State Machines
  - States
  - Transition events
  - Reachability
- Protocol Fingerprinting
- Protocol Testing



# Protocol Fingerprinting

- Distinguish between implementations
- Implementations often tied to platform
- Platform identification gives vulnerability list
- Compare FSMs
  - Find differences and specifically test those

# Protocol Testing

- Fuzz Testing
  - Random/Unexpected Inputs
  - Hard when no information on protocol
- Create an FSM!
  - Shows expected input
  - Shows state transitions

# Experimental Results

- MSN Instant Messenger
  - Reverse Engineered Protocol
- Pidgin
  - 61 Errors
  - Removing login from packets
- AMSN
  - 89 Errors
  - Skipped sending the contact list

# Conclusions and Future Work

- FSM are good for modeling protocols
  - Specific and unambiguous
  - Can be machine readable
  - Easier implementation testing
- Create tools for modeling?
- Formally specify protocols?

# Sources

- V. Cerf and R. Kahn. A protocol for packet network intercommunication. 22(5):637–648, May 1974.
- Yating Hsu, Guoqiang Shu, and D. Lee. A model-based approach to security flaw detection of network protocol implementations. In Network Protocols, 2008. ICNP 2008. IEEE International Conference on, pages 114–123, Oct. 2008.
- D. Lee, Dongluo Chen, Ruibing Hao, R. E. Miller, Jianping Wu, and Xia Yin. Network protocol system monitoring-a formal approach with passive testing. 14(2):424–437, April 2006.
- D. Lee and M. Yannakakis. Principles and methods of testing finite state machines-a survey. Proceedings of the IEEE, 84(8):1090–1123, Aug 1996.
- R. Movva and W. Lai. Msn messenger service 1.0 protocol, August 1999.
- G. Shu and D. Lee. Network protocol system fingerprinting - a formal approach. In Proc. 25th IEEE International Conference on Computer Communications INFOCOM 2006, pages 1–12, April 2006.