Q1 Review Session

Therac-25

- **Complex system fails for complex reasons**
- Therac-20
  - hardware interlocks — protective circuits
- Therac-25
  - software shared code with Therac-20
  - software interlock is a boolean flag

Therac-25

turntable position	electron therapy	x-ray	field light
beam energy	5 - 25 mev	25 mev	0
beam current	low	high	0
beam modifiers	magnets	flattener	none

Therac-25

- Tyler accidents
  - Operator inputs parameters, moves cursor down to the bottom field
  - Keyboard thread sets a variable
  - Turntable thread and parameter setting thread read variable, do their work
  - Operator notices a mistake, goes back and makes changes
  - Parameter setting takes a long time to finish (~8 seconds)
  - Turntable processes the changes, parameter setting thread does not
- Yakima accidents
  - Counter overflow

Therac-25

- **Based on the the investigation of the Therac-25 accidents (reading #4), which of the following statements about the Therac-25 are true?**
- A. True / False The race conditions that caused some of the accidents could have been avoided by the use of locks and condition variables.
- True. Proper use of locks and condition variables would have eliminated at least one of the bugs. For example, locking the MEOS two-byte variable would have prevented the prescription from being changed after Datent has read the index from the high-order byte of MEOS.
- B. True / False The manufacturer proved that faulty switches caused the first accidents.
- False. The manufacturer believed that this was the cause of the accident, but were not able to show their theory was correct.

Therac-25

- C. True / False The authors of the paper believe that, in practice, hardware interlocks are necessary for safety.
- True. The authors discuss the need for hardware interlocks in critical systems in the “System Engineering” section of “Lessons Learned”, on p. 38 of the paper.
- D. True / False The fact that the Therac-25 was a multi-function machine, supporting two types of radiation, contributed to the accidents.
- True. Some of the accidents occurred when one part of the machine was set for electron radiation and another part was set for x-rays.

Naming

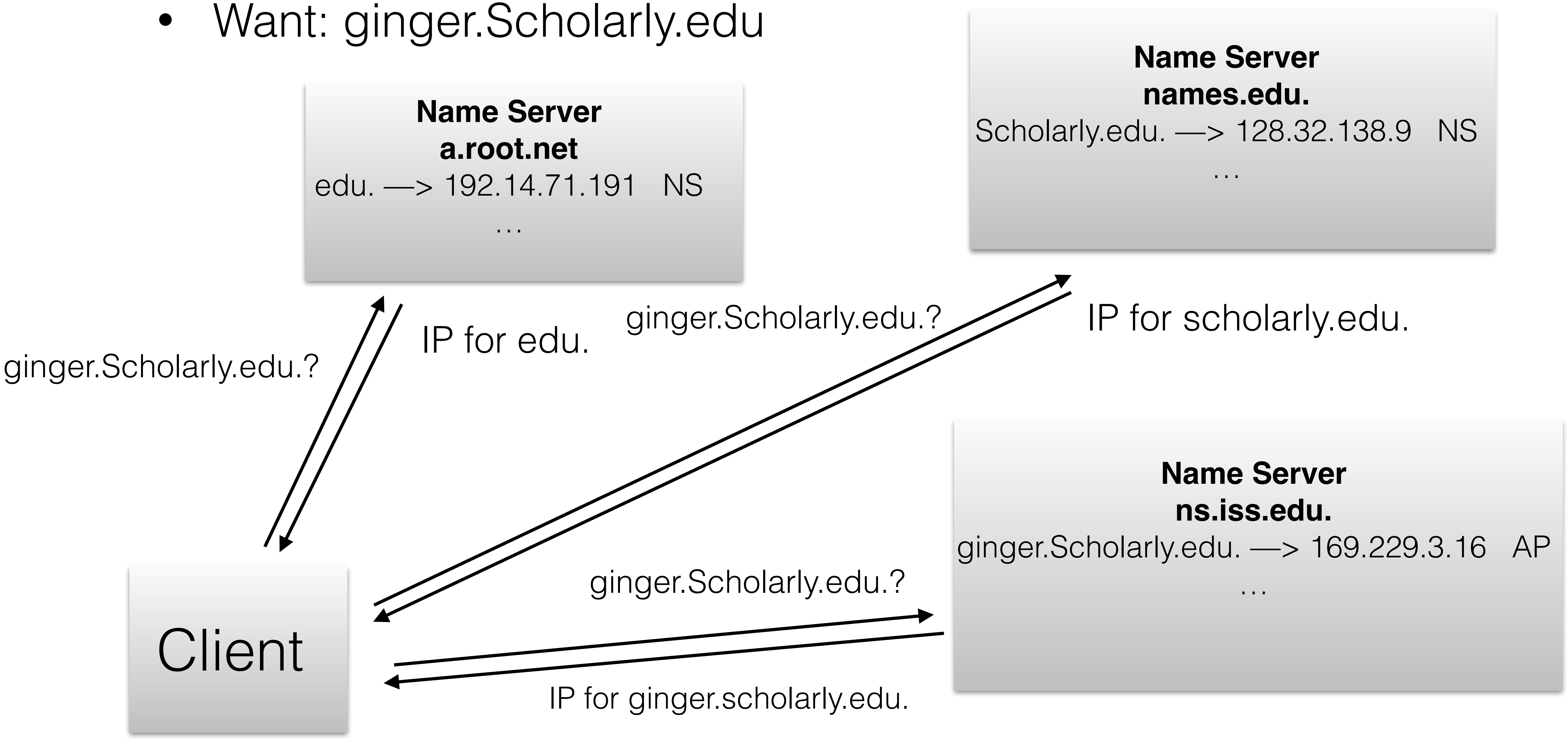
- Why naming?
  - User-friendly identifiers
  - Retrieval
  - Indirection
  - etc…
- Examples:
  - File systems
    - filename —> inode
  - DNS
    - hostname —> IP

DNS

- Mapping between hostname and IP
- Design
  - “Telephone book” — each user keeps
    - Update is a pain — network traffic
  - Centralized?
    - Possible performance bottleneck
    - Single point of failure
  - Decentralized

DNS

- Naming scheme: hierarchical
  - Want: ginger.Scholarly.edu



Name Server
a.root.net
edu. —> 192.14.71.191   NS
…

Name Server
names.edu.
Scholarly.edu. —> 128.32.138.9   NS
…

Name Server
ns.iss.edu.
ginger.Scholarly.edu. —> 169.229.3.16   AP
…

Client

ginger.Scholarly.edu.?

IP for edu.

ginger.Scholarly.edu.?

IP for scholarly.edu.

ginger.Scholarly.edu.?

IP for ginger.scholarly.edu.

DNS

- Types of records
    - A record (“address”)
        - hostname —> IP
    - NS record
        - domain name (e.g. foo.com) —> hostname of name server
    - CNAME record
        - alias name —> canonical name
    - MX record
        - name —> hostname of mail server

DNS

- Queries
    - Iterative
        - client has to handle resolving
    - Recursive
        - the server can return the final answer
        - can cache results

DNS

- Which of the following statements are true and which ones are false? (Circle True or False for each choice.) [Q1 2013]
- A. True / False A DNS name (e.g., cnn.com) may be associated with multiple IP addresses, but each IP address has to be associated with a single DNS name.
- Answer: False
- B. True / False DNS caching reduces the time to resolve an IP address, but does not reduce DNS traffic on the Internet
- Answer: False

DNS

- C. True / False If all root DNS servers fail, no DNS names can be resolved to IP addresses

- Answer: False

- D. True / False A DNS request for the IP address of a host foo.com will be resolved to the same IP address regardless of which machine issues the request.

- Answer: False

- E. True / False DNS servers remember which clients have cached DNS replies so that the servers can send invalidation messages when name bindings change.

- Answer: False