A Chat Room Assignment for Teaching Network Security

W. Garrett Mitchener

Applied & Computational Math

Princeton University

Princeton, NJ 08544

wmitchen@princeton.edu

Amin Vahdat

Department of Computer Science

Duke University

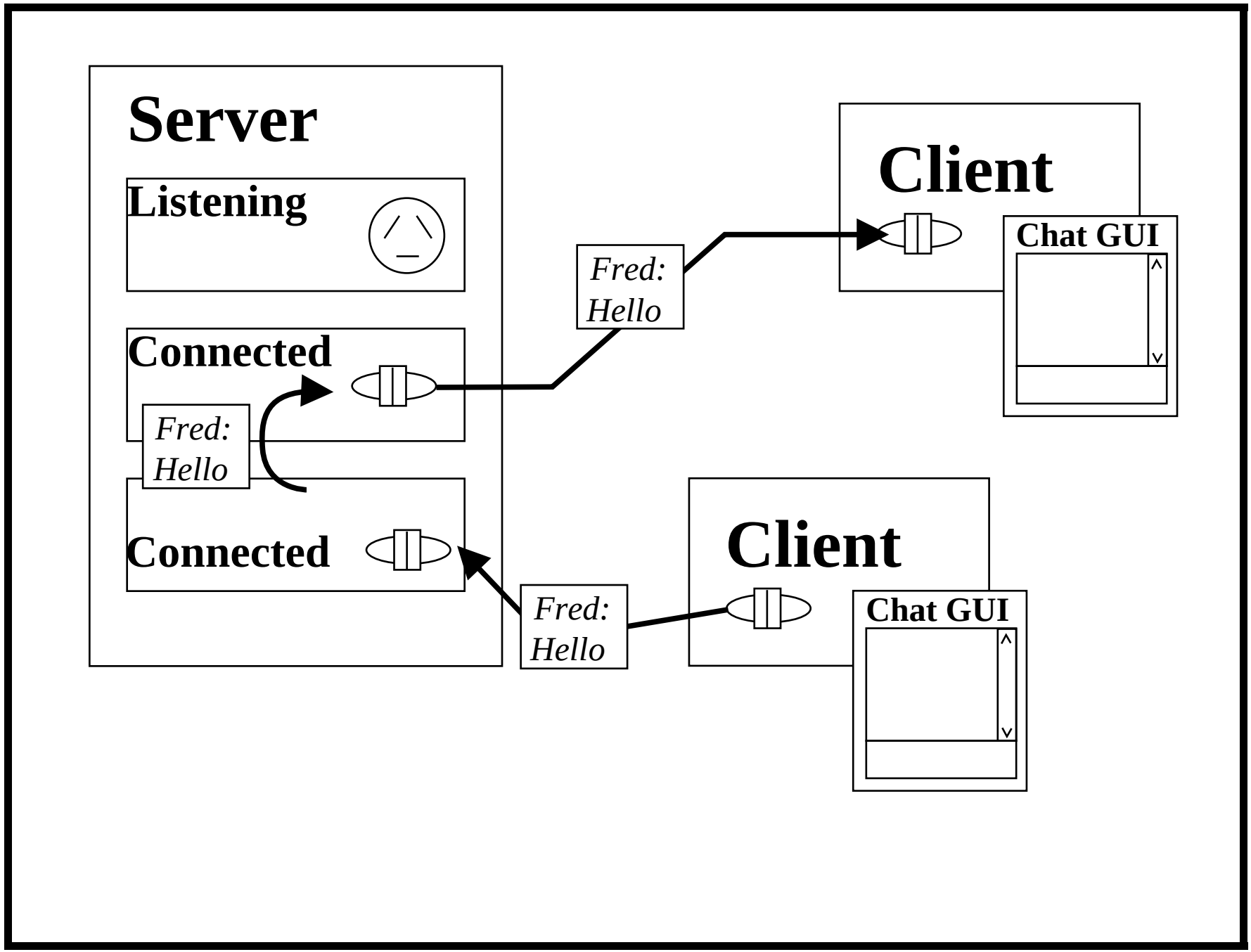
Durham, NC 27708

vahdat@cs.duke.edu

Thursday, February 22, 2001

Summary

- Basic chat room assignment
- Issues it raises
- Reasons to teach security
- Encryption for security
- Toy security system for our chat room
- Why use this assignment?

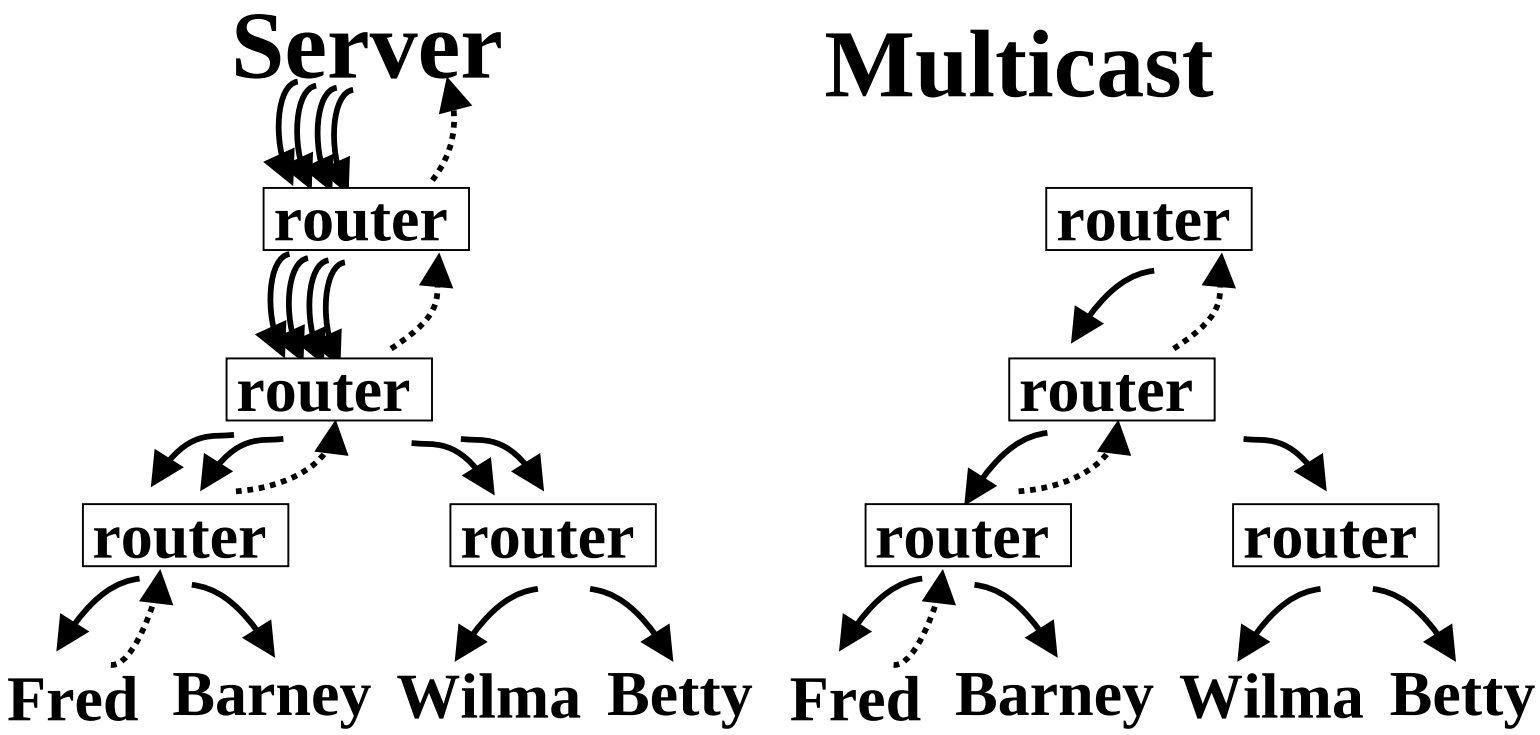

Server
Listening
Connected
Fred:
Hello
Connected
Client
Chat GUI
Fred:
Hello
Client
Chat GUI
Fred:
Hello

Concepts introduced in the basic chat room

- TCP, server sockets (listening) vs. client sockets
- Host name resolution
- Ports
- Multithreaded client and server
- Alternatives: multicast

Issues raised by the basic chat room

- Server is a bottleneck, solve with multicast



Security issues

- How can Barney be sure it's from Fred?
- Can Barney know who else saw the message?
- Is Barney sure this is what Fred said?

Why teach security?

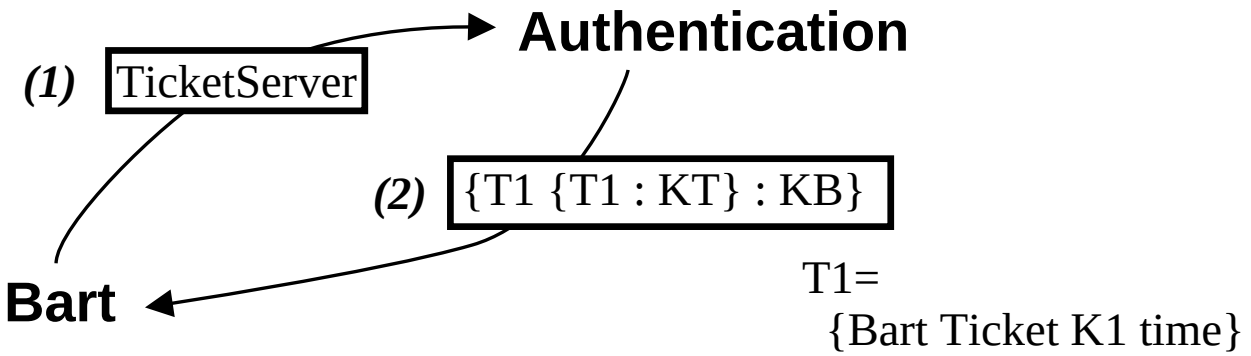
- Necessary for e-commerce
- Protect public servers from crackers
- Chat and e-mail

Vital knowledge for working in industry

Teaching security based on encryption

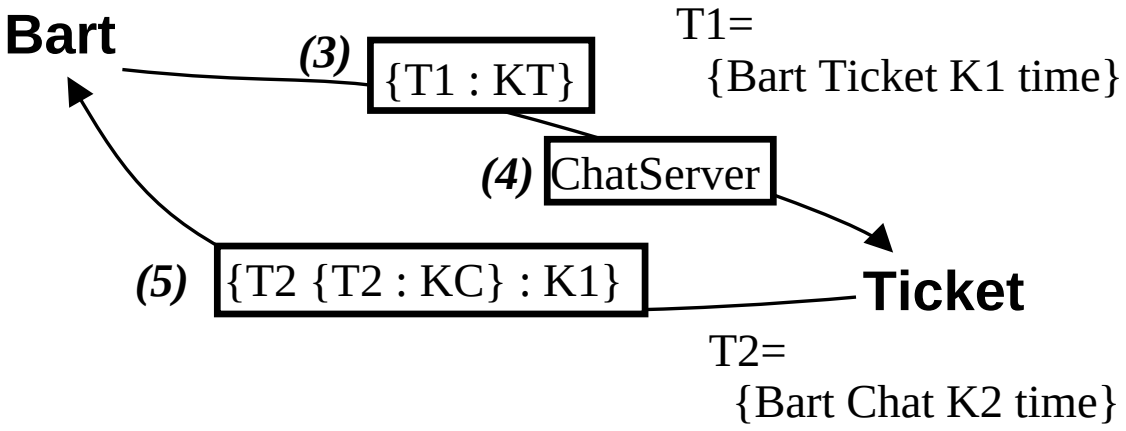
- How can encryption provide security?
  - Authentication
  - Privacy
  - Integrity
- What about existing security systems?
  - Kerberos
  - SSL
  - Digital signatures
- How secure is a system? Possible flaws? Break-ins?
  - Logic of authentication

Toy security system, based on kerberos



- Bart requests a session key for ticket server
- Authentication server constructs one, makes a “ticket”
  - One copy for Bart
  - One copy for the ticket server

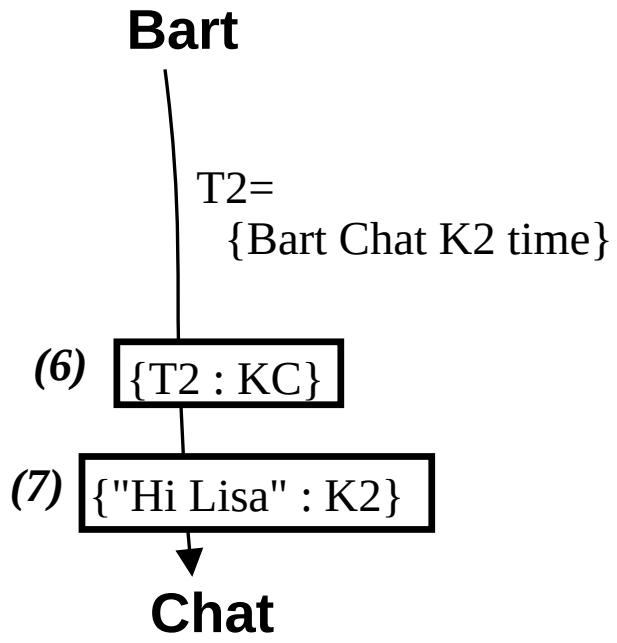
Toy security system, based on kerberos



- Bart sends first ticket to ticket server, requests a session key for chat server
- Ticket server constructs one, makes second ticket
  - One copy for Bart
  - One copy for the chat server

Toy security system, based on kerberos

- Bart sends the second ticket to the chat server
- Then he can chat



Why use this assignment?

- Why a chat room?
  - Basic assignment is simple and small
  - Entertainment value
  - Room for creativity: interface, architecture, protocols
- Why Java?
  - Threading, GUI, and parsing get out of the way
  - Focus on network concepts
  - Cryptography library readily available

The Assignment in Practice

- So far, only the insecure part has been used at Duke (CPS214).
  - Upper level undergrad, open to grad students
  - Syllabus includes how IP & friends work, routing, congestion control, mutlicast, wireless
  - First assigment
- Students who know Java take around 10 hours
- One group ported to Psion/Revo handheld, minimal effort
- Favorite bug: Not handling clients who disconnect

References & Information

- The code will be available from Dr. Vahdat
  `http://www.cs.duke.edu/~vahdat`
- *The Logic of Authentication:*
  `http://ftp.digital.com/pub/DEC/SRC/research-reports/abstracts/src-rr-039.html`
- Java Cryptography Extension:
  `http://java.sun.com/products/jce/index.html`
- This project was supported in part by the National Science Foundation (CISE-9634475).