CM214 Assignment 2003

Karl R. Wilcox
krw@ecs.soton.ac.uk
www.ecs.soton.ac.uk/~krw

Aims and Objectives

- **To construct an e-mail server**
  - **Implementing the POP3 protocol**
  - **Optional additional extensions**
- **To analyse the server for vulnerabilities**
  - **Resistance to malicious attacks**
  - **Resistance to accidental errors**
- **On completion, you should be able to:**
  - **Program with network "socket" connections**
  - **Understand and implement protocol specifications**
  - **Understand something about the trade-offs between features and security / reliability**

Resources

- Protocol Specification
  - RFC 1725
- Development environment (supporting sockets)
  - MS Windows
  - GNU/Linux
  - 'C‘ / 'C++'
  - Java
- Test Environment
  - Do not need real network
  - Can test using "loopback"
- Test Tools
  - No need to write a client
  - Telnet
  - Commercial E-mail client
- Help!
  - Peterson & Davie sec. 1.3
  - Ince & Freeman, "Programming the Internet with Java“
  - Google “POP3 tutorial”

Sockets

- A Socket is:
  - A Programming abstraction of a network connection
  - For our purposes, a reliable, error free, duplex byte stream
  - Distinguished from other sockets by its PORT number

'C' functions	Java Functions
int socket (...,addr,..)	sock = ServerSocket(port);
int bind (...)	conn = sock.accept();
int listen (...)	
int accept (...)	
int send (socket, message...)	conn.getInputStream();
int recv (socket, buffer...)	conn.getOutputStream();

An Example POP3 Session

```
S: <wait for connection on
  TCP port 110>
C: <open connection>
S:     +OK POP3 server ready
C:     USER karl
S:     +OK karl
C:     PASS secret
S:     +OK karl maildrop
C:     STAT
S:     +OK 2 320
C:     LIST
S:     +OK 2 messages (320
  octets)
S:     1 120
S:     2 200
S:     .
C:     RETR 1
S:     +OK 120 octets
S:     <the POP3 server sends
  message 1>
S:     .
C:     DELE 1
S:     +OK message 1 deleted
C:     RETR 2
S:     +OK 200 octets
S:     <the POP3 server sends
  message 2>
S:     .
C:     DELE 2
S:     +OK message 2 deleted
C:     QUIT
S:     +OK dewey POP3 server
  signing off (maildrop
  empty)
C:   <close connection>
S:   <wait for next
  connection>
```

Vulnerabilities

- Malformed requests, or headers....?
  - Careful parsing of input
- Password attacks?
  - Means to detect / deter
- Client does not close connection...?
  - Do we need a timeout?
- Very long requests paths...?
  - Check for string / buffer overflow
- Client or network fails during transaction...?
  - Handle errors returned from network

Assignment Details

- Will be posted on website
  - www.ecs.soton.ac.uk/~krw
- Web site will also include
  - FAQ list
  - Hints and tips
  - Updates
- Deadline(!)
  - Week 8 – 29th April 2003