CM214 Assignment 2004

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

Aims and Objectives

- **To construct a web server**
  - **Implementing part of the HTTP 1.1 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 2616
- 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
  - Any Web Browser client
- Help!
  - Peterson & Davie sec. 1.3 (2nd Ed) 1.4 (3rd)
  - Ince & Freeman, "Programming the Internet with Java"
  - Google "HTTP 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

```
int socket ( ...,addr,.. )
int bind ( ... )
int listen ( ... )
int accept ( ... )

int send ( socket,
    message... )
int recv ( socket, buffer... )
```

Java Functions

```
sock =
    ServerSocket(port);
conn = sock.accept();


conn.getInputStream();
conn.getOutputStream();
```

An Example HTML Session

REQUEST

```
GET /index.html HTTP/1.1
From: kwilcox@iee.org
Host: www.ecs.soton.ac.uk
User-Agent: Mozilla/5.0
[blank line]
```

RESPONSE

```
HTTP/1.1 200 OK
Date: Sun, 24 Feb 2002
23:55:43 GMT
Content-Type: text/html
Content-Length: 2334
[blank line]
<HTML>
<HEAD>
<TITLE>CM214 Assignment
</TITLE>
[rest of file.....]
```


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

- Are be posted on website
  - www.ecs.soton.ac.uk/~krw
- Web site will also include
  - FAQ list (currently last years)
  - Hints and tips
  - Updates
- Deadline(!)
  - Week 9 – 30th April 2004