Introduction to the Use of Computers

Christophe Rhodes
`c.rhodes@gold.ac.uk`

Autumn 2012, Fridays: 10:00–12:00: WTA & 15:00–17:00: WHB 300

The Internet

Address Resolution Protocol

We know: the network address (e.g. IPv4 address) that we want to send to; need to find: the hardware address (e.g. Ethernet MAC address) to send to.

- broadcast request;
- listen for reply.

Packet contents:

- Hardware (Ethernet = 1); Protocol (IPv4 = 0x800);
- Operation (Request = 1, Reply = 2);
- Sender Hardware Address;
- Sender Protocol Address;
- Target Hardware Address (zero in requests);
- Target Protocol Address;

'`arp who-has 158.223.80.218 tell router.gold.ac.uk`'

The Internet

Domain Name System

We know: the name of something we want to communicate with in some way; need to find: the network address.

- send request to ‘name server’ responsible for the domain (usually using UDP to a server on port 53);
- receive records requested back.

Types of record:

- A (IPv4 addresses)
- AAAA (IPv6 addresses)
- CNAME (host aliases)
- MX (mail handler names and ‘priorities’)
- NS (name server names)
- PTR (reverse DNS: numbers to names)

The Internet

HyperText Transfer Protocol

HTTP is for transmitting information over the World Wide Web (‘WWW’).

- HTTP/0.9 (obsolete)
- HTTP/1.0 (still in use)
- HTTP/1.1 (current)

Stateless protocol: each request/response between client and server is independent of all others.

Request format	Response Format
Request line	Status Code line
Headers	Headers
Empty Line	Empty Line
Optional Message Body	Optional Message Body

The Internet

HyperText Transfer Protocol: Requests

HTTP ‘methods’ (or ‘verbs’):

- GET (gets a resource)
- HEAD (like GET but meta-information only)
- PUT (uploads a resource), DELETE (deletes a resource)
- POST (submits data)
- TRACE (echoes request)
- OPTIONS (displays options), CONNECT (tunnels)

Example request:

```
GET /~mas01cr/teaching/fy04/ HTTP/1.0
Host: doc.gold.ac.uk
```

The Internet

HyperText Transfer Protocol: Replies

Status Codes:

- 1xx (Informational)
- 2xx (Success)
  - 200 OK
- 3xx (Redirection)
  - 301 Moved Permanently
  - 302 Found
  - 304 Not Modified
- 4xx (Client Error)
  - 401 Unauthorized
  - 403 Forbidden
  - 404 Not Found
- 5xx (Server Error)

The Internet

HyperText Transfer Protocol: Replies

Headers:

- `Content-Type`
  - `text/html`
  - `text/plain`
  - `image/gif`
  - `image/png`
  - `application/pdf`
- `Location` (used in redirection)
- `Date` (date and time of reply)
- `Server` (server name)

The Internet

The Apache HTTP Server

- Widely-deployed Web Server (running on `igor.gold.ac.uk`), developed since 1994;
- Available for a wide variety of Operating Systems;
- Supports many features;
- Free software.

Mechanism for user-level configuration: `.htaccess` files

- Password-protection;
- Customized error documents;
- URL rewriting.

The Internet

Apache: .htaccess files

Text files used for controlling the behaviour of the Web Server. Example file:

```
AuthType Basic
AuthName "Foundation Year"
AuthUserFile /home/mas01cr/public_html/teaching/is50004a/2012-13/lab07/u
Require valid-user

Options +Indexes

ErrorDocument 403 /~mas01cr/teaching/is50004a/2012-13/forbidden.txt
ErrorDocument 404 /~mas01cr/teaching/is50004a/2012-13/not-found.txt

AddType 'text/plain; charset=utf-8' text
AddType 'text/plain; charset=iso-8859-1' txt
```

The Internet

Apache: Basic authentication

Username and password dialog, protecting resources from unauthorized access:

- ‘name’ of authentication realm after `AuthName`;
- password information kept in a file;
- passwords maintained using `htpasswd` utility.

Problems:

- weak encryption;
- password transmitted in the clear over the network.

The Internet

Apache: Other customizations

- `Options`
  - `+Indexes`: allows the server to send directory indexes;
  - `+ExecCGI`: allows the server to execute scripts
- `ErrorDocument` *code url*: if the HTTP status is *code*, send *url* to the browser;
- `AddType`: associates a ‘MIME type’ with an extension.

The Internet

Simple Mail Transfer Protocol

SMTP is for sending e-mail. Handled for a domain by servers listed in MX records.

- `gold.ac.uk. 900    IN MX 7 mailhub.gold.ac.uk.`
- the ‘7’ is the server priority (used when there is more than one MX record)

Protocol:

- Greeting, handshake (banner and `HELO`)
- Envelope (`MAIL FROM` and `RCPT TO`)
- Data (`DATA`)
  - Message Headers (`Subject`, `Message-Id`, `References`)
  - Message Body

Extensions to basic protocol: use `EHLO` rather than `HELO`.

Security

Bestiary

- Virus
- Trojan
- Worm
- Phishing
- Zero-day
- Rootkit
- Backdoor

Security

Case Study: Morris Worm

Robert Morris (1988):

- "measure the size of the Internet"
- exploit vulnerabilities in multiple protocols:
  - sendmail
  - finger
  - rsh/rexec
- maybe 6000 infected hosts (estimates vary; 10% of Internet-connected Unix machines)

Security

Case Study: ILOVEYOU

- e-mail with `ILOVEYOU` as subject
- attachment named `LOVE-LETTER-FOR-YOU.txt.vbs`
- executes on opening:
  - installs password-stealing application;
  - adds windows registry entries for automatic startup;
  - finds image/audio files and replaces contents with itself;
  - e-mails itself to 50 contacts in Outlook contacts book.

Security

Case Study: Stuxnet

- spreads indiscriminately over USB sticks and peer-to-peer networking;
- uses four zero-day vulnerabilities in Windows;
- uses valid SSL certificates (Realtek, JMicron);

Security

Case Study: Stuxnet

- spreads indiscriminately over USB sticks and peer-to-peer networking;
- uses four zero-day vulnerabilities in Windows;
- uses valid SSL certificates (Realtek, JMicron);
- infects SCADA (Supervisory Control and Data Acquisition); software specific to Siemens

Security

Case Study: Stuxnet

- spreads indiscriminately over USB sticks and peer-to-peer networking;
- uses four zero-day vulnerabilities in Windows;
- uses valid SSL certificates (Realtek, JMicron);
- infects SCADA (Supervisory Control and Data Acquisition); software specific to Siemens
- makes SCADA software destructively alter rotation patterns of centrifuges.

See also: Flame

Privacy

Case Study: HMRC CDs

- CDs containing unencrypted details of Child Benefit recipients
- Sent through internal courier between HMRC and NAO...

Privacy

Case Study: HMRC CDs

- CDs containing unencrypted details of Child Benefit recipients
- Sent through internal courier between HMRC and NAO...
- ... never arrived (lost in the post)
- 25,000,000 sets of personal details

Privacy

Case Study: HMRC CDs

- CDs containing unencrypted details of Child Benefit recipients
- Sent through internal courier between HMRC and NAO...
- ... never arrived (lost in the post)
- 25,000,000 sets of personal details

See also:

- Sony Online Entertainment / Playstation Network
- Citigroup credit cards
- Bank of Scotland mortgage details
- ... many many other examples

Privacy

Case Study: HMRC CDs

- CDs containing unencrypted details of Child Benefit recipients
- Sent through internal courier between HMRC and NAO...
- ... never arrived (lost in the post)
- 25,000,000 sets of personal details

See also:

- Sony Online Entertainment / Playstation Network
- Citigroup credit cards
- Bank of Scotland mortgage details
- ... many many other examples

Remedy: ubiquitous encryption (e.g. GPG)

Privacy

Case Study: Google Streetview

- Cars driving around, taking pictures
- (Some) automated blurring of faces ...
- ... but imperfect

Privacy

Case Study: Google Streetview

- Cars driving around, taking pictures
- (Some) automated blurring of faces ...
- ... but imperfect

Meanwhile...

- cars also located WiFi Access Points...

Privacy

Case Study: Google Streetview

- Cars driving around, taking pictures
- (Some) automated blurring of faces ...
- ... but imperfect

Meanwhile...

- cars also located WiFi Access Points...
- ... and snooped traffic, logging e-mails, passwords, and so on

Privacy

Case Study: Google Streetview

- Cars driving around, taking pictures
- (Some) automated blurring of faces ...
- ... but imperfect

Meanwhile...

- cars also located WiFi Access Points...
- ... and snooped traffic, logging e-mails, passwords, and so on

Remedy: Move to Germany or India; even more encryption (e.g. WPA2)

Privacy

Case Study: General Petraeus

- Paula Broadwell's gmail monitored because of harrassment
- IP address accessing Broadwell's gmail also accessing another gmail account
- a different IP address also accessing that second gmail account...
- ... which turned out to be an IP address associated with Petraeus.

See also:

- cases against alleged 'Anonymous' activists

Privacy

Case Study: General Petraeus

- Paula Broadwell's gmail monitored because of harrassment
- IP address accessing Broadwell's gmail also accessing another gmail account
- a different IP address also accessing that second gmail account...
- ... which turned out to be an IP address associated with Petraeus.

See also:

- cases against alleged 'Anonymous' activists

Remedy: consistent anonymisation (e.g. Tor), privacy-conscious e-mail providers (e.g. not gmail)