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

Security

Bestiary

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

Security

Virus

A virus is a computer program which can:

- attach itself to existing files;
- replicate itself;
- spread from computer to computer.

Security

Virus

A virus is a computer program which can:

- attach itself to existing files;
- replicate itself;
- spread from computer to computer.

Examples of transmission/host mechanisms:

- executable files;
- volume boot / master boot records;
- application-specific script files;
- web cross-site scripting.

Security

Virus

A virus is a computer program which can:

- attach itself to existing files;
- replicate itself;
- spread from computer to computer.

Examples of transmission/host mechanisms:

- executable files;
- volume boot / master boot records;
- application-specific script files;
- web cross-site scripting.

```
--
Hi!  I'm an e-mail signature virus!  Copy me into your
~/.signature and watch me spread!
```

Security

Trojan / Worm

A Trojan (from Trojan Horse):

- is an application or file that looks innocuous;
- has malicious effects when accessed or run.

Security

Trojan / Worm

A Trojan (from Trojan Horse):

- is an application or file that looks innocuous;
- has malicious effects when accessed or run.

A worm:

- is an application;
- attempts to propagate to other hosts on a network (by abusing vulnerabilities in other network services).

Security

Phishing

A *social-engineering* attack:

- fools users into giving away credentials;
- masquerade as trusted entities in communication;
- (often) involves facsimile websites;
- (usually) involves sending bogus e-mails.

Security

Phishing

A *social-engineering* attack:

- fools users into giving away credentials;
- masquerade as trusted entities in communication;
- (often) involves facsimile websites;
- (usually) involves sending bogus e-mails.

Particular problem: URLs

- `www.sainsburysbank.co.uk`
- `www.sainsburysbank.co.uk`

Security

Zero-day

A zero-day (*Zero-day vulnerability*):

- a newly-discovered vulnerability in an application or system;
- has not been disclosed to anyone in advance.

Particularly valuable to agents hoping to use vulnerabilities:

- can measure according to price:
  - Android: $\sim$ \$30k
  - Word: $\sim$ \$50k
  - iOS: $\sim$ \$100k
- (selling vulnerabilities is – at present – legal)

Security

Rootkit

A rootkit (*root* is the name of the administrative user on Unix):

- an application which modifies the behaviour of the operating system;
- hides its own existence;
- hides existence of other malicious software;
- prevents its own removal.

Security

Rootkit

A rootkit (*root* is the name of the administrative user on Unix):

- an application which modifies the behaviour of the operating system;
- hides its own existence;
- hides existence of other malicious software;
- prevents its own removal.

Example: Sony BMG music player

- Extended Copy Protection software:
  - music player;
  - rootkit (preventing some uses of CD).
- hid files with names beginning with `$sys$`;
- soon after discovery, other malware applications began naming their files in this way.

Security

Backdoor

A backdoor:

- unadvertised mechanism for bypassing authorization;
- allows undetected access to systems

Example mechanisms:

- hard-coded administrative usernames/passwords
- command shell on open network port
- broken cryptographic algorithm use

Computers and the Law

I am not a lawyer

Computers and the Law

I am not a lawyer

Nothing in these lectures is legal advice

Computers and the Law

I am not a lawyer

Nothing in these lectures is legal advice

If in any doubt: pay a laywer for legal advice

Computers and the Law

Computer Misuse Act

`http://www.legislation.gov.uk/ukpga/1990/18`

Computer Misuse Act (1990) covers criminal acts involving misuse of computers:

- unauthorised access to data; or
- unauthorised modification of computer material.

Aggravating factor:

- data accessed or modified intended to be used in a subsequent crime. ('... with intent')

Maximum penalty: 6 months' imprisonment, amended to 2 years in Police and Justice Act (2006).
(At the moment, 'smartphones' do not count as computers)

Computers and the Law

Computer Misuse Act: Case Study

Andrew Auernheimer and Daniel Spitler:

- discovered that AT&T displayed e-mail addresses of iPad users
- mechanism was based on URLs encoding ICC-ID of iPad
- generated all possible URLs
- accessed URLs (not password-protected, not encrypted)
- sold list of iPad user e-mail addresses to news outlet

Computers and the Law

Computer Misuse Act: Case Study

Andrew Auernheimer and Daniel Spitler:

- discovered that AT&T displayed e-mail addresses of iPad users
- mechanism was based on URLs encoding ICC-ID of iPad
- generated all possible URLs
- accessed URLs (not password-protected, not encrypted)
- sold list of iPad user e-mail addresses to news outlet
- Auernheimer convicted in New Jersey
- Sentence of up to 10 years in federal prison

Computers and the Law

Computer Misuse Act: Case Study

Andrew Auernheimer and Daniel Spitler:

- discovered that AT&T displayed e-mail addresses of iPad users
- mechanism was based on URLs encoding ICC-ID of iPad
- generated all possible URLs
- accessed URLs (not password-protected, not encrypted)
- sold list of iPad user e-mail addresses to news outlet
- Auernheimer convicted in New Jersey
- Sentence of up to 10 years in federal prison

(This is US law really: Computer Fraud and Abuse Act (1986))

Computers and the Law

Data Protection Act

`http://www.legislation.gov.uk/ukpga/1998/29`

Data Protection Act (1998) covers handling of personal data for non-domestic use:

- data may only be used for its stated purpose;
- data may not be disclosed to third parties without individual consent;
- individuals have a right of access to information held about them;
- entities holding data are required to have adequate security measures in place.

Compliance is overseen by the Office of the Information Commissioner. The Data Protection Act interacts with the Freedom of Information Act (2000), also overseen by the OIC.

Computers and the Law

Data Protection Act: Points to Ponder

- Journalistic exemption (cf Leveson)
- Responsibilities of businesses:
  - startups: cloud services (e.g. Google Drive)
  - larger organizations: data location
- Not just about loss of data (cf Prudential fine for inaccurate data)

Computers and the Law

Communications Act

`http://www.legislation.gov.uk/ukpga/2003/21`

Communications Act (2003) covers electronic communication

- sets up Ofcom
- recognizes community radio;
- reduces rules of cross-media ownership

Computers and the Law

Communications Act

`http://www.legislation.gov.uk/ukpga/2003/21`

Communications Act (2003) covers electronic communication

- sets up Ofcom
- recognizes community radio;
- reduces rules of cross-media ownership
- criminalizes use of open wifi without permission
- covers improper use of electronic communications network

Computers and the Law

Communications Act: Case Study

Azhar Ahmed:

- reacted to death of 6 British soldiers by an IED in Afghanistan:
- posted to Facebook page that "all soldiers should die and go to hell"
- sentenced under the Communications Act to £300 fine and 240 hours of community service

related:

- Paul Chambers (fined £385, conviction eventually overturned)
- Matthew Wood (imprisoned for 12 weeks)
- (currently anonymous) Kent teenager

Computers and the Law

Copyright

Covers the **expression** of ideas:

- books;
- music recordings;
- films, art, musical scores, plays, ...

Computers and the Law

Copyright

Covers the **expression** of ideas:

- books;
- music recordings;
- films, art, musical scores, plays, ...
- ... computer programmes.

Under what circumstances are you allowed to copy them?

- never;
- ... unless specifically allowed.

Running a computer programme involves making digital copies!

The Law

Copyright: Licences

Terms under which you may use or distribute software:

- End User Licence Agreement (EULA): typically only use.
  - not allowed to give install CD to friend;
  - not allowed to install on more than one computer;
  - not allowed to install on certain kinds of computer.

The Law

Copyright: Licences

Terms under which you may use or distribute software:

- End User Licence Agreement (EULA): typically only use.
  - not allowed to give install CD to friend;
  - not allowed to install on more than one computer;
  - not allowed to install on certain kinds of computer.
- 'Free Software' licences:
  - no restrictions on use of software;
  - redistribution allowed, subject to conditions

The Law

Copyright: Licences

Terms under which you may use or distribute software:

- End User Licence Agreement (EULA): typically only use.
  - not allowed to give install CD to friend;
  - not allowed to install on more than one computer;
  - not allowed to install on certain kinds of computer.
- 'Free Software' licences:
  - no restrictions on use of software;
  - redistribution allowed, subject to conditions

Example: GNU General Public License (GPL), used for Linux kernel

- allowed to redistribute software in source code form;
- allowed to redistribute software in binary form, if source code is also made available.

Computers and the Law

Patents

Protects the **use** of an idea ("invention"):

- only the patenting organization can exploit it...
- ... for 20 years.
- At present, software (on its own) is not patentable in the UK
- ... but that may change.

Effects seen in US (where software patents exist):

- 'submarine' patents;
- patent trolls.

Computers and the Law

Patents: Case Study

"Submarine" patent / patent ambush:

- patent some invention;
- allow use of invention without disclosure of patent existence;
- once use invention is embedded, start requesting patent licence fees.

Example: Unisys / GIF-LZW patent.

Computers and the Law

Patents: Case Study

Patent trolls

- patent some invention (or, more likely, buy patent);
- does not attempt to exploit patent itself;
  - non-practicing entity;
- instead, sues other companies for patent infringement.

Example: Eolas vs Microsoft / browser plugin