COM6650/6655
Professional Issues in Information Technology
Part IX:Computer Misuse and Computer Crime

Dr. Amanda Sharkey

Department of Computer Science
University of Sheffield

- Take home exam: to be released on Mole on Tuesday 1st December
- 3 exam-style questions
- Due Monday 14th December

- 1 Introduction
- 2 What is Computer Misuse?
- 3 Computer Fraud
- 4 Software Piracy
- 5 Viruses
- 6 Hacking
- 7 The Computer Misuse Act 1990
- 8 Conclusions
- 9 Summary

- **1 Introduction**

- IT has changed the way in which crimes are committed:
- Valuable assets are stored as computer data;
- Telecommunications have broadened the geography of crime;
- Computers have given rise to a new range of criminal activities such as computer hacking and viruses.
- Much of this activity has captured the imagination of the public, but is computer crime really a big problem?

Type of		1994		1990		1987
	No.	*Direct Loss*	*No.*	*Direct Loss*	*No.*	*Direct Loss*
Fraud	*108*	*2,904,430*	*73*	*1,102,642*	*61*	*2,526,751*
Theft	*121*	*196,305*	*27*	*1,000*	*22*	*34,500*
Hacking	*47*	*65,500*	*26*	*31,500*	*35*	*100*
Viruses	*261*	*30,485*	*54*	*5,000*	*0*	*0*
Totals	*537*	*3,196,720*	*180*	*1,140,142*	*118*	*2,561,351*

- **1.1 What is the scale of computer crime?**
- Data on computer crime is collected by the Audit Commission (http://www.auditcommission.gov.uk).

- Theft covers loss to employers through theft of data or software; seldom does this cause any direct loss.

  1997 update to this survey found 10% increase since 1994 in number of organisations reporting computer misuse

- Audit Commission UK (2005) figure for total value of fraud in public sector was £83 million (not restricted to computer fraud)
- Problem of under-reporting.
- US survey (2004) estimated that phishing attacks cost US banks $1.2 billion in 2003, and 57 million Americans had received phishing e-mails.

2012 Cost of Cyber Crime Study: United States

- Ponemon institute report:
- Average annual cost of cyber crime for 56 organisations was $8.9 million per year
- Most costly: denial of service, malicious insiders and web-based attacks.

2 What is Computer Misuse?

- In the late 1980s there was growing concern about hackers and the damage they could cause.
- Two studies: Scottish Law Commission (reported 1987), English Law Commission (reported 1989)

- Scottish Law Commission identified eight different categories of computer misuse in a 1987 report.
- Prompted the Computer Misuse Act 1990 (CMA).
- Bear in mind that the actions described below will sometimes give rise to liabilities under civil law.

Eight different categories of computer misuse identified by Scottish Law report (1987)

(1) Erasure or falsification of data or programs to gain a financial or other advantage

This category deals with fraud or theft

(2) Obtaining unauthorised access to a computer

This covers hacking and unauthorised use of an employer's computer by an employee.

Hackers that damage computer systems often have no intention of doing so. Without intent, there is no crime. This loophole has been addressed by the CMA.

Eight different categories of computer misuse identified by Scottish Law report (1987) continued ….

3) Eavesdropping on a computer

This involves the use of equipment to pick up radiation emissions from a computer screen.

(4)Taking information without physical removal

Legal problems arise here since 'information' is not a physical thing; it cannot be stolen.

Dealing with this problem would require changes to the law of theft; a major undertaking.

Copyright, patents and law of confidence offer some protection.

Eight different categories of computer misuse identified by Scottish Law report (1987) continued

(5) Unauthorised borrowing of computer material

Borrowing of computer media does not constitute theft.

(6) Denial of access to authorised users

A user of a computer system could prejudice other users by denying them access to the computer, or denying them access to particular data that they need.

(7) Unauthorised use of computer time/facilities

Authorised users of a computer could use them for unauthorised uses, such as private research and development which is competitive with their employer.

(8) Malicious or reckless corruption or erasure of data or programs

The results of this activity could cause financial loss, damage to the environment or even loss of life.

Basics of English criminal law

- Most criminal offences are set out in Acts of Parliament: e.g. Theft Act 1968, Fraud Act 2006, Computer Misuse Act 1990.
- Some common law offences remain, e.g. Murder
- Elements of an offence can be analysed in terms of
  - *Mens rea* (mental element, and intention)
  - *Actus reus* (actual behaviour)
- Some offences termed 'strict liability offences' for which there is no *mens rea*
  - *(*e.g. Driving at night with faulty rear light is an offence even if the driver did not know the light was faulty)

- Criminal offences:
  - Police informed
  - They may charge the person and then pass the case over to the Crown Prosecution Service.
  - Accused appears in Magistrates court
  - Case may be committed for trial in Crown Court.
  - Minor (*summary*) offences dealt with in magistrates court
  - Serious (*indictable*) offences tried in Crown Court.
  - Intermediate offences, e.g. Theft and fraud, are triable either way (magistrate or crown court).

3. ICT Fraud

- Computer systems vulnerable to fraud.
  - E.g. **R v Sunderland (unreported) 1983,** employee of Barclays Bank used bank's computer to find a dormant account, and then forged the holder's signature to withdraw £2,100.
  - Sentenced to 2 years imprisonment, but illustrates vulnerability of such systems, especially from within an organisation.

3.1 Types of computer fraud (Audit Commission)

3.1.1 Entry of an unauthorised instruction (input fraud)

Unauthorised alteration of data prior to it being input into a computer. Probably common.

Example: input data forms

3.1.2 Alteration of input data (data fraud)

Data held on a computer system is modified for fraudulent means.

3.1.3 Suppression of data (output fraud)

Output from a computer system is destroyed or altered. The motive is usually to conceal criminal activity.

Example: audit rolls from cash till

3.1.4 Program fraud

Alteration of a computer program. Sophisticated, and therefore hard to detect

Example: salami fraud

3.2 Fraud offences

- Fraud is a collection of similar offences, some of which were covered by the Theft Acts 1968 and 1978

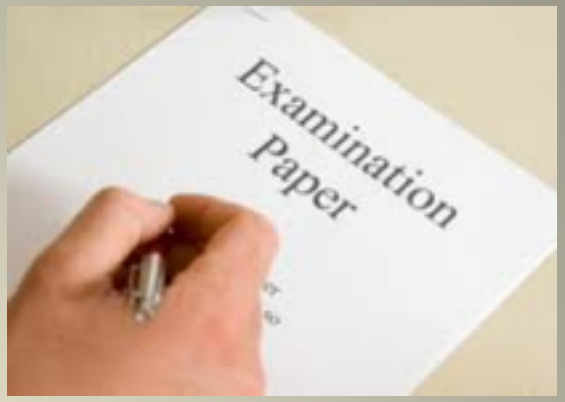
3.2.1 Obtaining property by deception

- **Problems with old deception offences**

- **The Theft Act 1968** defines the offence of theft as follows:
- ***A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it, shall on conviction on indictment be liable to imprisonment for a term not exceeding ten years***.
- This definition implies the deception of a person. The Law Lords confirmed this view in 1974: for a deception to take place there must be some person or persons who will have been deceived
- A person committing a computer fraud deceives the computer, not a human mind. So, this offence is probably inappropriate for computer fraud.

- The **Theft Act 1968** defines the offence as follows:
- ***A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it, shall on conviction on indictment be liable to imprisonment for a term not exceeding ten years***.

- If a person gains access to a computer system without permission and then makes a printout of the information contained therein, has he committed theft?



- **Oxford v Moss (1978)**
- Student ‘borrowed’ an examination paper before the exam
- Could not be prosecuted for theft since he returned the item
- Was prosecuted for theft of confidential information
  - But acquitted on grounds that information cannot be regarded as property and so cannot be stolen.

- **R v Lloyd (1985)**
- Projectionist in a cinema and 2 others, took films from cinema, and copied them but returned them.

The pirated copies were sold at a considerable profit

- BUT the charge of theft (conspiracy to steal) was held to be inappropriate
- no intention to permanently deprive.
- charge of conspiracy to defraud might have worked better

- **3.2.2 Conspiracy to defraud**
- **Common law offence**
- A conspiracy is an agreement between two or more persons to carry out an unlawful act.
- Conspiracy to defraud may be applicable to computer fraud, since deception need not be proven

- **Theft Act 1968**:
- Dishonestly extracting electricity
  - Unauthorised access will result in some consumption of electricity
  - But will have to demonstrate that the person realised they were being dishonest
  - R v Ghosh (1982) *Ghosh Test*
  - *Need to determine whether the defendant himself realised that what he was doing was by [ordinary standards of reasonable and honest people] dishonest*

- **3.2.3 Attempts**
- To be charged with an attempt, a person must have done an act which is 'more than merely preparatory to the commission of an offence'.
- A computer fraud which is not completed may be an attempt to steal money. Confusion over this is one reason why section two of the Computer Misuse Act 1990 was enacted (see later).
- See also Fraud Act 2006
- **3.2.4 Fraud as theft**
- Applying the offence of theft to computer fraud normally presents no problems, excepting our reservations about permanently depriving.

Fraud Act 2006

Deals with some of deficiencies of Theft Acts 1968 and 1978, especially ICT fraud

A person is guilty of fraud if in breach of any of the following:

- (i) fraud by false representation
- (ii) fraud by failing to disclose information
- (iii) fraud by abuse of position

Penalties:

Summary conviction (Magistrates court): imprisonment for up to 12 months and/or fine

Conviction on indictment (Crown court trial by jury): imprisonment for up to 10 years and/or fine

- ***(i) Fraud by false representation*** (Fraud Act 2006, section 2)
  - Occurs when person dishonestly makes a false representation, intending to make a gain for himself or another, or to cause loss to another, or to expose another to risk of loss.
  - E.g. '**phishing**' obtaining information such as bank account details by sending email (or SMS) purporting to be from that person's bank
  - E.g. '**pharming**' (directing traffic to genuine website to bogus one)
  - Unlike Theft Act 1968 (permanently deprive), no need for actual gain or loss, or for it to be permanent.

- ***(ii) Fraud by failing to disclose information (Fraud Act 2006 Section 3)***
- This form of offence of fraud applies when a person dishonestly fails to disclose to another person information which he is under a legal duty to disclose, and intends, by failing to disclose the information, to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss.
- Maybe relevant for online transactions –
  - E.g. Electronic submission of tax returns, road tax fund, television licenses.

- ***(iii) Fraud by abuse of position (section 4 of Fraud Act 2006)***
- Applies when a person occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person.
  - Typical example of offence: person with enduring power of attorney misuses position to draw funds from the donor's bank account.
  - Or where employee of software company uses his position to make unauthorised copies of his employer's software to sell for his own benefit.
  - Or where employee sells an email containing confidential information belonging to the employer to a rival company.

- ***Articles for use in fraud***
  - Possession of article, or making or supplying articles

  - **Section 6 of Fraud Act 2006**, makes it an offence for a person to have in his possession or under his control any article for use in the course of or in connection with any fraud.
    - Might include decryption software if intended to be used for fraud

    - Summary conviction: up to 12 months imprisonment and/or fine
    - On conviction in indictment: maximum penalty 5 years imprisonment

  - **Section 7 of Fraud Act 2006**: an offence made out if a person makes, adapts, supplies, or offers to supply any article
    - Knowing that it is designed or adapted for use in the course of or in connection with fraud;
    - Intending it to be used to commit or assist in the commission of fraud.
    - E.g. Software to circumvent technological m Summary conviction: up to 12 months imprisonment and/or fine
    - On conviction in indictment: maximum penalty 10 years imprisonment measures applied to copyright works to prevent unauthorised acts in relation to those works.
    - .

- ***Obtaining services dishonestly***
- Fraud Act 2006, section 11
  - Replaces section 1 of Theft Act 1978, obtaining services by deception.
  - Might not have applied when deception did not operate on a human being e.g. Service obtained by entering password, checked by computer.
  - Offence committed by person who obtains services for himself or another by dishonest act where
    - A) the services are made available on the basis that payment has been, is being or will be made for or in respect of them
    - B) he obtains them without any payment having been made for or in respect of them or without payment being made in full and
    - C) when he obtains them, he knows
      - That they are being made on the basis described in (a) or that they might be, but intends that payment will not be made, or will not be made in full.
  - Maximum penalty
    - On summary conviction, imprisonment for term not exceeding 12 months, and/or fine
    - On conviction on indictment, imprisonment for 5 years and/or fine.

- 1 Introduction
- 2 What is Computer Misuse?
- 3 Computer Fraud
- 4 Software Piracy
- 5 Viruses
- 6 Hacking
- 7 The Computer Misuse Act 1990
- 8 Conclusions
- 9 Summary

4 Software Piracy

- For many, the concept of software piracy is a difficult one to grasp because, in economic terms, software resembles what is called a 'public good'.
- Example: a public good
  - Free-to-air-television
    - non-rivalrous (consumption by one doesn't reduce availability to others) and non-excludable (no-one can be excluded)

- Anti-piracy organisations such as FAST mount raids on software pirates, using special search warrants.
- FAST estimate that 30% of all software in use in the UK is infringing, costing the software industry several 100 million pounds per year.
- See http://www.fast.org.uk

4.1 Fighting software piracy

- Auditing programs can automate the detection of illegally copied software on computer networks.
- Hardware copy-protection 'keys' can be used, but are unpopular with consumers.
- An alternative is a software key.

- **4.2 Legislation applicable to software piracy**
- Copyright, Designs and Patents Act 1988; defines a number of criminal offences; the most serious are for distributing and importing.
- Forgery and Counterfeiting Act 1981; a disc, tape or other recording medium may be a 'false instrument'.
- Trade Descriptions Act 1968; intended to protect consumers from buying inferior goods, e.g. copied software which is being sold as the genuine article.

5 Viruses

Viruses are programs that are devised to be copied inadvertently. They are concealed in other programs or data, and damage or slow the operation of their 'host' systems.

The Audit Commission find that viruses are the most common form of computer abuse.

The '**I Love You**' virus released in 2000 was estimated to have a worldwide economic impact of $8.75 billion (CSI/FBI Computer Crime and Security Survey, 2002)

- Computer Misuse Act 1990: one of its purposes was to criminalise the use of computer viruses

6. Hacking

- Computer hacking is the accessing of a computer system without the express or implied permission of the owner of that computer system.
- **6.1 R v Gold (1988)**
- See: Bainbridge, p. 440 Sixth edition

The case of R versus Gold:

Two journalists gained access into BT Prestel Gold computer network without permission and altered data.

One also gained access to Duke of Edinburgh's personal computer files and left message

"Good afternoon HRH Duke of Edinburgh"

They claimed they gained access to network to highlight deficiencies in security.

They were charged under Forgery and Counterfeiting Act 1981 on making a false instrument – the CIN (customer identification number) and password.

Journalists found guilty at Crown court, and fined (£750 and £600)

Convictions quashed by Court of Appeal, and confirmed by House of Lords

Acts were a dishonest trick, not criminal offences

If the conviction had been upheld, would mean defendants had deceived a computer

After R vs Gold case, which concluded that hacking was not a criminal offence per se, the computer industry became dissatisfied with the scope of criminal law.

This prompted the **Computer Misuse Act 1990**. Unusually, this was introduced as a private member's Bill.

Hacking with the intent to commit a further crime such as theft, or damage by altering data, is now a serious criminal offence under the Act.

Hacking without intention to commit a further crime is a minor criminal offence under the Act.

6.2 Other offences associated with hacking

The Computer Misuse Act 1990 is the main weapon against hacking, although other areas of criminal law may be relevant:

The law of theft

Regulation of Investigatory Powers Act 2000 (RIPA)

Data Protection Act 1998 (DPA)

RIPA concerns the intentional interception of communications on public and private telecommunications system, including data networks.

The DPA regulates the use and storage of 'personal data', i.e. information relating to individuals that can be identified from that information.

If a computer hacker copies personal data and stores it on his own computer, he is holding personal data without being registered. This is a criminal offence.

7 The Computer Misuse Act 1990

The Act creates three new offences.

CMA Section 1: Unauthorised access to computer material

A person is guilty of this offence if he *'...causes a computer to perform any function with intent to secure access to any program or data held in any computer;*

the access he intends to secure is unauthorised;

and he knows at the time when he causes the computer to perform the function that this is the case..'

This offence aims to deter hackers without requiring any evidence of intention to commit a crime or alter data or programs.

The penalty is moderate - a fine, or a prison sentence not exceeding six months duration.

What is the significance of the third clause?

- **CMA Section 2: Unauthorised access with intent to commit or facilitate further offences**
- **(ulterior intent offence)**
- A person is guilty of this offence if he commits an '...unauthorised access offence with intent to commit an offence to which this section applies; or facilitate the commission of such an offence (whether by himself or any other person)..'
- The 'offence to which this section applies' means any criminal offence for which the sentence is at least five years, such as fraud, theft or blackmail.
- Addresses a more serious form of hacking, in which unauthorised access is gained with intent to commit a further crime, whether or not that further offence involves the use of a computer.
- Particularly useful if the offence is not completed. E.g. Person attempts to gain access to a computer with the intention of sending a blackmail message, but doesn't get beyond login screen. Could still be convicted if it's shown that they had
  - Intention to secure access
  - Knowledge that access is unauthorised
  - The intention to commit blackmail
- The penalty is greater - a large fine, a prison term not exceeding five years, or both.

- **CMA Section 3: Unauthorised modification of computer material**
- A person is guilty of this offence if 'he does any act which causes an unauthorised modification of the contents of any computer; and at the time when he does the act he has the requisite intent and the requisite knowledge'.
- The term 'requisite intent' means to:
  - Impair the operation of a computer
  - Prevent or hinder access to a program or data held in any computer
- Impair the operation of a program or reliability of data
- The intent need not be directed specifically at:
  - A particular computer
  - A particular program or data or a program or data of any particular kind
  - A particular modification or a modification of any particular kind
- Penalty: Like section 2, maximum of 5 years imprisonment or unlimited fine

- This offence covers four forms of conduct:
- 1. Unauthorised erasure of programs or data contained in computer memory or on a storage medium.
- 2. The circulation of a virus infected program, with the intention of causing a modification that will impair the operation of the recipient's computer.
- 3. Unauthorised addition of a virus to a computer's library of programs, which will impair the operation of the recipient's computer by using up its capacity.
- 4. Unauthorised addition of a password to a data file, thereby rendering that data inaccessible to anyone who does not know the password.

7.4 Problems with the Computer Misuse Act

The first contested Crown Court trial under the CMA came to court in April 1993, and had problems.

First major case brought under Computer Misuse Act

7.4.1 The Paul Bedworth case

R v Paul Bedworth

Southwark Crown Court

Computer Misuse Act 1990, ss 1, 3 Unauthorised access - Unauthorised modification - Conspiracy

Hacking from his bedroom in mother's house- JANET, BT, Financial Times, European Commission sites. Alleged damage of £120,000. Expert psychiatric evidence of obsessive addiction to hacking. Held - defendant was "addicted to hacking", and lacked criminal intent. Defendant acquitted.

Possibly his young age (18) was a factor, also heavy-handed arrest.

Hackers' charter?

7.4.2 Following the Bedworth case

There was some consolation for the police. Two of Bedworth's friends, Neil Woods and Karl Strickland, pleaded guilty to similar charges under the CMA.

They both got six months imprisonment. In his summing up, judge Michael Harris said:

'...if your passion had been cars rather than computers we would have called your conduct delinquent, and I don't shrink from the analogy of describing what you were doing as intellectual joyriding...hackers need to be given a clear signal by the Courts that their actions will not and cannot be tolerated...'

It seems unlikely that the Bedworth case represents a legal loophole in the Computer Misuse Act 1990. A member of the Law Commission commented:

'...I don't think there's a loophole. Only in limited circumstances is this defence likely to be used again, and the jury's decision in this case strikes me as extraordinary...'

Indeed, there have been many successful prosecutions since.

7.4.3 Are there problems with the Act?

- The Computer Misuse Act 1990 is cautious, reflecting the great care that must be taken when drafting this kind of legislation.
- The CMA addresses most of the areas of computer misuse identified by the Scottish Law Commission report, apart from electronic eavesdropping.
- **The term 'computer' is not defined by the Act. Is this a problem?**
- A concern is the meaning of 'unauthorised access'. What is the situation when access is authorised but the function performed is not?
- Example: DPP v Bignell (1998)
- See Bainbridge pp. 442-3 sixth ed.


- **DPP v Bignell (1998**)
- Two police officers used police national computer to gain access to details of motor cars they wanted for private purposes unconnected with duties as police officers.
- Charged with unauthorised access to computer material under section 1 of CMA 1990
- Appeals allowed – their access was authorised
- ....worrying decision

- But soon reversed in House of Lords:

- **R vs Bow Street Metropolitan Stipendiary Magistrate (2000)**
- Employee of American Express in Florida was authorised to access specific customer accounts – but she accessed other accounts and passed on confidential information allowing counterfeit credit cards to be made.

- Decision: Authorisation should not extend to access computer material for unauthorised purpose

- Lord Hobhouse criticised the decision made in **DPP v Bignell-** should have been concerned with authority to access the actual data involved, not just the kind of data.
- Employee had authority to access the kind of data she accessed, but not the particular data she accessed.
- i.e. Authorisation to access computer material does not extend to accessing computer material for an unauthorised purpose.

- Using logged on computer if someone has left themselves logged on.
- ***Ellis v DPP(2001)***
- Ex-student of Newcastle University. Used non-open access computers to browse websites, when computer left logged on by previous users.
- Told by admin officer he did not have permission to use non open-access computers.
- Convicted under section 1 of Computer Misuse Act 1990
- The claim that what he had done was like picking up a discarded newspaper and reading it was rejected.

- How many prosecutions under Computer Misuse Act?
- 1999-2000 proceedings against 32 persons
  - 26 found guilty
  - surprisingly low number

- **8 Conclusions**
- The Computer Misuse Act 1990 was an important step in English Law, that goes some way towards protecting computer programs and data as legal property under the criminal law.
- Prevention is better than prosecution. The Audit Commission recommends several ways to improve computer security:

  More staff are being given computers to perform their tasks, but few of them receive training in terms of protecting the data they use;
- With the greater use of networks, more attention needs to be given to restricting and controlling access;
- Simple, basic controls could do much to reduce risk;
- Audit departments have a vital role to play in advising on and helping to design security measures;
- More computer-literate auditors are needed.
- A good sign is that the courts appear to be treating computer crime seriously, with custodial sentences being administered in many cases.

Summary

Computer crime is a serious (and growing) problem.

Four important areas of computer crime are fraud, software piracy, hacking and viruses.

Prior to the introduction of the Computer Misuse Act 1990, the ability of criminal law to deal with computer crime was questionable.

The Computer Misuse Act was introduced in 1990. It introduces three new offences:

- –unauthorised access to computer material
- –unauthorised access with intent to commit or facilitate further offences
- –unauthorised modification of computer material

Application of the Act has met with mixed success. The Bedworth trial is considered to be a legal anomaly that is unlikely to be repeated.

Successful examples:

- –R v Bow Street Metropolitan Stipendary Magistrate
- –Ellis vs DPP (2002)

- Fraud Act 2006: brought in a number of offences to tackle ICT fraud
  - Most offences can be committed without the completion of the relevant gain or loss actually taking place
  - If fraud is completed then a charge of theft may be appropriate

- A secure computer system is a better protection against computer crime than legislation.

- Next week:
- The Social Context of Computing

- Tomorrow: release of take home ‘exam’
- (worth 70% of module mark)