

# Spam 'n' chips - a discussion of internet crime

A.M.Marshall BSc CEng MBCS FRSA,  
Centre for Internet Computing,  
University of Hull

&

Eur. Ing. B.C.Tompsett BSc MSc CEng MBCS,  
Dept. of Computer Science,  
University of Hull

17th April 2002

## **Abstract**

The Internet presents unique challenges for investigation and enforcement. By its very nature, it encourages transparent and transient transnational activities. The volumes of data transferred across the Internet daily add to the complexity of the investigators' task, as does the unwillingness of some victims to publicise their vulnerability. As a result, the Internet is becoming increasingly dangerous and miscreants more inventive and/or subversive.

To assist investigators and enforcers alike, the authors present a draft taxonomy of computer and internet crime, identifying relationships to 'conventional' crime and highlighting likely fruitful avenues of investigation.

Typical case studies from the taxonomy are presented to identify some key problems that are encountered in the course of investigation of illicit activity involving the Internet. Potential avenues for future research and development in evidence and intelligence gathering are suggested.

## 1 Introduction

The concept of 'internet crime' is one that is discussed by many in both the law enforcement and computing worlds, but understanding of the terms used varies widely. Attempts have been made [1] in the past to provide standard glossaries of terms, but these have largely concentrated on the technical terminology used to describe attacks on the Internet and its services.

In this paper we aim to provide a broad overview of crimes involving the Internet and computers more generally. In doing this, we also aim to assist in the identification and development of techniques to assist both the investigator and the preventer of such crimes.

Our approach in preparing this information has been twofold. As technical specialists in the computing and network fields we have considered the nature of the undesirable activities that we encounter every day, and also the nature of 'conventional' crimes that can be commissioned using technological solutions.

## 2 Growth of Computer Usage & Internet Usage

With the advent of the World-Wide Web in 1991 [2] and the improvements in usability of modern computer systems provided by software such as the Macintosh OS [3] and Windows 95/NT families [4] of operating systems, we have seen a period of explosive growth in computer usage and internet connectivity. The growth patterns presented by Zakon [5] in Fig. 1 and Fig. 2 correspond closely to the growth in computer usage worldwide. Fig. 1 in particular shows how Internet usage increased after a "friendly" operating system with IP connectivity built-in became readily available on standard hardware platforms. It is worth noting that Zakon's [5] figures are somewhat conservative as he only measures the number of IP addresses registered in DNS servers. In practice, many IP addresses are re-used by different users at different times, and using address translation and proxying techniques one address may represent the entry point into a complete "hidden" network, hence the growth curve is likely to be considerably steeper than he presents.

In the context of criminal or illicit activity, Detective Chief Superintendent Len Hynds of the National High-tech Crime Unit [6] noted that

“ around 1995 [...] point and click became second nature to pretty much all of us, and with that hackers started to develop tools that each and every one of us [...] could make use of. ”

This, in itself, gives a clue to the nature of most online criminal activity, namely that the computer and the network are being used as tools, rather than as targets in their own right. This will be clarified further in the next section.

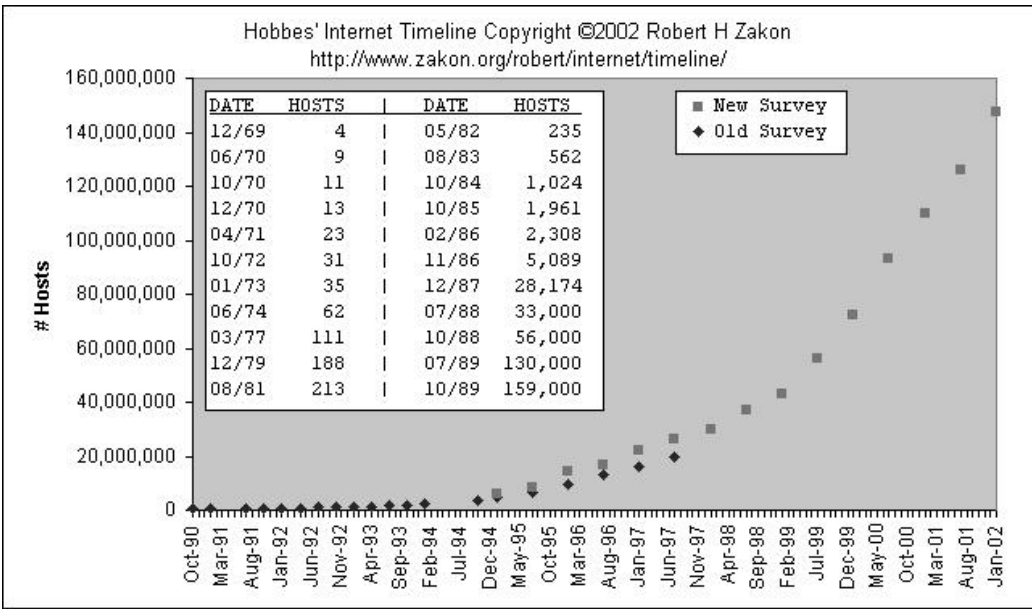


Figure 1: Growth in Internet usage (reproduced by permission)

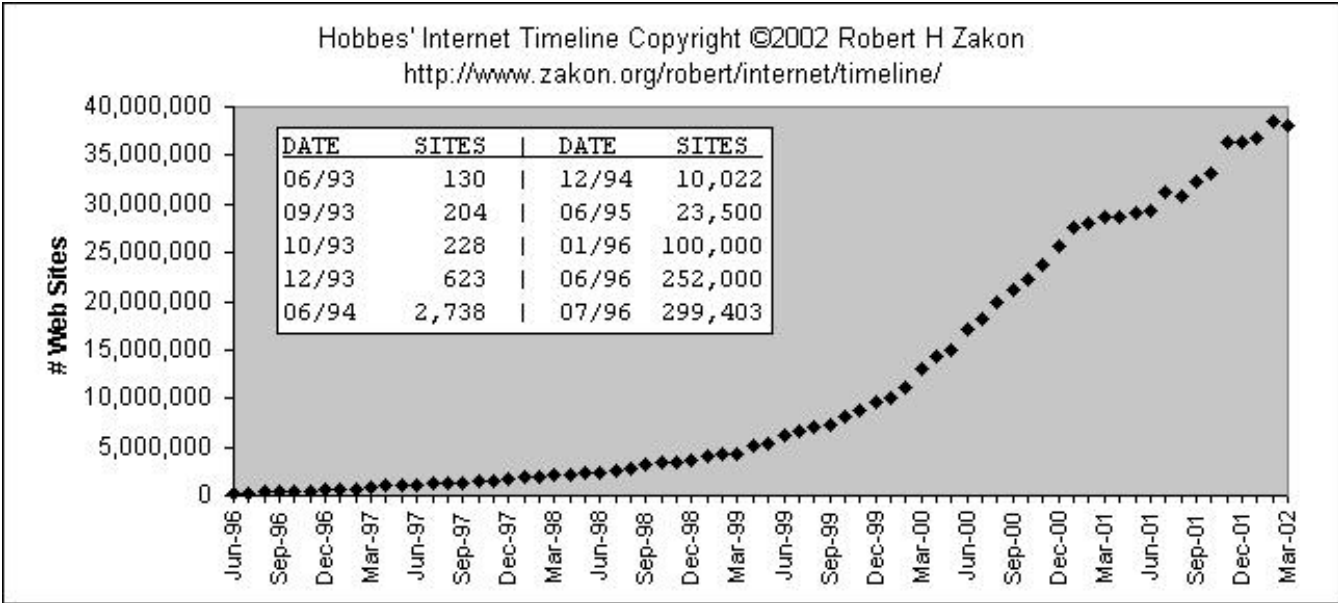


Figure 2: Growth in WWW presence (reproduced by permission)

### 3 Classification of computer & Internet crime

To provide a worthwhile classification we need to consider not only the technology used by the criminal, but also the nature of the crime being committed. As a result we propose the following six broad categories of 'cybercrime' :

**Computer Assisted** Those crimes which are easily committed using conventional means, but are equally possible using computing equipment. In this respect, they may bear some similarity to legitimate activities which are also made easier by the use of computing equipment.

**Computer Enabled** Crimes which can be committed using non-computing techniques, but are difficult to perpetrate successfully without technological support.

**Computer Only** Crimes which cannot be committed without computers being directly involved.

**Internet Assisted** Crimes which can be committed easily by conventional means, but are also possible using internet technologies.

**Internet enabled** Crimes which are difficult, but possible, to commit using conventional means, but are made easy by the application of internet technologies.

**Internet only** Crimes which require the existence of the Internet for their perpetration; for example, crimes against virtual entities. These are internet crimes perpetrated against entities which have no clear existence in the normal corporate sense, and exist only as collections of data held on Internet servers or as streams of data passing between other Internet entities.

Table 1 summarises these categories with the addition of some typical examples.

	<b>Assisted</b>	<b>Enabled</b>	<b>Only</b>
<b>Computer</b>	Blackmail	Music Piracy	Virus Propagation
<b>Internet</b>	Stalking	Money Laundering	Denial of Service
	<b>Useful Tool</b>	<b>Preferred Tool</b>	<b>Essential Tool or Target</b>

Table 1: Classification summary with examples

It will be seen, from the list above, that we have two broad categories with three sub-categories each. These subcategories arise from consideration of the "target" of the activity being attempted. In both the "assisted" and "enabled" subcategories, the target is some entity in the "real" world (e.g. goods, persons or businesses), whereas the "only" subcategory defines, as targets, services or

entities which exist or have value only within the context of a computer or internetworked environment.

Furthermore, crimes in the “assisted” and “enabled” categories are more likely to involve physical evidence which can be examined and reported using well-known established forensic techniques, and are likely to initially manifest themselves as crimes that do not obviously involve technology.

### **3.1 Non-technological crimes apparently involving technology**

In producing the classifications listed above it should be noted that we have considered only those crimes where computers and/or networks are directly involved in the commission of the crime. There are some crimes which appear to be related to computers or the Internet, but would not be classified as computer or internet crimes, as that technology has not been used to perpetrate the criminal act.

For example, if computers are stolen, either from a house, office, or in transit, that would be classified as a theft, and not a computer crime. The evidence gathered would usually be by conventional means, and it is unlikely that evidence relating to the theft would be obtainable from the computer itself.

Similarly, cases can be cited for an Internet example. A business receives a phone call from a sales agent, that indicates that a particular domain name has not been registered and that if someone registered it and put material harmful to the company on it it could damage the sales, income or reputation of that company. It is suggested if a payment is made, then this domain would be reserved for the company’s sole use and they could avoid the damage. This activity is quite common, appears to be Internet related, as it involves domain name registration, but is not. It is no different from common blackmail that was made before the Internet was invented.

## **4 Non-internet crime**

The first three categories are, in essence, crimes involving the use of ‘stand-alone’ computing equipment, typically PCs in modern cases. In these situations, evidence is relatively easy to recover as it exists and is stored locally to the device in question, or in removable media which can be traced to the culprit or equipment in question.

The 1999 ACPO principles of computer based evidence [7] apply very well to these situations as the main requirement is the recovery of evidence of activity that has occurred on the machine under investigation.

The techniques applicable to evidence in these cases are well documented by Sammes & Jenkinson [8], but can be broadly summarised as “non-invasive inspection or duplication of the contents of permanent or semi-permanent storage for the purposes of data recovery”.

Because the devices are not network-enabled or connected there is no minimal probability that unrecorded activities have been carried out, hence the investigator can be fairly confident that recovered data is complete. Of course, this takes no account of the inherent difficulties presented by the use of encryption (e.g. encrypting filesystems) [9] or steganographic [10] techniques.

#### 4.1 Case Study - Blackmail

Victim Y received anonymous letters threatening disclosure of sensitive personal information unless appropriate payment was made. Y suspected that X, who was known to hold a grudge, was the originator of the threatening letters.

In order to prove or disprove X's involvement, X's computer was seized and copied using verified imaging software. Initial inspection of the disk image thus produced revealed no visible trace of the text contained in the letters. Lower-level inspection, searching for deleted files, revealed a number of deleted documents, both complete and incomplete <sup>1</sup> which, in date order, appeared to contain drafts of the letters sent to Y. As the machine in question was known to be used only by X, and this fact was confirmed by independent witnesses, it seemed highly probable that X was the originator of the blackmail material.

Non-computing evidence, using techniques similar to those for the identification of origin of photocopies, also proved that it was highly probable that X's printer had been used to generate the letters in question.

#### 4.2 Features of non-internet crime

In all of the non-internet crime categories, the key feature is that the device in use is effectively a stand-alone system and hence the locality of offence is obvious. Any illicit activity is covered by the legal system in operation in the geographical location of the computer.

Although removable peripherals, removable media or even hand-held computers may be used in conjunction with it, the majority of data storage, generation and processing occurs within a single computing system <sup>2</sup>. As a result, all evidence originates from this system and, as a result of the use of temporary files, swap files [11], "auto-saving" and other common features of modern application and operating system software, copies of evidence are likely to exist somewhere within the (semi-)permanent storage devices associated with the system.

Thus the techniques required by ACPO [7] and described by Sammes & Jenkinson [8] remain valid, regardless of advancing technology. The primary problem that arises, when applying these techniques to advanced systems, lies with the volume of data to be analysed. Large storage devices, encrypted or steganographically hidden information take time to analyse. There is a real risk that the examiner may miss data which contradicts the evidence found so

---

<sup>1</sup>incomplete documents were not fully recovered as they had been partially overwritten by later files

<sup>2</sup>for the purposes of this discussion the system is taken to include all removable devices

far, and which could affect the outcome of any proceedings taken against the suspect.

However, as long as the correct procedures have been followed and the images are preserved intact, the possibility of performing a complete, albeit time consuming and expensive, analysis or even of re-visiting the evidence remains.

## **5 Internet crime**

Broadly, internet crimes are those which involve the use of the Internet to commission crime, or directly affect the performance of some service on the Internet. Recent analysis of illicit activity suggests that the majority of internet crimes fall into either the assisted or enabled categories.

### **5.1 Internet assisted and Internet enabled crime**

It is now generally accepted that the Internet, as we know it today, is primarily another channel for the delivery of services, or another means of communicating with customers, colleagues, friends, family etc. The main advantages of the Internet over other channels are the relatively low cost, the ability to cross national boundaries with ease and the ability to communicate with huge numbers of the world's population in a very short timescale.

As a result, it has become a necessity for any business to use the Internet effectively. Unfortunately, not all "businesses" using the Internet are completely honest and the dishonest members of the Internet community have been quick to discover and invent new ways of using the technology to re-engineer some very well known old-fashioned criminal activities.

#### **5.1.1 Case Study: Internet Assisted Crime.**

Web pages are static information files held on computer and provided to readers with the assistance of the Internet, but such pages were readily provided to readers on disks and CD (such as in the case of electronic manuals and catalogues) long before the Internet was in common use.

There are many documented [12] cases where an outside party has used the Internet to gain access to the computer holding the pages and made changes to those files.

This is only an Internet Assisted Crime, as the pages could still have been changed at the computer itself, and the Internet only enabled the perpetrator to remain remote from that location.

#### **5.1.2 Case Study: Internet Enabled Crime.**

The Internet has enabled new forms of money laundering that could not easily be achieved by other means, and work around many money laundering regulations. One scheme involves the creation of franchised adult oriented web sites. A

provider of adult material, who may or may not be legitimate, wishes to reach a wider audience, and hence greater sales for the material.

A franchising scheme is created whereby the content of the site is licensed for a fee for others (affiliates) to hold on their own web sites, and any referers the affiliate makes to the franchisee earn a commission. The attraction to the affiliate is that they could have a business with only a small outlay that could be earned back in commission, and eventually make a profit selling someone else's material.

The attraction for the money launderer is that the original payment could be made with "dirty money", often a stolen credit card. The commission comes back in the form of clean money. The Internet, however, enables the criminal to go one step further, in that all purchases, and all traffic generated are made automatically by a computer program. It is possible, through the use of relatively simple software, to generate many millions of synthetic "readers" to a web page, all of whom appear to be from different locations, or make many small purchases from a store, all with stolen card numbers that were themselves stolen from Internet locations.

## 5.2 Internet Only Crime

The concept of Internet Only Crime is difficult to define because of difficulties in identifying what constitutes a crime on the Internet. Broadly, we consider an Internet Only Crime to be an activity which is intended to directly affect some service or entity which only exists or has value in an internetworked environment. Experience suggests that this an acceptable definition in use by most network administrators worldwide, although personal views tend to focus more on the local network than the global.

As a result of this broad definition a form of "frontier law" has sprung up around the Internet whereby "Acceptable Use Policy" and "Terms of Service" documents are used to try to control activities on the Internet.

This is for two main reasons. Firstly, legislation lags technology. Hence legal definitions of crime are not appropriate to current and/or future technology. Secondly, and perhaps more importantly, the locality of offence problem makes it difficult to determine which definition of crime should be applied to internet transactions in general. This also applies to Internet Enabled and Internet Assisted crimes, though to a lesser degree as they will involve some "real world" entity as a target.

### 5.2.1 The "Locality of Offence" problem

There is often great difficulty in determining whether or not a crime has taken place in an internetworked environment, not least because of the problem of locality of offence.

Legal systems are, on the whole, tied to national or state boundaries and hence something that is perceived as a crime in one geographical location may not be considered a crime in another. Even if there is a trans-national agreement

on what constitutes a crime, there remains the problem of determining where the crime has been perpetrated.

When an Internet user is the victim of an Internet-based criminal activity while using their own computer at home, but connecting through a local Internet Service Provider to the “backbone” of the Internet and thence via another Internet Service Provider to a server providing information and services in another country, where has the offence taken place ?

It could be argued that the offence takes place at the server as this is where the information supplied by the user to enable the crime is acted upon. It could equally be argued that the offence takes place in the user’s location as this is where the information is being extracted from them.

Currently, there is no simple answer.

As a result, there is often no way of identifying whether or not a crime really has been committed, within the strictly legal sense, as it can be impossible to determine which legal system has jurisdiction over the transaction taking place, and hence whose national definition of a “crime” should be used.

## **6 Intelligence aspects**

### **6.1 Intelligence**

Intelligence can be considered as extracting information from entities involved with a crime that may provide pointers to the perpetrators, and relating that information to other information held in store to form larger patterns of information.

Shimeall and Dunlevy [13], in considering threats to networked systems state that

“Intelligence analysis requires many of the same analytical methods and techniques, irrespective of domain. From this perspective, intelligence analysis for Internet security is no different from the intelligence task in any other area of national and international security. The purpose of intelligence, irrespective of domain, is to guide action. Intelligence may identify the need for action. Once the need is established, it may provide the insight and context for deciding among courses of action. Finally, during and following the action, it may provide information on the effectiveness of pursuing the selected course of action.”

Hence, information that is useful in an internet related crime, could often be the same as collected for other investigations, such as names, telephone numbers, and so on.

### **6.2 Internet Intelligence**

In the context of criminal intelligence, we need to consider the Internet from two different perspectives. Firstly as a source of information which can be used by

investigators dealing with all crimes and secondly as a generator of information which can be used by investigators of internet related crimes.

### **6.2.1 The Internet as information source**

As mentioned previously, the Internet has become a primary communications channel for many businesses and individuals. As a result, considerable quantities of information are now relatively easy to locate using search engines etc.

The Internet is a rich resource for information searching and collation, and can greatly assist in the intelligence gathering for Internet related activities. Some simple and basic resources are online telephone directories, and resident listings, as well as other forms of public documents.

### **6.2.2 The Internet as information generator**

Because the Internet is a collection of smaller networks joined together by inter-networking devices (e.g. routers) effectively sharing a common “backbone” and cooperating to deliver traffic to its destination, each and every piece of information travelling on the Internet carries with it information about the source and destination, and frequently the intermediate devices used to transfer it from one to the other.

Thus, in an Internet specific activity we should also be able to gain intelligence from email addresses, domain names, and Internet, or IP addresses. Hence, the Internet can act as the source of much of the information required during an investigation.

### **6.2.3 Information gathering challenge**

The collection of evidence from a stand-alone computer is now a well documented procedure. The collection of information that could lead to evidence or intelligence from an Internet connected computer is less straight forward. Data relating to Internet related crimes, or for general intelligence gathering that may lead to the detection of such crimes may be gathered from a computer suspected of being involved in the crime, or from any Internet connected computer.

The data that is required is either a computer host name, or a Web Page address (or URL) or an email address, or IP address. These often need collecting in conjunction with timestamps, so the information can be correlated with other evidence from other locations. For these timestamps to be useful the real time clock on the computer needs to be accurate and the resolution often needs to be greater than a second. The timezone used is also valuable in time coordination.

Many of these information points exist in a computer transiently, so must be collected in an orderly manner as soon as possible. For example, some of the information sources are tables in the memory of the computer that only have a lifetime of ten minutes. If the delay in collecting the information is longer than ten minutes, or the computer is switched off, then some information would not be found. The kind of information that can be collected from an Internet active

computer are such things as a list of IP addresses recently used, or copies of web pages recently visited. The computer also records its network configuration, such as the addresses of the network servers it uses. If similar information can be collected from these servers then a more complete picture of activity can be built up.

The interesting thing about information gathering regarding Internet connected computers is, sometimes, much of it is available at many locations on the network distant from the perpetrator of a crime. Most servers and significant network nodes record, in log files, the requests and traffic addresses, and these, when combined, can form a picture of Internet traffic activity.

### **6.3 Case study: Web defacement**

Consider the following case study, regarding successful attempts to compromise an Internet information server. A web server operator discovers that pages on a web server have been altered. If the alteration is discovered within a few minutes of the change being made then useful information about the origin of the attack can be obtained from the tables contained in the memory of the server, such as the IP address of the perpetrator. If the server is disconnected from the network and powered down, much of that contemporaneous information is lost.

Even without the detailed information from the server itself much can be garnered from other systems in the same network area as the compromised server. It is usually the case that many systems have been scanned prior to a successful intrusion, and contain partial information which, when combined, can form a picture. If the logs from the different systems are examined (which would need to be done mechanically rather than manually as they might contain many millions of data items) and regular traffic is excluded, then patterns of unusual traffic can be shown. From these a collection of IP addresses or host names can be obtained. These addresses can then be used to start a search using the many data sources available on the Internet which describe the Internet itself.

#### **6.3.1 Information available**

There are many such Internet related public documents, such as the registration data for Internet addresses and the databases mapping domain names to IP addresses. In addition to these, perhaps the most useful in Internet related investigations are the databases of those hosts that log scans of their own network's intrusion events and make their logs available for public perusal. A particularly good example of such a service is <http://www.incidents.org/> operated by the SANS institute.

There are also databases of sites that are known to originate improper traffic, and sites that appear to be unmanaged or improperly managed. As these Internet locations attract those that might perpetrate such attacks these databases assist in profiling the attack origin, as do databases of known compromised or unsecured systems.

In the web defacement example described above, it was discovered that the system attacked was infected with the Nimda [14] virus, and the Nimda infection attempt can be detected from the logs of many systems on the same network as the victim computer. The logs also showed a later scan for Nimda compromised systems. Shortly after this scan, the attacker performed the web page change.

The two IP addresses (for the initial infection and the later exploitation) can be used to gather information from the network databases. In this case, as in most, the infection came from a well managed network (by consulting the IP registration data, and lists of networks that respond to complaints) and the infection agent was, most likely, also a victim of Nimda and in need of assistance.

However, the exploiter is often found to have penetrated the network through an address on an unmanaged network or through a known insecure system in an attempt to cover their tracks. In these cases considerably more effort is required to track the perpetrator and take appropriate action against them.

## 7 Conclusion

In considering the topic of cybercrime it is important to consider the nature of the “crime” being perpetrated and, perhaps most importantly, the target victim of the crime. This will assist the investigator in identifying appropriate channels of investigation. The draft classifications presented above may assist in this.

Where the activity under investigation involves significant use of the Internet, the continued and persistent use of large datasets and intelligence gathering, can reveal much about the identity and origin of the culprit(s). Matching of the use of IP addresses and host names from various datasets over time often leads to web pages that contain further details of the suspect, their activities and their contacts.

By collaborating effectively to share information about suspect activities it should be possible to detect such events as virus propagation before they have become the sort of global problem exemplified by Nimda.

## 8 Future trends

The volume of data that requires processing as part of intelligence gathering in the investigation of Internet related activities gets larger and larger, but the public donations of information to assist in that information also get more organised. For example, on a new computer set up on our network for the investigation of the frequency of these intrusion attempts, we are measuring about 10,000 intrusion attempts per annum. If each one of these succeeds on some computer somewhere, then that is a large amount of intrusion activity that underlies a large amount of computer crime.

In order for this information to be collated and analysed efficiently and effectively there is a clear need for new automated intelligence agents to assist the human investigator.

## References

- [1] Howard, J.D. and Longstaff, T.A. A Common Language for Computer Security Incidents. Sandia National Laboratories, USA, 1998
- [2] Berners-Lee, T. The World Wide Web: a very short personal history. (URL:<http://www.w3.org/People/Berners-Lee/ShortHistory.html> Last viewed: 11th April 2002)
- [3] apple-history.com (URL: <http://www.apple-history.com/h3.html> Last modified: 6th February 2002 Last viewed: 11th April 2002)
- [4] Zachary, G.P. Show-Stopper! The breakneck race to create Windows NT and the Next Generation at Microsoft. Little, Brown and Company. London. 1994
- [5] Zakon, R.H. Hobbes' Internet Timeline (URL: <http://www.zakon.org/robert/internet/timeline/> Last updated: 1st April 2002. Last viewed: 9th April 2002)
- [6] Hynds, L. Hacker Cracker. RSA 2001 (URL: <http://www.rsa.org.uk/acrobat/len.hynds.pdf> Last viewed: 9th April 2002)
- [7] Association of Chief Police Officers of England, Wales and Northern Ireland. Good Practice Guide for Computer Based Evidence, Version 2. ACPO Crime Committee, 23 June 1999.
- [8] Sammes, T and Jenkinson, B. Forensic Computing - A Practitioner's Guide. Springer-Verlag, 2000.
- [9] Bindel, D. Cryptographic file systems. (URL: <http://www.cs.berkeley.edu/~dbindel/oceanstore/fs.html> Last viewed: April 12th 2002)
- [10] Johnson, N.F. and Jajodia, S. Steganography: Seeing the unseen. IEEE Computer, February 1998: 26-34 (also at URL: <http://www.jitc.com/pub/r2026.pdf> Last viewed: April 12th 2002)
- [11] Stallings, W. Operating Systems. Prentice-Hall, 1995: 286-344.
- [12] Attrition.org, Defaced Commentary Mail List Archive, (URL: <http://www.attrition.org/security/commentary/> Last viewed: 8th April 2002)
- [13] Shimeall, T.J., and Dunlevy, C. What to Expect of Network Intelligence Analysis. in Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. IEEE June 2001

(also at URL: <http://www.cert.org/archive/html/spie.html> Last viewed:  
17th April 2002)

- [14] CERT/CC, CERT Advisory CA-2001-26 Nimda Worm.  
(URL:<http://www.cert.org/advisories/CA-2001-26.html> Last updated:  
25th September 2001. Last viewed 14th April 2002)

## Glossary

Terms defined herein are summaries only.

**auto-saving** - a technique used by some programs to ensure that the user's work will not be lost if there is a power failure. Periodically, the program will, without human intervention, save the current contents of its workspace into a file on the disk.

**DNS** - Domain Name Service or System. The worldwide network of databases that provide the mapping from human readable machine names to machine usable IP addresses.

**internet** - any computer network constructed by joining two or more networks together.

**Internet (the)** - the commonly used global network of networks using IP suite protocols to allow nodes and users to communicate.

**IP** Internet Protocol - the format used to package information for transmission on the internet. Packaging includes the IP addresses of the source and destination machines.

**IP address** Internet Protocol Address - a 4 byte number usually written in the form aaa.bbb.ccc.ddd which uniquely identifies a node within an IP network.

**log** - (also server log) A file of information about activity which is written by the program supporting that activity. Typical examples include session/server logs which record resources being accessed and details of the node accessing those resources.

**node** - an entity on the network which can originate, consume or pass-through IP traffic.

**protocol** - an agreed standard format for communication between nodes and/or programs.

**router** - node which connects two or more networks together. When information needs to flow from one network to another, the router performs the transfer.

**search engine** - an internet service, typically provided via a web interface, which allows users to search through databases of information about other services and resources.

**snail mail** - ordinary postal mail.

**spam** - Common term for UCE and similarly unwanted e-mail. Originates from a Monty Python sketch involving a large number of Vikings in a cafe where everything on the menu contains spam.

**steganography** - a techniques for hiding information by embedding it other information. Literally “shadow writing”. Can be used to hide, for example, a word processor file inside a graphics file. Without detailed inspection of the graphics file’s contents, the word processed document may not be found.

**UCE** - Unsolicited Commercial E-mail. The internet equivalent of “junk mail”. The main difference is that, unlike snail mail, the sender pays very little to originate the UCE, but the senders may have to pay to receive it.

**URL** - Uniform Resource Locator. An internet standard format for specifying the protocol, location and name of a resource. (e.g. <http://www.cic.hull.ac.uk/commercial.shtml>)

**virus** - In computer terms any program which is capable of reproducing itself and distributing itself to other computers without voluntary human intervention. Not all viruses are destructive, but all consume resources in some way.

**web server** - a node specifically providing services associated with the World Wide Web and its related protocols.