Future-proofing the Computer Misuse Act

Submission to the APIG Public Enquiry on Revision of the Computer Misuse Act 1990

Introduction

The Computer Misuse Act 1990 (the Act) was conceived and implemented before the explosion of interconnectivity engendered by popular and business access to the Internet. Inevitably, threats to computer systems have since emerged which were impossible to anticipate, and which are consequently are not well covered by the provisions of the Act. Revision of the Act is necessary (indeed, probably overdue) in the light of the emergence such network oriented threats.

In amending the Act, it might superficially seem tempting to explicitly address specific current technical threats (e.g. Trojan horses, viruses) in order to simplify the processes of legislating, and the recognition and prosecution of offences. However, the pattern of technical threats is continuously evolving, so such an approach would soon return us to the current position, in which quite specific definitions within the Act no longer cover the requisite ground. We therefore need generic amendments that will remain effective in the face of future change. Amendments should nevertheless be kept to a minimum, and should wherever possible extend rather than supplant the existing provisions of the Act. This is important to avoid the need to re-establish a substantial body of precedent. Precedent is expensive and hard won, and it takes time to create, during which there is much uncertainty as to interpretation, resulting in confusion and failure of prosecutions. The author believes that the basic framework of the 1990 Act is still viable, but offers here some suggested revisions that fulfil these conditions.

Definition of Computer

Although the term computer is not explicitly defined in the 1990 Act, COM(2002) 173[1] provides one which accords with current precedent. However, it is a somewhat limited definition for the modern context. The author suggests that this definition be combined with the COM(2002) 173 definition of "Electronic communications network" to create a new definition that encompasses any equipment that processes, distributes or transmits computer data as defined in COM(2002) 173. Recent threat reports show the urgent need for this.[2,3]

Any definition should be included, or available elsewhere and explicitly referred to, in any revision of the Act.

Misuse and Offences

At first sight, the sheer range of alternative ways to misuse modern networked computer systems seems daunting, including as it does "hacking", local and remote data misuse, direct and indirect resource misuse, viruses, worms, Trojan horses, denial of service, spyware, spoofing *et al* in all their multifarious incarnations. However, if we categorise these abuses in terms of their fundamentals we find that they break down into six generic categories:

[1] obtaining unauthorised read access to systems and their resources (the ability to browse and inspect data);

[2] copying, modifying or destroying data (including configuration data) without authorisation;

[3] storing data without authorisation (including program code and configuration data);

[4] executing programs without authorisation (including changing without authorisation the run-time execution flow of any running process, even if authorised in principle to execute the unmodified process);

[5] denying authorised users access to services and resources for which they are authorised (denying service), even if the party denying service is authorised to use the services and the processes employed to deny service in a manner that would not deny service.

[6] without the authorisation of the recipient, falsifying or suppressing information identifying the source of transactions.

The author proposes that these broad technology-neutral categories, and not the specifics of individual current technical threats, are what should be addressed by legislation. On this basis, categories [1]

[1] COM(2002) 173 final: Proposal for a Council Framework Decision on attacks against information systems

[2] e.g. Session Initiation Protocol vulnerabilities: ICAT CAN-2003-0761, CAN-2002-0671, CVE-1999-0938

[3] Saran C. 'Exploiter' hack program targets Cisco networks. Computer Weekly 06/04/2004, p 4.

through [4] appear to be covered adequately by the existing Act, with the exception of the suggested explicit reference to run-time execution flow as in [4].

Denial of Service

The Computer Misuse (Amendment) Bill[4] attempts to cover [5] Denial of Service. It does indeed address denial of service caused by triggering of system "crashes", but it fails to address the increasingly common class of transient denials of service that result from abuse of legitimate mechanisms to consume bandwidth and processing resources without jeopardising the fundamental operation or integrity of computer systems.

The classic transient denial of service against, for example, a public-facing web server is caused by sending large numbers of transaction requests at high speed and then failing to complete the resulting transactions, filling the transaction queue on the server and causing it to ignore subsequent transaction requests until the incomplete transactions time out and are cleared from the queue. As the web server is public-facing, any member of the public is implicitly authorised to access it in order to view the web pages it hosts. However, although high speed initiation of a large number of ultimately completed transactions could be considered a legitimate if unusual activity, initiating transactions with the intent not to complete them is clearly not a legitimate activity. An interesting variant example abused a routing protocol, causing the Internet core routers to deny service to a victim[5]. This is a two-stage process, whereby the perpetrator initiates illicit transactions using forged credentials with an innocent third party's equipment, which responds in a legitimate manner and in so doing unwittingly denies service to the authorised users of a victim's computer system. We need to ensure that the initiator of all such processes commits an offence. Fortunately, in most cases to perform these attacks transaction protocols must be breached in some recognisable manner which is visible in the transaction data.

To cover denial of service broadly without tying ourselves to specific technological implementations, we should define an offence in terms of maliciously or recklessly attempting to access a computer system with the intent of denying, or in a manner which has the effect of denying, authorised access by others to services or resources (irrespective of whether the attempt to access the computer system would be an authorised access in the absence of the intent or effect of denying service, and, in the case of intent, irrespective of whether services or resources are in fact denied to others by the attempt). The prima facie evidence could be derived from transaction logs.

Other Matters

The author suggests two new offences to serve as supplementary bases for prosecution:

[a] unauthorised use of computer processing capacity or network bandwidth resources. This would also help to control the growth in direct abuse of wireless networks.

[b] without the authorisation of the recipient, falsifying or suppressing information identifying the source of a transaction.

Finally, the author concurs with the Internet Crime Forum that all offences under an amended Act should be extraditable.

08 April 2004
Mike Barwise BSc, CEng, MBCS, MIIE
Computer Security Awareness
[REDACTED]

[4] Computer Misuse (Amendment) Bill (HL) , 2002 79

[5] Gibson S. 2002. Distributed Reflection Denial of Service. http://grc.com/dos/drdos.htm