



Association for Payment Clearing Services

Mercury House, Triton Court
14 Finsbury Square
London
EC2A 1LQ

Telephone 020 7711 6200
Facsimile 020 7256 5527
www.apacs.org.uk

Note to: All Party Internet Group Secretariat
23 Palace Street
London
SW1E 5HW

Direct line 020 7711 6317
Direct facsimile 020 7711 6299
Email Colin.Whittaker@apacs.org.uk

Our Reference SAG296

From: C Whittaker
Head of Security, Standards & Security

6 April 2004

APIG REVIEW OF THE COMPUTER MISUSE ACT (CMA)

The Association for Payment Clearing Services (APACS) is pleased to present its written evidence to the All Party Internet Group's public inquiry into the desirability of revising the Computer Misuse Act 1990 (CMA). APACS is the UK trade association for payments. It is also the banking industry voice on payments issues such as plastic cards, card fraud, cheques and electronic payments. It provides a forum for banks to come together on non-competitive issues to bring about change and to develop banking systems for the future. APACS was established in 1985 as a non-statutory association of major banks and building societies. APACS supplies scheme and project management, business consultancy and secretariat services to the UK payments industry. It works with the UK's leading banks and building societies to provide innovation and developments in payment processing.

The UK banking and payments industry has always been a strong supporter of the CMA. We believe that it is has been an important piece of legislation to place on the statutes, and increasingly so as computer based systems come to underpin ever more of our day-to-day activities. In general terms the CMA remains fundamentally sound, and the language and definitions are appropriate to cover the majority of technological developments. There are, however, four areas where we believe that the CMA could be enhanced to provide a better basis under law to prosecute potential offenders:

- Denial of Service (DOS) Attacks – These represent an increasing threat to modern networked computer systems, and when an enterprise suffers a DOS attack it can expend significant effort in time and resources to combat it. This is exemplified by the recent DOS attacks against the on-line gaming industry by what is believed to be Organised Crime. It is important to recognise that there are only limited technical measures that can be made to mitigate the threats of these attacks, and therefore effective legal action against the perpetrators of such attacks may be the only recourse for an enterprise. The industry continues to be an advocate for the amendment of the CMA to make DOS attacks illegal.

- Use of Deception to obtain Security Credentials – Computer users throughout the world have been subjected to a barrage of “phishing” attacks over the last 18 months. These attacks have attempted to deceive computer users into divulging their internet identities and passwords for a wide variety of internet based services. Although the use of these credentials to steal money from an on-line bank account would constitute a crime, there is a strong case to be made for the use of tools and techniques to deceive computer users to obtain such credentials, or the possession of such credentials, itself to be a criminal offence. Given that many security tools and techniques are dual-use, in that they can be used by system and security administrators to manage systems as well as maliciously by criminals, it is perhaps more prudent to concentrate legal sanction on the results of using these tools. In which case there may be merit in considering making it a criminal offence to be in the possession of a person’s security credentials, and in doing so reverse the burden of proof, as is the case with offensive weapons and knives – the onus could be placed upon the suspect to prove why they legitimately have in their possession a person’s security credentials.
- Unauthorised use of Computer Resources – The main thrust of the CMA, and in the wider considerations of computer crime, has been the need to prosecute people who gain unauthorised access to computer systems in the process of which the confidentiality, integrity or authenticity of information is compromised. The addition of denial of service as an offence under the CMA would add to this the compromise of availability. It is not clear, however, how one might use the CMA to prosecute a person who used unauthorised access, or authorised access in breach of policies, to store their own material on another persons system. Clearly where the material was offensive or illegal other offences may have occurred; in the latter case the introduction of “zombies” or “Bots” to execute DOS attacks, or distribute spam, might be considered crimes under the revision of this act. There is increasing evidence that people are inappropriately using other people’s computer resources to store their digital material upon, and consequently consideration may be given to the concept of virtual trespass under this act.
- Defrauding a Machine – The Theft Act 1978, as amended by the Theft (Amendment) Act 1996, describes “obtaining services by deception” in terms of what one person may do to another. There is clear case law precedence that asserts that this does not apply where a person is believed to have deceived a machine to provide services. We would argue that, with the ever-increasing use of microprocessors and computer-based systems at the point of service to individuals there is a need to amend this legislation. Alternatively one could equally argue that this could constitute some form of offence against the CMA, or one which may need to be enshrined in the CMA, perhaps in the context of misuse of security credentials of whatever form.

Irrespective of the language or content of the CMA the concerns on whether it has been effective or not, and whether it has helped to deter such offences should be best considered in the light of its record. Here it is possible to argue that there are three reasons why the CMA has been less effective than it was expected to be. Firstly there have been difficulties in how such cases have been presented in court and prosecuted.

Secondly one could reasonably question the ability of the judiciary to sufficiently understand the technology to which the CMA applies in order to be able to provide reasonable interpretations or guidance to the jury. Finally it is difficult to see in cases brought under the CMA how jurors who do not understand computer science can understand the evidence they are presented with; this is a similar issue to that found in presenting complex fraud cases to juries.

Consequently what ever measures are taken to reinforce the strength, applicability and durability of the CMA, as we move to an ever more technically sophisticated world, equal effort needs to be given to determine whether the legal processes are sufficiently mature to try cases brought under the act. Here there may need to be a much broader debate on whether cases under the CMA should be considered in the same light as that which has recently been given to fraud cases.

Moreover only by examining this wider context can one form a view on the level of severity of the penalties under the CMA. From a narrow banking and payments industry perspective the level of losses or damage that may be suffered from an attack, that may be an offence under the CMA, far outweigh the potential penalties that may be inflicted on the perpetrator, and therefore the deterrence effect is at best marginal. Examining the broader context in which computer based systems are used in society and the potential consequences of their compromise reinforces this view and the need to develop more robust sentencing guidelines.

One cannot ignore the international dimension of offences against this act and the need to harmonise and coordinate international legislation in this area. Here the work of the EU and the G8 groupings are very valuable and the UK should play an important and leading role in this process. Not only because of the importance of being able to prosecute offenders in any jurisdiction, but also because of the lessons learnt in formulating our own legislation and the innovative way in which our own legislation allows offenders to be prosecuted against the CMA no matter where the computer attacked was geographically located.

In summary we would fully support a constructive review of the CMA, with the goal of reinforcing its applicability to the modern application of computer systems, harmonising it with other legislation and a review of the penalties that can be applied in relation to the potential consequences of compromises to computer systems.

-oooOooo-