Two Recent Computer Misuse Cases

Computers & Law
16/5 January 2006

Peter Sommer

Two recent computer misuse cases with differing but "counter-intuitive" outcomes show, among other things, that the courts are not prepared creatively to reinterpret the 1990 Computer Misuse Act in the light of changing technological circumstances.

It's worth examining both cases in some detail.

In October 2005 Dan Cuthbert, a system penetration and software-tester contracted by ABN Ambro Bank, was convicted of unauthorised access to the Tsumani charity website run by the Disasters Emergency Committee (DEC). The facility that collected the donation was in fact run by British Telecom. The previous New Year's Eve, Cuthbert was working at ABN Ambro and running several simultaneous tests, operating from multiple browser windows on his Apple Powerbook. (The Apple Powerbook is a favourite among City-based penetration testers because, beyond its Aqua interface it is in fact a BSD Unix machine and it is extremely easy to adapt the multitude of existing Unix pen-testing, ethical hacking and other programs to work on it).

He had visited the site, donated £30, but had become concerned at its slow response and what he had regarded as poor graphics. There had been extensive press coverage of "phishing" attempts and a number of these had involved fake sites masquerading as well-known UK financial institutions. His concern was that he had just provided details of his name, address and credit card and that these might be abused. Cuthbert sought to test the site by using a directory traversal test – in effect he re-formed the URL he could see in the command bar of his Internet browser to see whether the security settings on the remote website would allow him access beyond the web root. His attempt was rejected, he felt relieved and thought no more of the matter.

But the test set off an alarm in an intrusion detection system (IDS) installed by British Telecom, the directory traversal being an obvious alerting signature. It wasn't difficult to trace him – he had just supplied his name, address and credit card details, and his IP address, which resolved to his employer, was captured both by the regular web-logs of the donation website and by the IDS. Cuthbert's subsequent interview with the Metropolitan Police Computer Crime Unit went badly. He says that he was panicked by the situation but instead of producing an accurate and straightforward account of events he sought to suggest that the activity was caused by the action of a proxy server which had been part of the ABN Ambro testing environment. The police investigator, who had formerly been seconded to NHTCU and had a MSc from Westminster University, probed further and Cuthbert then gave a more accurate account of events.

It was this initial lack of candour which partially influenced the CPS decision to prosecute – concern about potential loss of public confidence in the charity website

leading to a drop in donations may have been another. Cuthbert's lack of candour was also later remarked on by the District Judge.

At trial his defence team argued his intentions were obviously benign. The substantive evidence available consisted of the web-logs from the donation web-site and the activity logs from ABN Ambro. These both showed in significant detail what had happened on New Year's Eve 2004 – visits to various news websites dealing with the Tsunami disaster followed by the donation, followed by the attempted directory traversal. It was also possible to demonstrate that this was the totality of the relevant events; there were no other "attacks" on the DEC web facilities, no attempted frauds and no attempts at concealment. A certain amount of information was also obtained from a forensic examination of Cuthbert's Apple Powerbook, but the Internet browser cache only had a "life" of 7 days so that only deleted fragments remained. But it was possible to see how the Apple had been configured and to remark on the computer programs that had been installed on it. The defence were able to say that as a pen-tester Cuthbert possessed skills and tools to cause large-scale disruption without being detected – which he plainly had not used. The court was invited to draw conclusions.

But the prosecution said that Cuthbert must have known the directory traversal was unauthorised. It was this interpretation the court accepted; in effect, overall intent was irrelevant, there were no circumstances in which there was consent for directory traversal .

Cuthbert's case continues to be debated within the community of pen-testers. Some are alarmed that the decision potentially affects some of their techniques. Others point out that pen-testing should only ever be carried out against a highly specific set of consents; they also say that directory traversal is not the best or most obvious technical test for "phishing". (Better tests consist of *netstat* to establish the IP address of a suspect site, *whois* to discover who owns the site, plus a certificate verification of any supposedly "secure" site).

The following month a youth [subsequently identified as David Lennon] walked free from a Wimbledon court having admitted that he had used the mail-bomber program Avalanche to flood the mail server of an insurance company called Domestic and General from which he had been fired. Over 5 million emails were generated. By coincidence the same Met CCU officer and defence expert from the Cuthbert case found themselves professionally involved. The youth's defence was purely legal: it was said each email sent to an email server is "authorised" to modify it (otherwise email wouldn't work) and there is no specific point at which a large quantity of such emails suddenly become "unauthorised". All the emails sent were RFC compliant. A technical description of the operation of email was provided for the court.

The Prosecution cited *Yarimaka v Governor of HM Prison Brixton : Zezev v Government of the United States of America* (2002). This was an extradition case arising from an attempt to extort $200,000 from Michael Bloomberg by hacking into the business computer system that bears his name and then showing how it was done. One of the arguments advanced on behalf of the defendants was that causing a

computer to record the arrival of information that did not come from the source it purported to come from (in effect by providing misleading data) was not conduct affecting the reliability of the data for the purposes of s 3 Computer Misuse Act. The Court of Appeal rejected this interpretation.

The actions of the Wimbledon youth, which had included sending emails in the apparent names of Domestic and General staff, was, the Prosecution contended, very similar to those of Yarimaka and Zezev. The District Judge at Wimbledon mentioned the case in his written judgement but did not follow it.

Just as in the Cuthbert case where the judge declined defence invitations to look at the wider context of his actual motivation and the not the strict wording of the Act, so in the Wimbledon case prosecution pleas that the court should consider the obvious malign intent and damage caused were unsuccessful. Both judges felt it was not their job, but Parliament's, to extend the law. In both cases extensive arguments were made about the history of the Computer Misuse Act and the associated Law Commission reports and that the reasoning behind it reflected late-1980s perceptions about how computers might be attacked.

There were possible alternate prosecution routes: via s 43(1) Telecommunications Act 1984 (now s 127(2) Communications Act, 2003) which covers the persistent use of public telecommunications system for the purpose of causing annoyance, inconvenience or needless anxiety to another. This apparently ran out of time. Another approach could have been via the Protection from Harassment Act 1997 but it may be that this would require evidence of repeated acts of harassment.

At the time of writing it is not known if the CPS will appeal the Wimbledon decision.

The next legislative activity to introduce a will be in March 2006 when Tom Harris MP will reintroduce a 10-minute rule bill which arises out of the earlier work of the Parliamentary All Party Internet Group http://www.apig.org.uk/archive/activities-2004/computer-misuse-inquiry/CMAReportFinalVersion1.pdf) and of Derek Wyatt MP.

Indeed there is little need for a separate Computer Misuse (Amendment) Bill as the relevant clauses, could easily be incorporated into one of the regular Criminal Justice bills. A specific "denial of service" offence would provide additional armoury for police and prosecutors, removing any doubts about the scope of the existing s 3, and would also ensure that UK legislation complies with the Council of Europe Cybercrime Treaty, Article 5 of which deals with "System Interference".

Peter Sommer is Senior Research Fellow in the Information Systems Integrity Group at the London School of Economics and a frequent expert witness in criminal and civil matters. He is the author of the "Directors and Corporate Advisors' Guide to Digital Evidence" published by the Information Assurance Advisory Council (http://www.iaac.org.uk/Portals/0/Evidence%20of%20Cyber-Crime%20v08.pdf). He is the Joint Lead Assessor for the Digital Evidence speciality at the Council for the

Registration of Forensic Practitioners. He was instructed by Saunsbury & Co in the Cuthbert case and by Tuckers in the Wimbledon case.

Note: the CPS did successfully appeal the Lennon decision: DPP v Lennon [2006] EWHC 1201 (Admin)