This document was written in the Autumn of 2005 at the request of the Legal Subgroup of the Internet Crime Forum in order to better inform the discussion about the issues that arose when considering how to criminalise denial of service attacks on the Internet.

Representatives of the Home Office participate in the Legal subgroup and they were able to consider its contents whilst preparing the amendments to the Computer Misuse Act 1990 that were put forward in the Police and Justice Bill in January 2006.

The document benefited considerably from the expertise of other members of the Legal subgroup; however it is not an official publication of the Internet Crime Forum and, with the publication of the Government's Bill, it is no longer considered to be worthwhile to go through the process of making it such. It is therefore being published as an individual contribution to the debate around how denial of service might best be dealt with.

Please note that the document was essentially complete before the publication of the Police and Justice Bill and hence there is very limited commentary within this document upon the precise approach that the Government has decided to take in criminalising denial of service. Nevertheless, I believe that as background material, showing the complexities involved in the issue, it continues to have significant value.

Richard Clayton
February 2006

Complexities in Criminalising Denial of Service Attacks

Richard Clayton
February 2006

Background

A Denial-of-Service (DoS) attack on the Internet occurs when a deliberate attempt is made to stop a computer from performing its usual activities by having another computer create large amounts of specious traffic to it. The traffic may be valid requests made in an overwhelming volume or specially crafted protocol fragments that cause the serving machine to tie up significant resources to no useful purpose.

The protocol mechanisms exploited in DoS and DDoS attacks vary. In some cases, entirely innocent remote machines are used to “amplify” traffic. For example, sending

a single SYN packet with a forged source address will cause a normally configured machine to send several SYN/ACK packets to the victim. In other cases, machines are "taken over" by exploiting security flaws in their operating systems or by persuading their owners to execute an email "virus". The controlled machines are then instructed to send the attack traffic.

In a Distributed Denial-of-Service (DDoS) attack a large number of remote computers are orchestrated into attacking a particular target at the same time. One often speaks of the remote machines being "zombies", organised into a "bot-net". A DDoS attack can be difficult to deal with because you cannot just locate a single rogue machine and disconnect it.

In some cases, such as the mainly unsuccessful October 2002 attack on the root name servers [1], the attacks overwhelmed the connecting links to a machine rather than the machine itself – many of the root name servers were unaffected because insufficient traffic actually reached them to make any real difference to their operation. Clearly, when network links fill up (or routers become overloaded) then you can get significant collateral damage that extends beyond the machine that is actually being attacked – and then some legal conundrums could arise if a direct cause-and-effect is needed for a statutory offence to occur.

DoS and DDoS attacks are extremely common on today's Internet with academic studies measuring over 4,000 a week [2] (that study was back in 2001, and no-one believes that the problem has reduced). There are many different types of attack and the volume of traffic involved varies hugely, so it is difficult to generalise about their impact. At the lower end of effectiveness, the blips in traffic are hardly noticeable, however, at the upper end the APIG inquiry into reform of the Computer Misuse Act was told of examples where large University networks were made unusable for hours at a time [3].

Attacks vary widely in sophistication, it is understood that the attacks on UK Gambling sites in Spring 2004[4] were relatively "low tech" and that at present bot-net attackers seldom "spoof" the source addresses being used; which in principle makes the attack traceable; albeit only back to the bot-net "zombie" that the attacker is controlling. Tracing back to the instigator is complex and seldom successful.

Well-executed attacks are very hard to track, and are far from simple to distinguish from legitimate traffic (meaning that a court might not be convinced by what was "obvious" to a system administrator). Providing protection against some types of DoS (and especially DDoS) attacks can be extremely technically challenging. It is often the case that it is very hard to distinguish well between legitimate from illegitimate activity and this means that genuine traffic can be discarded by protective measures. This all means that the attacker is motivated to use sophisticated attacks whenever possible.

In passing, it should be noted that despite the relatively simple nature of the attacks, the perpetrators of the "Gambling" attacks were tracked down by traditional "offline" police-work rather than by locating the source of the DDoS attack itself. As attacks become more sophisticated the "offline" approach is likely to continue to be of key importance.

Current legislation

There is a widely held view in industry that the Computer Misuse Act 1990 (CMA) is not adequate for dealing with DoS and DDoS attacks, though detailed analysis of why this might be is rare. It has been well understood since at least 2002 that CMA s3 might not stretch to including all DoS activity; nevertheless where machines have been converted to zombies in a bot-net, it is very likely that s1 offences will have been committed (provided there is jurisdiction, which for the CMA is very wide-ranging).

It should also be noted that the 'EU Council Decision on attacks against information systems' – 2005/222/JHA [5] – requires that a criminal offence must be committed by "intentional serious hindering or interruption of the functioning of an information system" and also "suppressing or rendering inaccessible computer data", if either is done "without right" at least "for cases which are not minor". This appears to make it a requirement to have a criminal offence for DoS/DDoS on the statute book by 16 March 2007.

The "Convention on Cybercrime" [6], which the UK wishes to ratify, also requires a criminal offence for intentional "serious hindering without right of the functioning of a computer system" (the wording differs in layout but not in intent).

The Government's view (along with many academic lawyers and also the NHTCU), is that s3 is sufficiently broad to cover DoS attacks. In April 2003 the Internet Crime Forum (ICF) Legal Subgroup pointed out that s3 did not require unauthorised access[7], merely unauthorised "modification of the contents of any computer". The view at that time was that the test applied would be whether the attack had rendered unreliable the data stored on a computer or impaired its operation.

The APIG inquiry heard evidence from Energis and ISPA that they knew of DoS attacks that were not investigated because "no crime could be framed"; equally with the exception of the gambling sites episode (where the main crime was extortion) there's a general perception that most attacks are too minor and too hard to investigate to bother with. APIG recommended adding an explicit offence to the CMA of 'impairing access to data' saying "we consider that this would send a clear message to the police, to the CPS and to the courts that these attacks should be taken seriously. In addition, publicity about the new offence will reach DoS attackers and some will be deterred by knowing, without the doubts currently expressed, that their actions are clearly criminal."

Caselaw

At the time of the 2003 ICF report there had been no prosecutions for a DoS attack. The situation is only slightly changed today.

DoS was peripherally involved in R v Caffrey (2003), however, the illegality of DoS was not an issue. Aaron Caffrey was charged under s3 with having made a modification to the computers of the Port of Houston. That modification was made so as to carry out a DoS attack against persons unknown, and the effect of the

modification was such as to cause the Port of Houston server to crash. However, the evidence that was shown related purely to the modification, not to the result of the modification. It was an accepted point in the case [8] that the modification occurred, that it was unauthorised, that it was so as to impair that computer, and that such impairment was unlawful under s3 CMA 1990. In the event, Caffrey was acquitted [9].

In a 2005 case in the Wimbledon Youth Court, the defendant had been charged under CMA s3(1) with unauthorised modification of a computer. He had caused many millions of emails to be sent to an email server, which was unable to cope with the load – a so-called "mail bomb". The defence argued that there was it was implicitly permitted to send email to an email server, that there was no specific number at which permission ceased. The District Judge agreed that "no reasonable tribunal could conclude that the modification caused by the emails sent by the defendant were unauthorised within the meaning of Section 3" and the case was dismissed [10].

Other legislation

There is other relevant legislation as well as the CMA that may apply in particular circumstances; for example the Malicious Communications Act 1988 (if a DOS attack consisted of email messages that were indecent, grossly offensive, threats or false) and the Protection of Harassment Act 1997 (if the traffic amounted to harassment of a person).

If some of the traffic passes across a wireless network, then in special circumstance (using wireless signals to jam other transmissions) then s13 of the Wireless Telegraphy Act 1949 may be relevant.

However, of particular relevance to DoS/DDoS attacks, s127(2)(c) of the Communications Act 2003 provides that "a person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he … persistently makes use of a public electronic communications network". At present, no-one seems to have been charged with this offence, which carries a maximum sentence of six months, possibly because as a summary offence proceedings must begin within six months and this has ruled it out in some cases where the decision on what charge to proceed with has been unduly delayed.

Authorisation

Another key element of the CMA offences is the notion of authorisation and this leads to substantial difficulties when considering events on the Internet. For example, this was a key issue in the Wimbledon Youth Court case already mentioned.

Most people would assume that www.example.com was a webserver that they were entitled to attempt to access if they wanted to learn about Example Ltd, or Example Inc, or possibly even Mr & Mrs Example and their children. There's an implicit expectation that you can access the machine on the "well-known" port 80 which is used for the web protocol HTTP (in fact "well-known" is the standard way of describing the port number, because there's no way of discovering it by consulting a lookup service – you have to know it).

Does it therefore follow that if a home user installs a web server unintentionally (quite easy to do with some versions of Windows) and then fails to configure it correctly that it is acceptable for anyone on the Internet to access their machine and fetch documents from it? The court would have to decide how obvious it was that access was not authorised.

In R v Straszkiewicz (2005) there was a conviction for dishonestly obtaining a communications service with the intent to avoid payment (s125 Communications Act 2003) where someone was found standing in a residential area with a wireless enabled laptop computer and apparently using "open" wireless access points in nearby houses. Clearly the court was persuaded on the facts of the case that dishonesty had occurred, since in some circumstances wireless access points are intentionally left open by their owners, for example, by those participating in the CONSUME project [14].

There is an expectation that private material will be kept private by means of passwords or other controls – but when a Reuters journalist "guessed" the URL for an upcoming financial quarterly financial report the Swedish company Intentia International AB pressed for criminal charges to be filed [15]. There are a number of other cases related to URL links which have been decided in a hotch-potch of ways in various jurisdictions over the past few years [16].

So there is real doubt (and some real cases to fuel that doubt) about access to documents and even more doubt about the nature of authorisation for access to machines – not whether it is allowed, but what might be excessive.

In R v Cuthbert (2005) there was a conviction for unauthorised access under CMA s1 [17]. Daniel Cuthbert had contributed some money to a charity website set up to help victims of the Boxing Day Tsunami. He had attempted to test the security of the website by using a "directory traversal attack" (trying, and in fact failing, to access the non-public parts of the webserver by typing in a URL containing a string such as "../../../". The court held that he was not authorised to attempt such an access, suggesting authorisation can be determined, at least in straightforward cases.

Cyber-protest

Excessive access has long been used for protest. In 1998 the pro- Zapitista group "Electronic Disturbance Theater" targeted the Mexican Government, US Department of Defense and the Frankfurt Stock Exchange bringing sites down through excess traffic [18]; and their actions continue to this day (in July 2005 they persuaded 27,000 people to have a "virtual sit-in" on a US Border Patrol website [19]). In October 2000 a French group, "Federation of Random Action", organised a cyber attack on the IMF and World Bank – their tool would access these sites whenever a keyword, such as "poverty", "finance" or "investment" came up in an online chatroom [20]. The websites claim they were "unharmed". Other targets have involved oil companies, investment firms and Starbucks.

A potential difference that might be brought out to distinguish "cyberprotest" from "denial of service" is that these protest actions only succeed if many people join in. If they only make one or two accesses each then it will take thousands of people to

affect a website. However, if there is automation involved (viz: not people using their own mouse clicks to access the site) then there may be millions of accesses for each protester.

In a DoS or DDoS attack the attack rate is usually limited by the size of the attacking machine's own connection to the Internet – and they are seldom interested in what data, if any, is returned. In cyberprotest, as described above, the protesters are expecting to see the webpage returned (assuming the server can cope with the load).

It would be unwise to make a distinction between cyberprotest and DoS/DDoS by concentrating on the tools that are used (even standard browsers can be scripted in standard ways, so there's no need for a special program to be built) but the emphasis should be placed upon intent and amplification... one might still prosecute for excessive noise if a single protester brought a lorry with 100 bullhorns to a demo, whereas 10,000 protesters, just 100 of whom had a bullhorn, might well escape action by the authorities...

Intent

Of course, there is also the issue of "intent" to examine. It is common for systems to be overloaded unintentionally. The 1901 census website collapsed from overuse [21] when it was first made available (and there the collapse lasted for days, so you could hardly say that all of the people who looked at it after the first day were unaware that their access was likely to cause damage).

There is also the example of the UK (and Belgium and Holland) phone system collapsing when fans tried to purchase tickets for the World Cup in 1998 [22]. Similarly in 1999, ten million people tried to buy tickets for an England Scotland game in Euro 2000 – causing disruption (and some internal callers at Glasgow Council to obtain tickets by jumping the queue) [23].

In late 2004 an anti-spam system was proposed by Lycos Europe [24]. This was a screen-saver that was going to use a central list of websites owned by spammers and "attack" them by accessing the sites so as to degrade their performance. Leaving aside legal issues, this had numerous technical failings. The likelihood would be that other websites would have been hosted on the same machine as the spammer's site and certainly other sites in the same data centre would have been affected by the extra traffic. It is also unclear that there is remote monitoring technology that can accurately predict when a website is degraded (the intention) rather than shut down altogether. The system was widely criticised, some hackers attacked the distribution site (although the truth of what occurred is disputed) and Lycos withdrew the product fairly promptly.

In the summer of 2005 a startup called "Blue Security" based in California (R&D in Israel) has resurrected the general idea [25], albeit with some twists which they have patented (!) They pool spam that arrives advertising a website, then get clients to post automated complaints into forms on that website – hoping to overload the spammer, or make their order handling system collapse. The attack system remains available for download, but has again been widely criticised, and it is unclear if it has actually been used to attack anyone yet.

Proposals for revision of the CMA

The Police and Justice Bill that was announced on the 25th January 2006 contains provisions for amending the CMA so that it will cover DoS attacks.

There have been a couple of earlier relevant Parliamentary initiatives on criminalising denial of service:

- The Earl of Northesk introduced a 'Computer Misuse Amendment Bill' to bring DoS attacks squarely within the ambit of the CMA [11]. The Bill was given a second reading in the House of Lords on 20th June 2002, but made no further progress.

- More recently, Derek Wyatt brought forward a "10 minute rule bill" based on the APIG recommendations on 5th April 2005 [12] and in the current session, Tom Harris did the same [13].

APIG suggested that the reason for the wide disparity of legal opinion they were given, and the distrust they observed of the efficacy of the current law, is that when DoS and DDoS attacks occur on the Internet then it is the particular circumstances of each attack that makes it obvious whether the CMA wording applies.

In general, where a DDoS attack takes place then an offence will have been committed because many machines will have been taken over by the attacker and special software installed to implement the attack. Even when a system is attacked by a single machine, an offence will sometime be committed because the contents of the system will be altered. However, when the sole effect of an attack is to fill a nearby link with useless traffic, then it may be hard to show the elements of a CMA offence are present, although a DoS attack has certainly occurred.

APIG felt it was "clearly undesirable to have the illegality of an attack depend upon the exact mechanism used" so they recommended a new offence of "impairing access to data". This was expanded in the Wyatt Bill to cover situations where one machine was attacked with a view to affecting the performance of another. This was clearly intended to explicitly cover situations such as "filling a pipe" or impairing the performance of a firewall or router.

The proposals for amending the CMA have also incorporated increases in the maximum sentences for existing offences. The EU Council decision already mentioned requires that the tariff for s1 be raised from 6 months to at least a year. Wyatt's bill proposed two years for s1 and the same for his the new denial of service offence. This was in line with the APIG report recommendations. The Police and Justice Bill also proposes two years for s1, but ten years for the revised version of s3, within which DoS attacks are intended to fall.

Conclusions

There are a number of challenges to be met when considering how to criminalise denial-of-service attacks, many of which have been outlined above. The way forward seems to be to concentrate on the nature of the act – intentional damage – and leaving issues such as authorisation, collateral damage and all technicalities for the court to assess in the individual circumstances of each case.

Acknowledgements & caveats

The assistance of the other members of the Internet Crime Forum Legal subgroup has greatly improved the scope and accuracy of this document, for which grateful thanks are given. However, please note that this document has not been formally endorsed by the Internet Crime Forum and it has no formal status other than as a personal contribution. Also, it should be noted that I am not a lawyer, and this document should not be consulted for legal advice.

References

[1] P. Vixie, G. Sneeringer, M. Schleifer: Events of 21-Oct-2002 <URL:http://d.root-servers.org/october21.txt>

[2] D. Moore, G. M. Voelker, S. Savage: Inferring Internet Denial of Service Activity, Proceedings of the 2001 USENIX Security Symposium, Washington D.C., August 2001. <URL:http://www.caida.org/outreach/papers/2001/BackScatter/usenixsecurity01.pdf>

[3] A. Cormack: APIG Computer Misuse Act Enquiry – UKERNA submission 7th April 2004 <URL: http://www.apig.org.uk/archive/activities-2004/computer-misuse-inquiry/computer-misuse-inquiry-written-evidence/UKERNA_Evidence.rtf>

[4] M. Ward: Bookies suffer online onslaught. BBC News <URL:http://news.bbc.co.uk/1/hi/technology/3549883.stm>

[5] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, Official Journal L 069, 16/03/2005 P. 0067 – 0071 <URL:http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX :32005F0222:EN:HTML>

[6] Convention on Cybercrime <URL:http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

[7] Internet Crime Forum Legal Subgroup: Reform of the Computer Misuse Act 1990. <URL:http://www.internetcrimeforum.org.uk/cma-icf.pdf>

[8] N. Barrett: Feedback on CMA inquiry and report <URL:http://www.apig.org.uk/cma_feedback.htm>

[9] Dickinson Dees: IT Briefing Autumn 2003 <URL:http://www.dickinson-dees.co.uk/publications/itbriefing/itbriefing-autumn2003.asp>

[16] K. Grant DJ, R v a minor, Wimbledon Youth Court, 2 Nov 2005. Reported by ZDNet UK: <URL:http://news.zdnet.co.uk/internet/security/0,39020375,39235359,00.htm>

[11] Earl of Northesk: Computer Misuse (Amendment) Bill [HL], 2002 <URL:http://www.publications.parliament.uk/pa/ld200102/ldbills/079/2002079.pdf>

[12] D. Wyatt: Computer Misuse Act 1990 (Amendment) Bill <URL:http://www.apig.org.uk/CMAdft3.pdf>

[13] T. Harris: text of bill isn't available online; URL is for his speech. <URL:http://www.publications.parliament.uk/pa/cm200506/cmhansrd/cm050712/debtext/50712-05.htm#50712-05_spnew8>

[14] Consume project. <URL:http://www.consume.net>

[15] M. Delio: Rooting Around Site With Intent? Wired News, 30 Oct 2002 <URL:http://wired-vig.wired.com/news/politics/0,1283,56079,00.html>

[16] S. Ott: Links & Law <URL:http://www.linksandlaw.com/news.htm>

[17] Silicon.com: Tsunami 'hacker' found guilty. <URL:http://management.silicon.com/government/0,39024677,39153121,00.htm>

[18] Electronic Disturbance Theater: Bulletin, 5 Sep 1998 <URL: http://www.contrast.org/netstrike/archivio/thing.html>

[19] post.thing.net ! Virtual Sit-In Against Anti-Immigrant Website – July 20th to July 22nd, 2005 <URL:http://post.thing.net/node/388>

[20] S. Ferguson: 'Pecked to Death by a Duck' Hacktivists Chat up the World Bank, The Village Voice, 18-24 Oct 2000 <URL:http://www.villagevoice.com/news/0042,ferguson,19055,1.html>

[21] BBC: Census website a crashing success. 2 Jan 2002 <URL:http://news.bbc.co.uk/2/hi/uk_news/1737861.stm>

[22] C.P. Martin: Euro phone network collapse: France'98 Cup tickets, RISKS 19(71) <URL:http://catless.ncl.ac.uk/Risks/19.71.html#subj2>

[23] BBC: Council criticised in ticket fiasco report <URL:http://news.bbc.co.uk/1/hi/scotland/558563.stm>

[24] Infoworld: Lycos' anti-spam screensaver draws fire, 1 Dec 2004 <URL:http://www.infoworld.com/article/04/12/01/HNlycosscreensaver_1.html>

[25] TechWeb: Startup Aims To Overload Spammer Web Sites, 18 Jul 2005 <URL:http://www.techweb.com/wire/security/166400269>