scripted

Volume 11, Issue 3, December 2014

CAN CSIRTS LAWFULLY SCAN FOR VULNERABILITIES?

Andrew Cormack[*]

Abstract

Security teams routinely scan their own networks to identify computers that may be vulnerable to attacks that would damage the organisation's information or services. However, the discovery in early 2014 of the widespread Network Time Protocol (NTP) reflection and Heartbleed vulnerabilities highlighted that serious risks to information and systems can also result from vulnerable systems outside the organisation's network. Security teams would like to identify these vulnerable systems, both to prepare their own defences and to try to warn the systems' operators to fix the vulnerabilities. It is far from clear, however, whether UK criminal law permits scanning of external systems.

This paper considers the unauthorised access offences contained in the UK *Computer Misuse Act 1990* and the few reported cases. It concludes that scanning to determine whether or not a computer is vulnerable probably does constitute "access" and for an external computer is unlikely to be explicitly "authorised". However actions that have been accepted by courts as lawful (sending an e-mail and visiting a website) indicate that authorisation may also be implicit. Theories of cyberproperty and cases under the US *Computer Fraud and Abuse Act*, including the historic *US v Morris*, suggest that connecting a computer or service to the Internet does implicitly authorise actions related to the intended function of that service. This appears consistent with the UK decisions in *Lennon* and *Cuthbert* and implies that while scanning for NTP reflection vulnerabilities should be lawful, testing for Heartbleed probably is not.

DOI: 10.2966/scrip.110314.308

[*] Chief Regulatory Adviser, Janet

1. Introduction

Computer Security Incident Response Teams (CSIRTs) were originally created in the 1990s by organisations and network operators to mitigate the effects of security incidents that occurred within their constituencies. The authority of most CSIRTs was, and remains, either informal or contractual – for example in network terms of service;[1] only recently have a few European countries placed their national CSIRT on a statutory basis. The activities of CSIRTs quickly expanded to cover incident prevention and detection as well as remediation[2]: most now provide security information and advice to systems administrators and users,[3] and many monitor internal systems and network traffic for signs of problems.

Since the main source of risk to organisations' information and services was insecurities in the organisation's own networked computers, CSIRTs whose authority permitted it actively scanned internal networks to find these vulnerabilities and fix them before they were discovered and exploited by attackers. However, more recent attacks use insecure systems elsewhere on the Internet as launch-pads,[4] for example to discover the passwords of legitimate users[5] or to create massive flows of traffic[6] that can overwhelm even secure services and networks.[7] CSIRTs now need to discover these external weak links in Internet security[8] to protect their constituencies against possible attack. This paper will examine how this can be done in accordance with the UK's *Computer Misuse Act 1990*[9] and the Council of Europe *Cybercrime Convention*,[10] considering whether network scanning constitutes "access", how it may be "authorised" and what knowledge CSIRTs will be presumed to have.

2. Access

Scanning a computer aims to discover whether a service is absent, present but secure, or vulnerable. An optimal scan would therefore send requests that produce a different response in these three different states. Positive responses are preferred, since silence

---

[1] For example the Janet Security Policy available at https://community.ja.net/library/janet-policies/security-policy (accessed 20 Nov 2014).

[2] CERT, "CSIRT Services" (2014) available at http://www.cert.org/incident-management/services.cfm (accessed 20 Nov 2014).

[3] For example CERT-UK available at https://www.cert.gov.uk/ (accessed 20 Nov 2014).

[4] A Burstein, "Amending the ECPA to Enable a Culture of Cybersecurity Research" (2008) 22:1 *Harvard Journal of Law and Technology* 167-222, at 175.

[5] J Wakefield, "Heartbleed bug: what you need to know" (2014) available at http://www.bbc.co.uk/news/technology-26969629 (accessed 20 Nov 14).

[6] M Ward, "Hack attacks battled by net's timekeepers" (2014) available at http://www.bbc.co.uk/news/technology-26662051 (accessed 20 Nov 14).

[7] K Soluk, "NTP Attacks: Welcome to the Hockey Stick Era" (2014) available at http://www.arbornetworks.com/asert/2014/02/ntp-attacks-welcome-to-the-hockey-stick-era/ (accessed 20 Nov 14).

[8] A Burstein, see note 4 above, at 176.

[9] *Computer Misuse Act 1990*.

[10] *Convention on Cybercrime 2001*, CETS No.185.

may merely indicate that the request or response was lost en route. The particular requests chosen will depend on which service and vulnerability are being tested – two examples are discussed later.

The UK's *Computer Misuse Act 1990* defines access to a program or data:

> S17(2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he-
>
> ...
>
> (c) uses it
>
> ...
>
> (3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform-
>
> (a) causes the program to be executed; or
>
> (b) is itself a function of the program.

Scanning intends to cause the target computer to perform a function – returning a response – so will constitute "access" unless the response is generated by something other than a "program held in a computer". This might be argued for protocols where the computer's network interface hardware generates the "absent" response. However distinguishing vulnerable and non-vulnerable services will usually involve executing either a program or operating system service. In addition, vulnerability testing that involves discovering the version or settings of a program or operating system is likely to constitute access to data under s17(2)(d):

> d) has [data] output from the computer in which it is held (whether by having it displayed or in any other manner);

The Crown Prosecution Service guidance to prosecutors confirms that access involves "an intention to obtain information about a program or data held in a computer".[11] Vulnerability scanning does appear to require "*access*" under UK law.

Although the Council of Europe *Cybercrime Convention* was created a decade after the *Computer Misuse Act*, the UK has declared that its law conforms to the Convention[12] so its terms may assist with interpretation. The Convention does not define "access" but says it may apply to "the whole or any part of a computer system".[13] Since "computer system" includes "a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing

---

[11] Crown Prosecution Service, "Prosecution Policy and Guidance: Computer Misuse Act 1990" (2011) available at http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/ (accessed 20 Nov 14), at 1(2).

[12] Council of Europe, "Convention on Cybercrime: list of Signatures and Ratifications" (2014) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG (accessed 20 Nov 14).

[13] *Convention on Cybercrime*, Art.2.

of data"[14] it appears "access" might even cover responses generated by network interface devices. Cases under the American *Computer Fraud and Abuse Act*[15] (*CFAA*) have taken a narrower view:[16] *Moulton v VC3* ruled in 2000 that a port scan "did not grant...access to the Defendant's network".[17] However testing random dial-up access codes was "making use of any resources of a computer" under Washington's Act (*State v Riley*).[18,19] This variation, and Clough's observation that the "constantly evolving ways in which we interact with computers do not necessarily conform to the traditional idea of 'access'"[20] suggests the legal position of vulnerability scanning might change. A *CFAA* offence would, however, still require there to be damage to the target system.[21]

3. Authorisation

If scanning does constitute "access", it will be an offence under s1 of the *Computer Misuse Act* if the access is unauthorised[22] and the scanner "knows at the time...that that is the case".[23] Clough sees this offence as protecting confidence in data stored on computers, hence there is no requirement for damage[24] and, as in *Cuthbert*,[25]the motive for access is irrelevant.[26] According to s17(5) of the Act, a scanner's access will be unauthorised if:

> (a) he is not himself entitled to control access of the kind in question to the program or data; and
>
> (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.[27]

---

[14] *Ibid*, Art.1.

[15] D Carucci, D Overhuls and N Soares, "Computer Crimes*"* (2011) 48 *American Criminal Law Review* 375-419, at 394.

[16] J Clough, "Data Theft? Cybercrime and the Increasing Criminalisation of Access to Data" (2011) 22 *Criminal Law Forum* 145-170, at 155.

[17] *Scott Alan Moulton and Network Installation Computer Services Inc v VC3* (US District Court, Northern District of Georgia, 6th November 2000).

[18] *State v Riley* 988 A.2d 1252, 1258 (N.J. Super. 2009).

[19] J Clough, see note 16 above, at 156.

[20] *Ibid*, 153.

[21] D Carucci, see note 15 above, at 394.

[22] *Computer Misuse Act 1990*, s1(1)(b).

[23] *Computer Misuse Act 1990*, s1(1)(c).

[24] J Clough, see note 16 above, at 161.

[25] *R v Daniel Cuthbert* Horseferry Road Magistrates Court 7/10/2005, (report by BBC News available at http://news.bbc.co.uk/1/hi/england/london/4317008.stm (accessed 20 Nov 14)).

[26] P Sommer, "Computer Misuse Prosecutions" (2005) 16(5) *Computers and Law* 24-26.

[27] *Computer Misuse Act 1990*, s17(5).

3.1 Explicit Authorisation

For internal scans, CSIRTs may themselves be entitled to control access or have explicit consent from the system owner under either a contract[28] or the terms of use of a network. Provided scanning complies with the terms of the agreement, it is clearly authorised and lawful.

However many threats to networks and computers now arise from insecure computers outside the CSIRT's constituency. Recently Network Time Protocol (NTP) reflection attacks have used vulnerable systems to direct huge quantities of traffic towards victim networks[29] while the Heartbleed vulnerability leaks private information from many websites.[30] CSIRTs need to warn their users and network managers about these threats but discovering them requires scanning systems where it is infeasible to obtain the owner's explicit consent.

3.2 Implicit Authorisation

Fortunately consent to access an Internet service may "be implied from [the owner's] conduct in relation to the computer",[31] for example we access websites without asking first. Where implicit consent can be presumed, scanning should be lawful so long as the scanner does not know that their actions are unauthorised.[32] Such knowledge may be acquired during scanning by discovering a barrier to access or may be inferred in advance from the kind of access being sought. Statute and case law indicate some presumptions of consent to scanning and when a CSIRT should nonetheless know it is unauthorised.

3.2.1 Authorisation by Advertisement

Where vulnerability can be determined by connecting to an Internet service and making a normal request, this access should be authorised by the owner's action in advertising the service. *R v Lennon* accepted that providing an Internet e-mail service authorised attempts to send e-mails to that service,[33] including those the system owner "does not want".[34] *Re Yarimaka* said authorisation existed "in the case of legitimate e-mails such as are invited by the owner of a computer by the publication of his e-mail address".[35] Authorisation should likewise cover other services whose use is "invited" by the owner, for example by publishing a link to a web site or announcing in the

---

[28] R Walton, "The Computer Misuse Act" (2006) 11 *Information Security Technical Report* 39-45, at 44.

[29] M Ward, see note 6 above.

[30] J Wakefield, see note 5 above.

[31] *DPP v David Lennon* [2006] EWHC 1201 (Admin) (henceforth *Lennon*) at [9].

[32] *Computer Misuse Act 1990*, s1(1)(c).

[33] *Lennon* at [9].

[34] *Ibid* at [14].

[35] *Re Yarimaka and another* [2002] EWHC 589 (Admin) (henceforth *Yarimaka*) at [22].

Domain Name System ("the phone book of the Internet"[36]) a hostname widely understood to indicate a public service, such as www.example.com.

3.2.2 Authorisation by Availability

However, attacks can also come from Internet-connected computers whose services are unadvertised, or even unknown to their owners. These are frequently vulnerable because the owner is unaware of the need to maintain them. Unadvertised services can be discovered, both by attackers and by CSIRTs, by simply testing every Internet Protocol version 4 (IPv4) Internet address: modern network speeds mean this can take less than an hour.[37] In countries such as Germany[38] testing whether services exist is lawful thanks to an option in the *Cybercrime Convention* that "A Party may require that the offence be committed by infringing security measures".[39] Provided the scanner detects technical security measures and does not attempt to infringe them, no crime should be committed in these jurisdictions.

In UK law, however, the only requirement for unauthorised access to be criminal is that the person "knows at the time when he causes the computer to perform the function that [the access is unauthorised]".[40] Where a system owner – the source of authorisation according to s17(5) – makes a service accessible from the Internet without clearly indicating its intended users, an external CSIRT does not know whether its access is unauthorised. Walton considers "the boundary between what is authorised and what is not when connecting to open sites on the Internet can be somewhat blurred and it is not always clear when the line is overstepped"[41] and this "can make it quite hard to determine whether some specific actions are legal or not...until it is actually tested in court";[42] Clough appears to presume authorisation "in contexts such as public websites where it may not be apparent that access is restricted".[43] The legality of scanning unadvertised services that have been made technically accessible depends on what authorisation the law presumes from the act of connecting to the Internet. There are three possibilities: that all access is unauthorised, that all access is authorised, or that only some access is authorised.

The first option, that all access to unadvertised services is unauthorised and therefore criminal, conflicts with both technical and legal precedents. Vital Internet protocols such as the Dynamic Host Configuration Protocol (DHCP) locate servers by sending a

---

[36] J Chen, "Google Public DNS" (2012) available at http://googleblog.blogspot.co.uk/2012/02/google-public-dns-70-billion-requests.html (accessed 20 Nov 14).

[37] Z Durumeric, E Wustrow and J Halderman "ZMap: Fast Internet-Wide Scanning and its Security Applications" (2013) available at https://zmap.io/paper.pdf (accessed 20 Nov 14).

[38] Bundesministerium der Justiz und für Verbrauchershutz, "German Criminal Code: Section 202a" available at http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1710 (accessed 20 Nov 14).

[39] *Convention on Cybercrime*, Art. 2.

[40] *Computer Misuse Act 1990*, s1(1)(c).

[41] R Walton, see note 28 above, at 42.

[42] *Ibid*, 40.

[43] J Clough, see note 16 above, at 167.

"broadcast" message to all nearby computers, hoping that one or more will respond.[44] Under the UK's broad definition, this is an attempt to access every computer on the local network. If the law presumed that access was unauthorised without positive invitation, and system owners knew that, then every use of DHCP and similar broadcast protocols would be a criminal offence. Similarly in the case of *Svensson and Others v Retriever Sverige AB*[45] the European Court of Justice found that once "protected works [were] published without any access restrictions on another site",[46] "the authorisation of the copyright holders is not required" by someone who creates clickable links to them.[47] This seems incompatible with authorisation being required by a user who follows the links and accesses the material: indeed Hörnle concludes that following *Svensson* "a rightsholder who makes available a work on the Internet without technical protection measures or access restriction is taken to have enabled any use which an on demand user can make".[48]

However presuming that all access is authorised until informed otherwise also appears incompatible with UK legal precedent. In both *Lennon*[49] and *Cuthbert*,[50] access that was technically possible to an advertised site was nonetheless found to be unauthorised. The Crown Prosecution Service quotes *Lennon*: "although the owner of a computer able to receive e-mails ordinarily consents to the receipt of e-mails, such consent did not extend to e-mails that had been sent not for the purpose of communicating with the owner but for the purpose of interrupting the operation of the system".[51] According to these cases, something less than a technical barrier can negate presumed authorisation.

Lennon did not "try to define the limits of the [implied] consent"[52] and treated his "purpose" as relevant, something that is not justified by the wording of s1 of the *Computer Misuse Act*. At the time the Act did not cover denial of service attacks,[53] so this may have been the only way to fit Lennon's conduct into the unauthorised access offence. American cases provide more discussion of the boundary, and suggest various bases for it, though Kerr notes "courts have faced even greater difficulties trying to interpret the meaning of authorization"[54] and Goldman considers they "have not agreed on the proper interpretation".[55] Although the federal *Computer Fraud and*

---

[44] R Droms, "Dynamic Host Configuration Protocol, RFC2131" (1997) available at http://www.ietf.org/rfc/rfc2131.txt (accessed 20 Nov 14) at 3.1.

[45] *Svensson and Others v Retriever Sverige AB*, Case C-466/12 [2014].

[46] *Svensson* at [18].

[47] *Svensson* at [29].

[48] J Hörnle, "Is Linking Communicating?" (2014) 30 *Computer Law and Security Review* 439, at 442.

[49] *Lennon* at [13].

[50] P Sommer, see note 26 above.

[51] Crown Prosecution Service, see note 11 above, at 3.

[52] *Lennon* at [9].

[53] Section 3 was subsequently amended by s36 of the *Police and Justice Act 2006*.

[54] O Kerr, "Cybercrime's Scope: Decoding 'Access' and 'Authorisation' in Computer Misuse Statutes" (2003) 78 *New York University Law Review* 1596-1668, at 1628.

[55] L Goldman, "Interpreting the Computer Fraud and Abuse Act" (2012) 13 *Pittsburgh Journal of Law and Technology* 1-38, at 5.

Abuse Act requires either damage[56] or taking of information[57] in addition to unauthorised access, state legislators often compared computer misuse with trespass or burglary: like those, and as in the UK Act, "the intrusion itself seemed worth prohibiting".[58] Bellia describes this as a "property" approach, with authorisation defined by the owner, as opposed to a "liability" one, where it is defined by the state.[59] Physical trespass laws "presume that people have a right to be where they are, and often require posted notice in that place instructing them that they cannot enter or remain there".[60] That presumed authorisation might be reversed by direct communication, or by erecting a fence, or by a notice likely to be seen by intruders.[61] Lastowka is concerned that the trespass analogy establishes a "cyberproperty" concept of an absolute "right to prohibit others from interacting with their equipment in ways that cause no physical damage or software malfunctions",[62] unlike real-world notices and fences that only have legal effect when in socially recognised places.[63] All four authors are uncomfortable, like the court in *Nosal*,[64,65] that the "notice" analogy would make any breach of website terms and conditions a potential crime.[66,67] Nonetheless the original hearing of *Drew*[68] did conclude that use in breach of MySpace's Terms of Service was a criminal misdemeanour under the *CFAA*. Kerr argued that "violating the Terms of Service is the norm, complying with them the exception"[69] and that a statute that criminalised such conduct would be unconstitutionally vague through "leav[ing] the public uncertain as to the conduct it prohibits"[70] and "encouraging discriminatory enforcement".[71] Kerr's call for courts to "reject interpretations of unauthorised access that criminalize routine Internet use"[72] was heeded by Judge Wu in granting Drew's motion to acquit: moving the boundary of implied authorisation but still leaving it unclear.

---

[56] *Computer Fraud and Abuse Act*, 18 U.S.C. Section 1030(a)(5)(B).

[57] *Computer Fraud and Abuse Act*, 18 U.S.C. Section 1030(a)(2)(C).

[58] O Kerr, see note 54 above, at 1615.

[59] P Bellia, "Defending Cyberproperty" (2004) 79 *New York University Law Review* 2164-2273, at 2189.

[60] O Kerr, see note 54 above, at 1622.

[61] L Goldman, see note 55 above, at 26.

[62] G Lastowka, "Decoding Cyberproperty" (2007) 40 *Indiana Law Review* 23-71, at 23.

[63] *Ibid*, 66.

[64] *US v Nosal* 676 F.3d 854 (9th Cir. 2012).

[65] L Goldman, see note 55 above, at 12.

[66] O Kerr, see note 54 above, at 1638.

[67] P Bellia, see note 59 above, at 2258.

[68] *US v Lori Drew* 259 F.R.D. 449 (US District Court, CD California, 28 August 2009).

[69] O Kerr, "Vagueness Challenges to the Computer Fraud and Abuse Act" (2009-2010) 94 Minn. L. Rev. 1561-1587, at 1582.

[70] *Ibid*, at 1573.

[71] *Ibid*, at 1575.

[72] *Ibid*, at 1577.

To keep contract breach as a civil matter, Kerr proposes that "unauthorised" in a criminal statute "should require, at a minimum, the circumvention of a code-based restriction on computer access",[73] either exploiting a vulnerability or presenting false identification.[74] The absence of any barrier, as in trespass and burglary,[75] indicates consent to intrusion[76] though not to subsequent damage. Bellia agrees, considering that without a barrier there is no *CFAA* criminal "access" anyway.[77] Goldman, reluctant to decriminalise digital versions of crimes such as cashier fraud,[78] suggests a narrower interpretation, that the implicit consent is "limited to actions necessary to achieve the purpose of the consent".[79] This echoes an early Internet case, *US v Morris*,[80] which considered whether Morris's worm had used Internet services "in any way related to their intended function".[81] Kerr notes this "appears to derive largely from a sense of social norms in the community of computer users",[82] matching Lastowka's requirement that trespass boundaries be socially recognised. While Kerr's authorising anything that is technically possible conflicts with the UK precedents of *Lennon* and *Cuthbert*, a Goldman/Morris "intended function" interpretation does seem compatible with those UK cases.

Something like the *Morris* "intended function" test appears to have led the court in *R v Cuthbert* to conclude that access was not "of the kind"[83] the system owner had implicitly authorised. Access to the Disasters Emergency Committee website had been invited through television adverts. Cuthbert made a donation but then, concerned, tested the site for a well-known vulnerability.[84] Although there were no unusual characters in his request, the particular directory traversal sequence "../" was considered to be unauthorised and Cuthbert was found guilty under section 1 of the *Computer Misuse Act*. It may be significant that Cuthbert is a professional penetration tester. The Act's wording "he knows at the time..."[85] may create a subjective test, expecting a penetration tester to know in advance that "there were no circumstances in which there was consent for directory traversal"[86] (Walton considers it "very poor judgment on his part"[87]) while allowing the non-expert user more freedom to guess

---

[73] O Kerr, see note 54 above, at 1600.

[74] *Ibid*, 1649.

[75] *Ibid*, 1600.

[76] *Ibid*, 1652.

[77] P Bellia, see note 59 above, at 2254.

[78] L Goldman, see note 55 above, at 24.

[79] *Ibid*, 28.

[80] *US v Morris* 928 F.2d 504 (2d Cir. 1991).

[81] O Kerr, see note 54 above, at 1632.

[82] *Ibid*.

[83] *Computer Misuse Act 1990*, s17(5)(b).

[84] P Sommer, see note 26 above.

[85] *Computer Misuse Act 1990*, s1(1)(c).

[86] P Sommer, see note 26 above.

[87] R Walton, see note 28 above, at 43.

URLs when they cannot find information.[88] If this test is indeed subjective, CSIRTs are likely to be judged against the same high standard. To ensure they do not "know at the time" their scanning is unauthorised a CSIRT should apply the *Morris* test and only use standard commands in ways "related to their intended function". The same commands would be "necessary to achieve the purposes of the consent"[89] in Goldman's terms, so should be authorised by both theory and case law.

3.3 Impairing Performance

CSIRTs must be particularly careful if scanning may make the target machine or service crash or otherwise malfunction. Section 3 of the *Computer Misuse Act 1990* makes it a crime to perform an unauthorised act that impairs the performance of a computer. According to s3(3) of the Act recklessness, rather than an intention to impair the performance, is sufficient for this crime. Thus a CSIRT that is aware of the possibility that its action may impair performance and consciously takes that risk[90] may commit an offence under s3(3). For example, tests that exploit buffer overflows[91] may crash services so should only be run against systems where specific authorisation, accepting the risks, has been obtained. Although s3(1)(b) repeats the "knows that it is unauthorised" test from s1(1)(c), relying on implicit authorisation for these types of scan appears unwise as a performance-impairing action is unlikely to pass the *Morris* "intended function" test.

4. Illustrations

The implication of these conclusions for scanning may be illustrated by two recent vulnerabilities – Heartbleed and NTP reflection attacks.

Heartbleed[92] is a vulnerability in Secure Socket Layer (SSL) services that lets attackers obtain information from other connections to encrypted services, potentially including passwords, credit card numbers and encryption keys. CSIRTs wish to find vulnerable servers both to warn their own users against connecting to them and to inform the server owners of the problem. SSL uses the Transmission Control Protocol (TCP), so the availability of the service can be tested by connecting to the relevant TCP port (generally 443). Authorisation for this connection attempt may be implied, as in *Lennon*, from the computer's being connected to the Internet. This will immediately return a positive indication whether the service is available or not; if not, the scanner should move to the next computer or service. An accepted TCP connection would normally imply consent to execute a command, however an accurate Heartbleed test involves unusual parameters[93] so is likely to fall outside the

---

[88] I Walden, *Computer Crimes and Digital Investigations* (Oxford: OUP 2007) para 3.232.

[89] L Goldman, see note 55 above, at 28.

[90] M Allen *Cases and Materials on Criminal Law* 8th ed (London: Sweet and Maxwell 2001), at 117.

[91] Open Web Application Security Project, "Buffer Overflow" (2009) available at https://www.owasp.org/index.php/Buffer_Overflow (accessed 20 Nov 14).

[92] Codenomicon, "Heartbleed Bug" (2014) available at http://heartbleed.com/ (accessed 20 Nov 14).

[93] T Brewster, "Heartbleed: 95% of detection tools 'flawed' claim researchers" (2014) available at http://www.theguardian.com/technology/2014/apr/16/heartbleed-bug-detection-tools-flawed (accessed 20 Nov 14).

scope of the consent, as in *Cuthbert*. In some cases unusual parameters can cause services to crash so CSIRTs might also be expected to assess whether this was a foreseeable consequence before scanning a particular service. A normal command, permitted by both *Lennon* and *Cuthbert*, may allow the scan to determine the version of software in use and therefore whether it is likely to be vulnerable. However CSIRTs should only scan for the actual presence of the Heartbleed vulnerability within their constituencies where they have explicit authorisation.

NTP reflection attacks[94] involve a normal request to a Network Time Protocol server, but direct its response to a victim machine or network. The resulting volume of traffic – up to hundreds of Gigabits per second[95] – may overwhelm the victim's network, effectively disconnecting its users and services from the Internet. NTP runs over the connectionless User Datagram Protocol[96] (UDP) so the only way to determine whether the service is available is to send a command: unlike TCP there is no active acceptance or rejection of a request to connect.[97] Until some response is received, a scanner cannot know that their access is unauthorised. Since a single normal command can test whether an NTP service can be used for reflection attacks, sending that command should be within the implicit consent granted by making the system available over the Internet. It therefore appears that CSIRTs may lawfully scan for NTP reflection vulnerabilities, both to warn the service owners and to prepare defences against possible attack using the vulnerable systems.

5. Conclusion

UK law appears to presume implicit authorisation to access services that are advertised (*Yarimaka*) as well as those that are merely "not configure[d]...to exclude" requests (*Lennon*).[98] Scanning these services should not breach s1 of the *Computer Misuse Act 1990*, since the CSIRT will not "know at the time" of scanning that their access is unauthorised. This knowledge will be acquired when a service indicates that it is unavailable or restricted, so further scanning of that service on that machine would then be unlawful. To remain within the implicit authorisation, scans must only involve actions related to the intended function of the service (applying the *US v Morris* test) and not use unusual commands or options (*Cuthbert*). Scanning must avoid actions that may crash or otherwise impair the scanned service (*Computer Misuse Act* s3). As in *Cuthbert*, the Act's subjective test is likely to regard CSIRTs as having expert knowledge of which commands are unusual and which may impair the service's function.

This suggests that some scanning of external systems by CSIRTs should be lawful, even without explicit authorisation, provided the scans remain within the normal functions of the scanned service, avoid foreseeable risks of impairing the scanned service and move on as soon as an indication is received that a particular request is

---

[94] K Soluk, see note 7 above.

[95] *Ibid*.

[96] D Mills et al, "Network Time Protocol Version 4, RFC5905" (2010) available at http://www.ietf.org/rfc/rfc5905.txt (accessed 20 Nov 14).

[97] Mitre Organisation, "CAPEC-308: UDP Scan" (2014) available at https://capec.mitre.org/data/definitions/308.html (accessed 20 Nov 14).

[98] *Lennon* at [14].

unauthorised. This would permit scanning to test for NTP reflection vulnerabilities, but for Heartbleed it may lawfully only be possible to determine whether a service may be vulnerable, rather than whether it actually is.