Reacting to Cyber-Intrusions: The Technical, Legal and Ethical Dimensions

Richard E. Overill

INTRODUCTION

The classical three-layer security paradigm of 'Protect, Detect, React' has traditionally been applied to the field of information assurance with firewalls playing a major protective role while detection is handled mainly by intrusion detection systems. This somewhat simplified overview, however, leaves open two important questions: who or what should react, and how?

The potential range of options for reacting to cyber-intrusions has to date received substantially less critical attention than the protection from or the detection of cyber-intrusions. In many business-situations, recovery processing, which includes re-compiling code, relinking modules, reclaiming memory, restoring files, reconfiguring firewalls or network segments, and eventually resuming (a possibly reduced level of) business processing,[1] will naturally take priority over any form of reactive response.

However, in view of the introduction of automated response or 'active defence' capabilities into fielded systems during the past few years, this paper aims to address, highlight and critically evaluate the strategic issues that are associated with various types of reactive strategy. In particular, it is stressed that these issues must be viewed within the context of the portfolio of a particular organisation's mission statement, business continuity plan and information security policy.

The potential range of behaviours of these active defences raises at least three distinct kinds of issue for consideration:[2]

(1) technical possibilities — what behaviour is practically feasible;
(2) legal aspects — what behaviour falls within the appropriate legal framework;
(3) ethical considerations — what behaviour is acceptable in a particular cultural, social or business context.

This last category is especially influenced by an organisation's information security policy, business continuity plan and mission statement.

TECHNICAL POSSIBILITIES

In principle there exists a wide spectrum of potential responses that a reactive defence could make to a presumed intrusion. On a nominal graduated impact scale ranging from benign (0) to aggressive (9) these potential responses may be categorised within a schematic taxonomy as shown below:

(1) Notify the operator, system manager or network manager by means of a console alarm, pager, e-mail or text message (impact 0).
(2) Send a warning e-mail to the originator of the suspect process or connection (impact 1).
(3) Monitor and record suspect sessions or connections using system logs or raw network traffic data to provide forensic evidence or diagnostic material for any future investigation — the 'goldfish bowl' (impact 2).
(4) Lure the intruder into divulging identity information and other evidential material using a protective 'sandbox' or an enticing 'honey-pot' as a decoy (impact 2).
(5) Discard a stream of suspicious inbound network packets (impact 3).
(6) Discard all outbound packets destined for the originator of the process or connection — the 'black hole' (impact 3).
(7) Terminate the suspect user process (impact 4).
(8) Disconnect the offending user connection (impact 4).
(9) Disable the affected user account (impact 5).
(10) Modify a router filter list to reject connection requests from the suspect IP source address (impact 5).
(11) Reconfigure a firewall to block requests for the particular IP service used by the suspected intruder (impact 5).
(12) Shut down the affected machine (impact 6).
(13) Disconnect the affected machine from the network (impact 6).
(14) Perform an interrogatory probe, port scan or sub-net mapping on the presumed source of the suspected intrusion (impact 7).
(15) Mount a denial-of-service (DoS) reprisal attack

Journal of Financial Crime
Vol. 11, No. 2, 2003, pp. 163–167
© Henry Stewart Publications
ISSN 1359-0790

against the presumed source of the suspected intrusion using eg a worm, a worm-virus, a flood attack (impact 8).[3]

(16) Launch a retaliatory malicious software strike against the presumed source of the suspected intrusion using eg a virus, a worm-virus, a logic bomb, a Trojan horse (impact 9).[4]

It should be noted that three of the responses listed above (numbers 1, 3 and 4) can be classified further as ‘passive reactions’ since the intruder should in principle remain completely unaware of them. The remainder can be termed ‘active reactions’ since the intruder will sooner or later become aware of having triggered them. The time-frame within which an astute intruder is able to infer that some form of active reaction technique has been deployed is a key parameter in the tactical decision-making process for reaction. The longer an intruder remains unaware that a reaction technique is being employed against him, the more information can potentially be gleaned about his identity and his methodologies. However it also presents him with a greater opportunity for causing serious cyber-damage.

A ‘proactive’ defence, on the other hand, would not wait for a suspected intrusion to be flagged in order to become active. Rather, some form of preemptive countermeasure, such as one of those listed above, would be taken against any activity that did not appear to originate from a *bona fide* user at an approved site.[5]

There are however several potential problems with such ‘active defence’ strategies. In particular, unless the intrusion detection thresholds are very finely tuned to minimise the occurrence of false positives (without at the same time raising the occurrence of false negatives to an unacceptably high level),[6] a reactive defence may be triggered to disconnect an innocent user by a naturally occurring false positive, or it may be maliciously coerced by a strategically contrived false positive into unnecessarily shutting down a network connection.

These considerations were sharpened and focused by the announcement in 1998 of Blitzkrieg,[7] which was claimed to use self-replicating (worm-like) and self-repairing (core wars) technologies. Two versions of this system were reportedly developed: an aggressive military version designed to wage cyber-warfare by launching malicious software attacks against intruders and attempting to damage or destroy information on their computers, and a somewhat milder business version aimed at warding off DoS and other common attacks where the intruder’s aim was to prevent the operation of a commercial service rather than to destroy data *per se*.

A further strand in the reactive countermeasures or ‘strikeback’ debate is the claim by a group of hackers known as the Electronic Disruption Theater (EDT) that their cyber-attack in September 1998 on DefenseLink, the US Department of Defense’s (DoD) primary public information internet site, was cyber-ambushed by Pentagon officials. The web browsers of anyone logging onto the EDT website to participate in the DoS attack, which was based on the Java applet FloodNet, were automatically shut down. The hackers claimed that this alleged form of offensive information warfare was illegal under the US Computer Fraud and Abuse Act, a charge that was rebutted by the DoD and the Pentagon.[8] However, it has been pointed out that a prime US military directive, *posse comitatus*, was breached; this directive forbids the US military from taking unilateral action within the USA against US citizens.[9]

LEGAL ASPECTS

These technical strategies also raise questions of legality. In the UK, the Computer Misuse Act 1990 (CMA90)[10] includes both a basic hacking offence and an unauthorised modification offence. Any attempt by an active defence to gain unauthorised access to an intruder’s computer would fall foul of the former offence. The launch of a malicious software strike against an intruder’s system by an active defence is covered by the latter offence which carries a penalty of up to five years’ imprisonment and/or an unlimited fine on conviction. Both offences explicitly include transborder modes of operation to facilitate the prosecution of internet-based cybercrime. However, it should be noted that CMA90 does not explicitly cover DoS attacks, except insofar as such attacks can be held to modify the contents of the target computer without prior authorisation. Proposals to remedy this apparent deficiency in CMA90 were made by the Earl of Northesk to the House of Lords in May 2002.[11]

In the USA, the National Information Infrastructure Protection Act 1996 (NIIPA96),[12] which replaced the Computer Fraud and Abuse Act 1986, is broadly comparable in scope with CMA90, except that its later genesis permitted a more explicit coverage of DoS attacks to be undertaken within NIIPA96.

The Council of Europe has produced a report highlighting the problems of criminal procedural law connected with IT which contains recommendations for legal principles on computer misuse.[13] Subsequently the Legal Advisory Board of the European Commission commissioned a study on the legal aspects of computer-related crime in the information society which produced specific legal recommendations for the EU.[14] Still more recently, the Council of Europe has adopted the final version of its Convention on Cybercrime[15] with the aims of harmonising national criminal legislation and facilitating cooperative investigations between member state authorities. Article 6 of this Convention has caused considerable controversy because the sole means of discrimination between the use and the abuse of 'dual use devices' (such as network vulnerability scanners) is ruled to be the purpose for which the devices were primarily designed or adapted, which implicitly entails the legally awkward concept of intent.[16]

The Organisation for Economic Co-operation and Development (OECD) has very recently updated and revised its 1992 international guidelines for the security of information systems and networks.[17] Designed to develop a 'culture of security' among governments and businesses when establishing policies for online transactions (financial or governmental), the guidelines offer nine general but complementary principles: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment. The principle concerning response explicitly advocates the implementation of procedures for rapid and effective cooperation to respond to security incidents, where permissible involving cross-border information sharing and cooperation.

However, in the context of a military conflict between nation states, international law, embodied in the 1945 UN Charter, does not resolve the ambiguities that characterise information warfare activities. In particular, there is no real clarification of the apparent conflict between the notion of sovereign nation states and the reality of global digital networks.[18] Specifically, there is at present no conclusive legal authority for what, if any, information warfare activities would constitute 'armed attacks', 'aggression', or 'force' in international law.

The 4th Geneva Convention of 1949, Convention Relative to the Protection of Civilian Persons in Time of War, affords protection to individuals falling under the jurisdiction of a belligerent, and includes a provision which outlaws collective punishments and reprisals. Whether this would include 'collateral damage' to non-combatants and their vital infrastructures (such as hospitals, power and water supplies) is open to question since the feature of intentionality is absent in this case.

A similar comment applies to Article 17 of the 1950 European Convention on Human Rights (as modified in 1998), which prohibits any state, group or person from engaging in any activity or performing any act aimed at the destruction or limitation of any rights and freedoms set forth in the Convention (except as detailed).[19] The Convention was enacted in the UK as the Human Rights Act 1998,[20] taking force in October 2000, and was subsequently amended by Statutory Instruments 1216, 3644 and 4032 during 2001. It remains to be seen how its provisions, including derogation from Article 5(1) of the Convention, are realised in practice within the setting of developing UK case law.

In the cyber-defence context, it should be noted that the use of 'honey-pots' for enticing or entrapping intruders,[21] in order to determine their identities and monitor their techniques at close range, raises an interesting issue: it is at least possible that the use of a honey-pot might be held to constitute an incitement to commit a criminal act; as such it might render the deployer, rather than the intruder, liable to prosecution.

ETHICAL CONSIDERATIONS

Equally important as the legal issues are the ethical, social, cultural and business implications of reactive countermeasures. 'Strikeback' has come to prominence[22] with the announcement of a report from WarRoom Research Inc. entitled Corporate America's Competitive Edge.[23] Released in January 1999, the report consolidated an 18-month study into cyber-security and business intelligence issues. Of the 320 Fortune-500 companies surveyed, 30 per cent claimed that they had installed software capable of launching counterattacks on security breaches. This appears to be a reaction to companies' previous reluctance to inform law enforcement agencies of security breaches for fear of unwanted public exposure with consequential damage to business confidence. While the companies in the WarRoom survey appeared to view strike-back as a right similar to the use of force in physical self-defence, they did not appear to understand its potential drawbacks.

Under certain circumstances an active defence may retaliate against the wrong individual, or against someone who has made a genuine mistake or is harmlessly curious. In the latter scenario such behaviour might be considered unhelpful or even unethical. The former situation arises as a result of 'protocol spoofing'[24] where an attacker forges the internet protocol (IP) source address of the network packets to make them appear to originate from an authorised user. If the contents of the packets are so constructed by the attacker that the traffic itself appears to contain an attack then the active defence will react.[25] This leads to the unfortunate possibility of dumping a legitimate user who has become the unwitting victim of an 'electronic framing' attack. A false positive flagged against a potential or actual commercial customer is likely to result in a consequential loss of goodwill and/or business. To quote David Curry of IBM, 'the last thing you want is to blow away a legitimate customer'.[26]

Automated and concerted use of strategically contrived false positives and IP spoofing by an attacker may convince a reactive network-based defence that an entire network sub-domain is currently under attack and thereby subvert it into blocking legitimate network traffic, closing innocent network connections, or even shutting down the entire network sub-domain. The resulting denial of service to employees and customers alike could have disastrous consequences for online transaction processing (OLTP) capability and cede a significant advantage to market competitors. The degree to which an organisation chooses to react to a presumed cyber-intrusion must be determined by the organisation's policies and priorities on business continuity (which are linked directly to recovery processing) balanced against its policies and priorities on information security (which are indirectly linked to reaction processing through the perceived need to deter intruders). A reaction strategy that does not emanate directly from such policy considerations is likely to be dangerously flawed.

SUMMARY AND CONCLUSIONS

Verifying that a genuine intrusion incident has indeed occurred can often be extremely difficult. However, the cost of a verification failure will often be very high as well. Thus the risks associated with the occurrence of false positives and false negatives are both potentially high. This situation is one consequence of the asymmetric (or 'unproportionate') nature of information warfare in general, in that cost of defending an asset from attack is many orders of magnitude greater than the cost of attacking it.[27]

As a result, there is a situation in which the legal and ethical or policy-based constraints on the one hand stack up against the technical capabilities on the other. In this situation the prudent reactive option to adopt is one which employs software assisted reaction under human control, in order to minimise the possibility of potentially damaging compromises occurring in security, legality or business ethics.

References

(1) Jajodia, S., McCollum, C. D. and Ammann, P. (1999) 'Trusted Recovery', *Commun. ACM*, Vol. 42, No. 7, pp. 71–75.

(2) Overill, R. E. (1998) 'How Re(Pro)active Should an IDS be?', in Proceedings of the 1st International Workshop on Recent Advances in Intrusion Detection (RAID'98), Louvain-la-Neuve, Belgium (14th–15th September), at www.zurich.ibm.com/pub/Other/RAID/Prog_RAID98/Talks.html#Overill_39

(3) Overill, R. E. (1999) 'Denial of Service Attacks: Threats and Methodologies', *Journal of Financial Crime*, Vol. 6, No. 4, pp. 351–354.

(4) Overill, R. E. (1998) 'Trends in Computer Crime', *Journal of Financial Crime*, Vol. 6, No. 2, pp. 157–162.

(5) Rathmell, A., Overill, R. and Valeri, L. (1997) 'Information Warfare Attack Assessment System (IWAAS)', in Proc. 1st DERA Quadripartite Information Warfare Seminar, London (22nd–23rd October).

(6) Overill, R. E. (1998) 'Intrusion Detection Systems: Threats, Taxonomy, Tuning', *Journal of Financial Crime*, Vol. 6, No. 1, pp. 49–51.

(7) Robinson, C. A. Jr. (1998) 'Make-My-Day Server Throws Gauntlet to Network Hackers', *AFCEA Signal Magazine*, Vol. 52, No. 9, pp. 19–24.

(8) Seffers, G. I. (1998) 'Is Turnabout Fair Play?', *Defense News*, 28th September–4th October, at http://fedcirc.llnl.gov/news/dod-edt.html

(9) Schwartau, W. (2000) 'Can You Counter-attack Hackers?', 7th April, at www.cnn.com/2000/TECH/computing/0407/self-defense.idg

(10) Computer Misuse Act (1990) Chapter 18, at www.legislation.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

(11) Computer Misuse (Amendment) Bill (2002) HL Bill 79, at www.publications.parliament.uk/pa/ld200102/ldbills/079/2002079.htm

(12) Computer Fraud and Abuse Act (1986), National Information Infrastructure Protection Act (1996) 18 USC S1030 at www.usdoj.gov/criminal/cybercrime/1030_new.html

(13) 'Problems of Criminal Procedural Law Connected with Information Technology' (1995) Council of Europe Recommendation No. R(95)13.

(14) Sieber, U. (1998) 'Legal Aspects of Computer Related Crime in the Informatics Society', version 1.0 (1st January) at http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html

(15) 'Convention on Cybercrime' (2001) Council of Europe ETS No. 185, 23rd November, at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

(16) Pounder, C. (2000) 'The Council of Europe Cyber-Crime Convention', *Computers & Security*, Vol. 20, No. 5, pp. 380–383; Carr, I. and Williams, K.S. (2002) 'Draft Cyber-Crime Convention', *Computer Law & Security Report*, Vol. 18, No. 2, pp. 83–90.

(17) 'OECD Guidelines for the Security of Information Systems and Networks' (2002) OECD, 25th July, at www.oecd.org/doc/M00034000/M00034478.doc

(18) Greenberg, L. T., Goodman, S. E. and Soo Hoo, K. J. (1997) 'Information Warfare and International Law', Institute for National Strategic Studies, National Defense University, Washington, DC, ch. 4.

(19) 'Convention for the Protection of Human Rights and Fundamental Freedoms' (1950) Council of Europe ETS No. 5, 4th November, at http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm

(20) Human Rights Act (1998) Chapter 42, at www.legislation.hmso.gov.uk/act/acts1998/19980042.htm

(21) Spitzner, L. (ed.) (2001) *Know Your Enemy*, Addison-Wesley-Longman; Honeynet project at http://project.honeynet.org

(22) Yasin, R. (1998) 'Think Twice before Becoming a Hacker Attacker', at www.infowar.com/hacker/hack_1217998b_j.shtml; 'The Enterprise Strikes Back', at www.warroomresearch.com/MediaPresenSpeak/InterviewIW.htm

(23) 'Corporate America's Competitive Edge' (1999) WarRoom Research Inc., at www.warroomresearch.com/ResearchCollabor/CorpAmerica.htm

(24) daemon9, route, infinity (1996) 'IP Spoofing Demystified', *Phrack Magazine*, Vol. 7, No. 48, File 14, at www.phrack.com

(25) Ptacek, T. and Newsham, T. H. (1998) 'Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection', at www.nai.com/media/pdf/nai_labs/ids.pdf

(26) Power, R. (1998) 'CSI Roundtable: Experts Discuss Present and Future Intrusion Detection Systems', *Computer Security Journal*, Vol. 24, No. 1, pp. 1–18.

(27) Overill, R. E. (2001) 'Information Warfare: Battles in Cyberspace', *Computing & Control Engineering Journal*, Vol. 12, No. 3, pp. 125–128.

***Eur Ing Dr Richard E. Overill**, FBCS, FIMA is Senior Lecturer in Computer Science at King's College London (www.dcs.kcl.ac.uk/staff/richard/), and a member of the Information Assurance Advisory Council (www.iaac.org.uk). His current research focuses on computer-related crime and information assurance, particularly intrusion detection technologies and financial fraud detection using artificial immune systems.*

Guernsey tightens its anti-money laundering regime

The Guernsey Financial Services Commission is consulting on proposed amendments to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations and the Guidance Notes on the Prevention of Money Laundering and Countering the Financing of Terrorism. Most of the changes will enable the Bailiwick to comply with standards set by the International Monetary Fund and the Financial Action Task Force, while others deal with aspects of mail services and issues raised by the Law Officers' Chambers and the Financial Intelligence Service (FIS).

The proposed principal changes to the regulations are for financial services business to:

- have wire transfer procedures as prescribed in the guidance notes;
- ensure that internal reports are made in writing to the reporting officer and that these reports are retained;
- pay special attention to all complex, unusual large transactions or unusual patterns of transactions, or transactions with persons that do not have adequate systems in place to prevent or deter money laundering or the financing of terrorism;
- ensure staff are suitable, adequately trained and properly supervised;
- ensure that where there are foreign branches of a financial services business whose parent entity is based in Guernsey, the provisions of regulation 10 are followed;
- maintain compliance and audit arrangements.

Key recommended changes to the guidance notes include:

- a new section on risk;
- clarification of the point that all staff have a duty to report under the relevant laws, not just key personnel;
- a reminder that financial services businesses must inform the FIS when circumstances change following the earlier submission of a report to the FIS;
- staff training requirements relating to the prevention of money laundering and terrorist financing extended beyond key staff;
- an appendix setting out the Commission's expectations when 'hold mail services' are provided to clients.