How Re(Pro)active Should an IDS be?

Richard E Overill
Department of Computer Science
and
International Centre for Security Analysis
King's College London
Strand
London WC2R 2LS
U.K.
¡reo@dcs.kcl.ac.uk¿

0 Introduction

The classical security paradigm of Protect, Detect, React has traditionally been applied to the field of information security with Firewalls taking on the role of protection while detection is handled by Intrusion Detection Systems (IDS). This admittedly simplistic picture leaves open two questions: who or what should react? and how?

While the role of reaction has traditionally been assumed by the system or network manager, it has become evident that an IDS which operates online and in real-time can also be programmed to behave either reactively or proactively, thus taking on at least part of the manager's role.

The potential behaviour of such 'active defence' IDS raises at least three kinds of issue for consideration: technical issues (what behaviour is possible in practice); legal issues (what behaviour is within the appropriate legal framework); and ethical issues (what behaviour is acceptable in a particular social, business or military context).

1 Technical Possibilities

A 'reactive' IDS could in principle respond to a flagged intrusion on a graduated scale ranging from benign to aggressive; for example, it could *finger* the originator of the suspect process and send them a warning email, terminate the suspect process, disconnect the offending user, modify a router filter list, or even deploy retaliatory malicious software or a denial-of-service reprisal.

A 'proactive' IDS, on the other hand, might not wait to flag an intrusion but would instead take pre-emptive countermeasures; it could, for example, actively interrogate all extant user processes, perhaps using counterfeit Trojan utilities [1], and terminate all those processes which did not originate from *bona fide* users at approved sites [2]. It might even launch a malicious software or denial-of-service attack against such unauthorised users.

There are potential problems with these 'active defence' scenarios. Firstly, unless the IDS detection thresholds are very finely tuned to minimise the occurrence of 'false positives' [3], a reactive IDS may be triggered to disconnect an innocent user by a natural false positive, or coerced to unneccessarily shut down a network connection by a strategically contrived false positive. There is also the possibility of dumping a user who has unwittingly become the subject of an 'electronic framing' attack, involving 'protocol spoofing' of traffic that itself appears to contain an attack [4, 5].

These considerations have recently been sharpened and focussed by the announcement of *Blitzkrieg* [6] from Network Waffen und Munitionsfabriken Group [7]. It is claimed to use self-replicating (Worm-like) and self-repairing (Core Wars) technologies. Two versions of this system have reportedly been developed: an aggressive military version is designed to wage cyberwarfare by launching malicious software attacks against intruders by attempting to damage or destroy information on their computers; a somewhat milder business version attempts to ward off denial-of-service and other common attacks where the intruder's aim is to prevent the operation of a commercial service rather than to destroy data *per se*.

2 Legal Issues

These technical strategies also raise questions of legality. In the UK, the Computer Misuse Act of 1990 (CMA90) includes both a Basic Hacking offence and an Unauthorised Modification offence. Any attempt by an IDS to gain unau-

thorised access to an intruder's computer would fall foul of the former offence; the launching of a malicious software or denial-of-service attack against an intruder's system by an IDS would be covered by the latter offence which carries a penalty of up to 5 years imprisonment and/or an unlimited fine on conviction; it is explicitly a transborder offence. These actions are also illegal in several other EU states and in the USA [8]. The EU Directive on Computer Misuse currently being developed will probably require all member states to enact criminal legislation which covers these actions (amongst others) [9].

However, in the context of a military conflict between nations 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 [10]. 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 and water supplies) is open to question since the feature of intentionality is absent in this case.

In the IDS context, the use of 'honeypots' to attract intruders in order to study their techniques at close range raises an interesting issue: it is at least possible that the use of a honeypot 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.

3 Ethical Considerations

At least as important as the legal issues are the ethical implications. An active IDS may retaliate against the wrong individual, or against someone who has made a genuine mistake or is harmlessly curious. Such behaviour might be considered anti-social at best.

A false positive flagged against a legitimate commercial customer is likely to result in consequential loss of goodwill and/or business. To quote David Currry

of IBM "the last thing you want is to blow away a legitimate customer" [11].

An active network IDS might also be subverted by a strategically contrived false positive into blocking legitimate traffic or closing a specific connection with potentially disastrous consequences in the context of modern battlespace warfare.

4 Summary and Conclusions

Verifying that a genuine intrusion incident has actually occurred can sometimes be extremely difficult. The cost of a verification failure may however be very high.

We should not be seduced by the image of ICE, the Intrusion Countermeasures Electronics (coined by Tom Maddox) in William Gibson's novel *Neuromancer* [12], into imagining that we can completely delegate human responsibility to automated systems in this highly sensitive area. Software-assisted re(pro)action is the realistic limit of what can be safely achieved.

To conclude, a couplet from Robert Frost's poem *Fire and Ice* [13]:

> Some say the world will end in fire,
> Some say in ice.

While we need to ensure that the fire is kept outside our firewalls, we also need to take care that ICE does not cause our downfall.

References

[1] S M Bellovin, There Be Dragons, in *Proc 3rd Usenix UNIX Security Symposium*, Baltimore, MD (September 1992) Ch.27, pp.1–16.

[2] A Rathmell, R Overill and L Valeri, Information Warfare Attack Assessment System (IWAAS), in *Proc 1st DERA Quadripartite IW Seminar*, London (October 1997).

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

[4] T Ptacek and T H Newsham, Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection, (January 1998) at URL http://www.secnet.com/papers/

[5] F Cohen, 50 Ways to Attack Intrusion Detection? *Computer Security ALERT*, No.177 (December 1997)

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

[7] URL http://www.fvg.com/

[8] Computer Fraud and Abuse Act, 18 U.S.C. §1030.

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

[10] L T Greenberg, S E Goodman and K J Soo Hoo, Information Warfare and International Law, Institiue for National Strategic Studies, National Defense University, Washington, DC (1997), Ch.4.

[11] R Power, CSI Roundtable: Experts discuss present and future intrusion detection systems, *Computer Security Journal*, Vol.XIV No.1 (Winter 1998) pp.1–18.

[12] W Gibson, *Neuromancer*, Victor Gollancz (1984), Ch.2.

[13] R Frost, Fire and Ice (1923), *Selected Poems*, Penguin Books (1973).

Biography

Dr Richard E Overill is a Senior Lecturer in Computer Science at King's College London (www.dcs.kcl.ac.uk/staff/richard/), and a member of staff of the International Centre for Security Analysis (www.kcl.ac.uk/orgs/icsa/). His current areas of research are parallel computing, computer-related crime, and computer security, particularly Intrusion Detection Systems. He has published over 50 academic papers.