SCOPE AND DEFINITIONS
The provision of any service requires the utilisation of resources. In a digital context these resources might be processor cycles, memory capacity, disk space or communications bandwidth. A Denial of Service (DoS) attack implies either the removal of those resources by some external event or their pre-emption by a competing process; this should be understood to include rerouting or replacing a service. The sole objective of a DoS attack is thus to prevent the normal operation of a digital system in the manner required by its customers and intended by its designers. As such, DoS attacks on the mission-critical or business-critical infrastructure systems of financial, commercial or other enterprises offer the potential for sabotage, blackmail or extortion operations.

Four general types of DoS attack will be considered here, namely line-of-sight devices, worm programs, flood attacks and subversion of intrusion detection systems.

LINE-OF-SIGHT DEVICES
One recently described line-of-sight device is the HIRF (high-intensity radio frequency) or HERF (high-energy radio frequency) gun which can temporarily disrupt digital circuits at close range (of the order of 1m). A parts list and circuit design for such a device was posted on an Internet bulletin board in 1995 and described at InfoWarCon in 1996; see Figure 1. The device has subsequently been built and tested to demonstrate the veracity of the design.

The EMP (electromagnetic pulse) cannon can permanently damage digital circuits at longer ranges (of the order of 1km) by blasting them with a pulse of microwave energy in the frequency range 0.5–100 gigahertz (GHz). The circuit boards are effectively ‘fried’ by this process, which a US hacker using the handle Dark Tangent has claimed can release 2 megawatts (MW) in 0.001 seconds.

The two devices described above thus have the capability of halting the operation of critical computer systems or communications networks, either temporarily or permanently.

WORM PROGRAMS
Worm programs were originally designed to ‘mop up’ the idle time on a network of computers with useful computations in a manner transparent to the users. The worm program replicates itself in each node of the network and activates a portion of the desired computation if the node is quiescent; if a node becomes busy its computation is suspended and withdrawn.

Malicious worms, however, may simply consume system and network resources by increasing exponentially in numbers until they render the system incapable of performing any useful work whatsoever. This state of ‘electronic gridlock’ represents another form of DoS attack which is no less disruptive to a commercial online transaction processing (OLTP) system than a HIRF gun attack.

The best-known example of a worm-mediated DoS attack occurred in November 1988 when Robert Morris Jr, a student at Cornell University, released a worm program which exploited known defects in the Unix and VAX/VMS operating systems to spread itself swiftly through 6,200 computers on the Internet, bringing them to a standstill for up to a week at an estimated cost of over $100m.
Ritey, an R.F. Jammer.... briefly for those who dont know what the fuck it is..... Its a device that when powered on near a machine such as a Petrol Pump, Fruit Machine, Vending Machines etc.... It will give R.F which will in theory fuck up the workings of the machine... so possible free fuel better odds, etc..... also possible for it to do the opposite, so beware.

Ok this is not the best circuit diagram in the world but if you have any sense, you should get it right.

Ok heres a key & the parts list.

Parts:

- PCB = Vero board or similar
- TR1 = BC547 = This is a transistor !)
- C1 = 330puff = as i call it!
- C2 = 330puff =
- C3 = 5.6puff =
- C4 = 5.6 puff =
- R1 = 2K = this is a Red, Black, Red resistor.
- R2 = 100ohm = this is a Brown, Black, Brown.
- R3 = 100K = this is a Brown, Black, Yellow resistor.
- L1 = Coil of copper wire wound with a diameter of 1/4 inch, only do about 3 turns which should give you a freq of about 130Mhz.

9V DC = either a PP3 or a power supply will do.

Key:

- = Vero board track used.
- = Vero board track
- = Resistor
- = Capacitor and so {s l}
- = Transistor TR1

Make the Antenna out of a length of wire, keep it straight for best results.

Next time ill do a GIF or a coreldraw file.... but for now this will do.

18rs yall

pom 90 21/11/95

Greetz 2: tEQ, Talon, Sonic, MadXn, Dark Heart, Atrocity, Erazor RamRaider, Crash!, Dave X, Raver, Yoder, Slam-Tilt.

Flames 2: All the lame FUCKS who are out to fuck the scene.

You know who you are, and i just dont mean the feds.

Older Generation Hz - False Impressions 441703-SURITA

Response IS alwayS a NICE tHINg - IF YA KEEp mE ON YER TRAVELs MAIL Me!!!
programs are thus potential candidates in sabotage, extortion, or blackmail operations.

**FLOOD ATTACKS**

Flood attacks operate by pre-empting vital system resources using an automated concerted strategy. They may be directed at a modem or PABX (Private Automatic Branch Exchange) dedicated to receiving incoming calls, at a Web-based server performing OLTP, or even at an entire network infrastructure, and work by inundating the target system with vast numbers of spurious calls, messages, requests or enquiries.

Web, mail, telnet and FTP (File Transmission Protocol) servers are notably vulnerable to synchronisation (SYN) flood attacks; the first recorded such attacks on a Web server were directed at the US ISP (Internet Service Provider) Web Communications in December 1997. Essentially, by sending a stream of bogus TCP (Transmission Control Protocol) SYN packets, each requesting the establishment of a synchronised connection, the attacker aims to completely fill up all the available 'slots' allocated by the networking software of the target system for synchronising new TCP connections with entries for 'half-open' connections that are never going to be realised.

UDP (User Datagram Protocol) packet storms in general only affect computers attached to the Internet running some older versions of the Unix operating system (eg SunOS), as such they are no longer considered to be quite such a serious threat as was formerly the case.

ICMP (Internet Control Message Protocol) 'ping' floods can be used to effectively disable a computer attached to the Internet by overloading it with spurious enquiries ('echo requests') as to its current status, each of which requires an individual reply ('echo response'). The 'ping' terminology is derived by analogy with submarine active sonar.

Thousands of US military and NASA computers on the Internet running Windows NT were crashed in March 1998 by hackers who managed to coerce one machine to broadcast an ICMP echo request to all the machines on the target network instructing each of them to broadcast the ICMP echo response to all the others. The term 'Smurf' has been coined to describe this type of attack.

Further details of flood attack methodologies and recommendations for preventative countermeasures are available from the Computer Emergency Response Team (CERT) Advisories and Summaries.

**SUBVERSION OF INTRUSION DETECTION SYSTEMS**

The basic principles and techniques behind Intrusion Detection Systems (IDS) were described by the author at the 15th International Symposium on Economic Crime (Jesus College, Cambridge, 14th–20th September, 1997).

DoS attacks on IDS are founded on the principle of IDS resource exhaustion. If an attacker can identify an IDS processing activity which requires the allocation of a vital system resource, and is able to contrive the occurrence of a situation that consumes all of that resource then a passive IDS will almost certainly 'fail open'. That is, a compromise in the availability of the IDS does not at the same time compromise the availability of the network, thereby allowing the attacker to gain unfettered access to the network.

A reactive network IDS has other vulnerabilities, one of which is its potential for being subverted into becoming the agent of a DoS attack itself. If an IDS with a reactive countermeasure capability is vulnerable to attacks which result in 'false positives' then it can be coerced to react to attacks that did not in reality occur. Thus its built-in countermeasures can be subverted to block access to completely legitimate traffic or to close down perfectly valid connections. Since an attacker can forge (or 'spoof') Internet Protocol (IP) traffic appearing to originate from almost any IP address, the IP address cannot be considered trustworthy; and if the traffic from that address appears to the IDS to contain an attack (ie a deliberately planted false positive) then the IDS will react to it, doing more harm than good. Thus it might be reasonably maintained that, as far as Denial of Service attacks are concerned, far from being a panacea, Intrusion Detection Systems are in fact part of the problem!

**EVALUATION AND CONCLUSIONS**

Over 50 'electronic siege attacks' employing some form of DoS are reported to have been launched against financial institutions and other organisations worldwide since January 1993, with an average extortion demand of about £10m sterling. While HIRF guns have been conjectured as possible tools
for such attacks, automated flood attacks on the modem, PABX or server involved in handling the incoming calls or requests are also plausible weapons for these scenarios.\(^\text{14}\)

Software 'patches' are generally made available quickly for virtually all the known kinds of flood attack; however, in practice they are seldom applied by overbusy system and network managers, thereby leaving businesses unnecessarily exposed and vulnerable.\(^\text{15}\)

Taken together, the inherent potential of line-of-sight devices, worm programs, flood attacks and IDS subversion techniques makes for a current repertoire of Denial of Service attacks which appears to offer the would-be cyber-extortionist or cyber-vandal an effective and attractive range of options.

REFERENCES

(1) InfoWarCon papers available at URL http://www.infowar.com/papers/
(9) Available at URLs http://www.cert.org/advisories/ and http://www.cert.org/summaries/ respectively.
(12) Ibid.
(15) Smith, ref. 8.

Dr Richard E. Overill, FBCS, FIMA 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/icsal). His current areas of research are computer-related crime and Information Warfare, particularly Intrusion Detection Systems. This paper was given at the 16th International Symposium on Economic Crime, Jesus College, Cambridge, 13th–19th September, 1998.

CORRUPTION

Police Corruption

Tony Williams

'Power tends to corrupt and absolute power corrupts absolutely.' (Lord Acton)

Before considering anti-corruption operations it would be helpful if the role of the Police Complaints Authority were briefly outlined. It is an independent body established by Act of Parliament — the Police and Criminal Evidence Act 1984 — to oversee complaints by members of the public against police officers in England and Wales. There are just 12 members, supported by 60 civil servants seconded from various government departments. The members are all full time and come from a wide variety of backgrounds.

The Authority covers 49 police forces in England and Wales and has three main functions: to supervise the investigation of the most serious complaints against police officers; to supervise inquiries into non-complaint matters voluntarily referred by forces because of their potential gravity — most