Trick of the net fends off hackers

BARRY FOX

HACKER attacks designed to bring down websites for days or weeks on end may have met their match, if an idea being patented by IBM can be made to work.

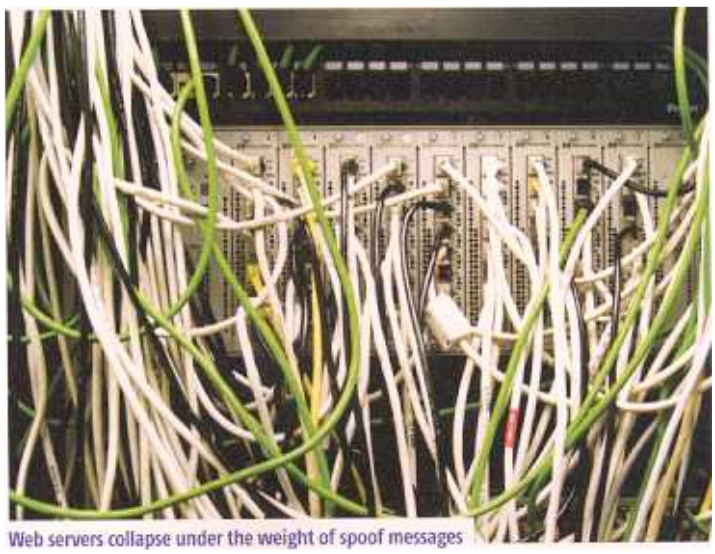
In what is called a distributed denial of service (DDoS) attack, the hacker infects a large number of PCs with a virus that at a given moment tries to contact the target website. This synchronised bombardment ties up the website and effectively forces it offline.

DDoS attacks exploit the internet's "three-way handshake". When working normally, a browser trying to contact a site begins by sending a page request. The site responds with a message to the browser acknowledging the request, and the browser completes the handshake with a final acknowledgment message. If one of these stages fails, the request is abandoned, but it cannot expire immediately, otherwise a slight delay on the net would prevent connections being established.

In a DDoS attack, the virus arranges for the browser to send a phoney address, so when the site sends its acknowledgment to that address it doesn't get a response. When tens of thousands of virus-infected PCs ask for pages simultaneously, the targeted website becomes swamped with half-open connections and is paralysed. As long as infected PCs continue sending spoofed requests faster than connections can expire, the site will be crippled. Shutting down open connections more quickly might be one answer, but this risks cutting off legitimate requests.

IBM's plan for defeating DDoS attacks is twin-pronged. First, it makes a web server continually monitor delays on the internet, known as its "latency", by checking the time stamps in all messages coming in and out. All messages which do not complete the handshake within the current latency time have their connections cut off, as they are likely to be spoof requests.

"A single global wave of denial of service attacks could cost companies $1 billion"



Web servers collapse under the weight of spoof messages

The second line of defence is to continually change, according to a secret pattern, the data ports on the servers that the browsers can connect to. This pattern is only sent to a browser after it has completed the handshake – and proved itself to be legitimate. Connections switch between ports at a speed which suits the internet latency at any given moment: slowly if the net is highly congested, and fast if traffic is moving quickly.

DDoS attackers cannot keep connections open long enough to swamp the site because their connections are disconnected faster than new requests arrive. Legitimate requests hop ports when they complete the handshake and remain connected.

The damage DDoS attacks can do became apparent in January this year, when the website of software house SCO effectively disappeared after the MyDoom computer worm bombarded it with demands for its home page for a full two weeks. According to D. K. Matai of London-based cyber security analyst Mi2g, a global wave of DDoS attacks could now easily cost $1 billion. ●

CUTTING EDGE

I'M WORKING LATE...AT THE CIRCUS

Ever wanted to disguise where you are when answering a call on your cellphone? Romanian company Simeda has software to place you where you'd like to be. The program, called SounderCover (try it at www.simeda.com/soundercover.html), comes with nine background sounds, including a traffic jam, roadworks, a dentist's surgery and the circus. There is even the sound of another phone ringing, so you can get rid of an unwanted caller by telling them you are wanted on the landline. The first versions will work on selected Nokia phones.

BEACH BALL CONQUERS SOUTH POLE

A giant beach ball could be the next rover used to explore the Martian polar caps. NASA's Jet Propulsion Laboratory recently completed the toughest tests yet on its Tumbleweed Rover, a ball 2 metres in diameter and stuffed with electronics.

In its eight-day mission it rolled around the Antarctic polar plateau for 70 kilometres, gathering meteorological information in one of the harshest environments on Earth. It measured temperature, pressure and position, and transmitted the figures back to JPL in Pasadena via the Iridium satellite phone network. Measurement instruments, radio transmitters, a GPS receiver and batteries are suspended inside the ball (http://robotics.jpl.nasa.gov/~behar/southpoletw.htm).

The rolling rover travelled at up to 16 kilometres per hour during tests, in -30 °C. But unusually gentle winds meant the rover stopped long before its target of 200 kilometres.

EXOSKELETON LIGHTENS LOADS

The exoskeleton used by Sigourney Weaver in the *Alien* movies came a step closer to reality this week. The Berkeley Lower Extremity Exoskeleton (BLEEX) made its debut at a defence symposium in Anaheim, California. It is part of a military project designed to allow foot soldiers to carry heavy loads over long distances (*New Scientist*, 10 November 2001, p 32). Wearers strap on the 45-kilogram robotic legs and a backpack that contains its gasoline engine and control system (http://me.berkeley.edu/hel/bleex.htm).

In tests, a volunteer carrying a 32-kg pack plus the 45 kg exo said it felt as if they were carrying a mere 2 kg, according to project leader, Homayoon Kazerooni of the University of California, Berkeley. The aim now is to increase the maximum pack load to 55 kg.