Seeking to tighten the Net against attack

July 11 2006

As more users switch to broadband internet access, security providers are playing a frantic game of 'catch-up' to secure networks against the many threats. While new menaces are always just around the corner, one project believes it may have part of an answer to one of the most common and destructive forms of intrusion.

The IST-funded DIADEM Firewall project has developed a novel and comprehensive security solution for secure broadband services, focusing on denial of service attack and mitigation, thanks to collaboration between a consortium of interested stakeholders from France Telecom, Polish Telecom, IBM Research, Imperial College London, University of Tübingen, Groupe des Ecoles des Télécommunications and Jozef Stefan Institute.

A distributed denial-of-service attack (or DDoS attack) attacks computer

systems or networks and usually results in a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the system. The attack typically uses thousands of compromised home and business computers (or zombies) to bring down corporate systems, often as part of a blackmail attempt.

How big a problem is it? Well, DDoS attacks affected over 13 per cent of businesses in the United Kingdom at a cost of more than £558m in 2004 alone, according to the UK's National Hi-Tech Crime Unit (NHTCU). The malicious data traffic can also significantly degrade the broadband experience for residential internet users, and impose dramatic network and customer support costs on broadband service providers. With broadband penetration projected to increase significantly in the coming years, that figure is likely to increase exponentially.

"There is no doubt that denial-of-service attacks are a growing issue as more and more services, such as online games, IP telephony, television over IP and e-shopping are provided to broadband users through the internet," explains Yannick Carlinet, project coordinator of DIADEM Firewall. "It is a crucial and vulnerable aspect of broadband security and will become even more so in the future as more users move over to broadband connections," he adds.

A distributed detection and reaction system

To strike back at the broadband bandits, the DIADEM Firewall partners opted to develop a distributed detection and reaction system located in the network and managed by the network operator. As Carlinet notes, this is already a radical move away from the current approach where end users are responsible for their own online security.

"The current security paradigm requires all end-users to organise and

manage the security of their own terminals. This has many shortcomings and the failure of such an approach has been demonstrated too often in recent times for it to be considered a viable solution," he says.

The DIADEM Firewall solution, by contrast, puts the focus back on the network provider. "Our overall goal was to develop and deploy innovative network components that enable service providers to offer to their customers secure broadband services in an effective and cost-efficient way," says Carlinet.

The project's approach combines flexible implementation techniques for high-speed packer processing, advanced algorithms for intrusion detection and policy-based techniques for automated configuration and decision-making.

This included designing and implementing an innovative architecture for provider-controlled distributed high-speed edge devices, thereby paving the way towards the next generation of distributed high-speed broadband firewalls with policy-based control. The project team also succeeded in developing and deploying enhanced techniques capable of detecting and reacting to a wide range of security violations, in particular detecting DDoS attacks, but also suitable for detecting and identifying other types of malfunctioning.

"Functional and performance tests are taking place right now and we are optimistic that we'll be able to show substantial progress over the state-of-art intrusion and prevention systems," he says.

The need to tackle strategic issues

Indeed, technical issues are the least of the worries facing DIADEM Firewall as the project seeks to convince the key network players that they need to be proactive in ensuring the security of their broadband

services.

“I think the main difficulties that need to be overcome now are strategic,” says Carlinet. “We need business units of Internet Service Providers (ISPs) and network operators to take account of the paradigm shift in security matters that is currently taking place, such as the transition from uncoordinated end-terminal security management to distributed network security policies.”

While operators may be somewhat resistant to the idea of change, they recognise nevertheless the commercial value of DIADEM Firewall solution, adds Carlinet.

“Discussions are ongoing with France Telecom and Polish Telecom business units with regard to commercial exploitation of our solution. We are also in contact with some application-level packet processor manufacturers that are interested in our approach.”

Other follow-ups are also planned to build on the sterling work achieved by the project. “There are a number of collaborative projects that have recently started and there is also the likelihood of future project proposals, for instance to extend the DIADEM solution to cope with internet worms,” concludes Carlinet. “There are also various internal projects by the individual partners and discussions with manufacturers for the implementation of functions designed in the project in commercial products.”

Source: IST Results