Super firewall aims to stop DDOS

European researchers build Diadem Firewall, which uses data filtering and intrusion prevention to detect rogue activity

By Jeremy Kirk, IDG News Service

July 13, 2006

Computer researchers in Europe are developing a new prototype architecture for halting distributed denial-of-service (DDOS) attacks, where a barrage of traffic is directed at a Web site or server to shut it down.

The Diadem Firewall deploys both hardware and software on the edge of a provider's network rather than within, said Georg Carle, chair of the computing and Internet department at the University of Tübingen in Germany.

Diadem uses data filtering and intrusion prevention technologies to detect rogue activity, then coordinates an automatic reaction based on policies, Carle said. Current firewalls don't incorporate policies into their capabilities, he said.

When suspicious behavior is detected, a network can then cut off certain computers that appear to be violating policies, such as a machine that suddenly consumes a dramatically higher amount of bandwidth, Carle said.

Diadem could prove worthy in the fight against DDOS attacks, which often involving thousands of hacked computers across the Internet working in concert to attack another machine. The attacks are often hard to trace.

Cybercriminals have used DDOS attacks as a threat, particularly against online gambling sites expecting a rush of business around a sporting event, to extort businesses. Those criminals often control networks of computers they have commandeered through software faults of computers connected to the Internet to carry out the attack.

"The significant number of non-protected equipment connected to the Internet provides a very fertile ground for the recruitment of new agents and the automation of the attacks," according to the Diadem Web site.

The project, which started in 2004, was budgeted at €3 million (US$3.8 million) and received funding in part from the Information Society Technologies, a European Union organization that coordinates IT programs. It has been extended for three more months, Carle said.

Diadem hasn't resulted in a product but rather a group of technologies that could be employed in different ways, Carle said. The project mandate called only for a prototype, and France Télécom SA and Polish Telecom are expected to begin testing Diadem by September.

Diadem could be particularly effective for Internet Service Providers (ISPs) who have peered, meaning they have directly connected with one another to reduce the cost of moving data traffic.

Carle said both ISPs could share a common policy using Diadem, strengthening their effectiveness with a coordinated reaction to DDOS attacks.

"A large distributed denial-of-service attack may emerge from many different providers," Carle said.

Those involved in the Diadem Firewall include France Télécom's R&D department, the University of Tübingen in Germany, IBM Corp.'s Zurich Research Laboratory, Imperial College London, Groupe des Ecoles des Télécommunications in France, Jozef Stefan Institute in Slovenia and Polish Telecom.