



Ashley has come up with strategies for making the protection of websites cheaper and more effective

SEDUCING HACKERS TO BOLSTER WEB SECURITY

During the turmoil following the recent disputed Iranian elections, computer activists worldwide rendered the official website of President Ahmedinejad inaccessible on several occasions. They did so by bombarding the website with so many trivial requests that its ability to respond became overloaded. This technique is known as distributed denial of service (DDoS).

DDoS is fast becoming a standard weapon not only of cyber-warfare, but also of computer blackmail. Attacks on prominent websites such as Yahoo, Amazon and eBay have already cost those companies hundreds of thousands of dollars in business.

How to defend against DDoS is what Deakin computer scientist Ashley Chonka has been studying for his PhD. Using information and chaos theory, he has come up with at least three different strategies for making the protection of websites cheaper and more effective. "Websites can be designed to be resistant," he says, and countermeasures can be taken when an attack is mounted.

"Computer scientists are very interested in this topic, partly because the internet service providers and software companies themselves don't focus on security, which is concerning," he says. "They seem to think building in security features will diminish the functionality of their products."

In order to test his model defences, Ashley decided he had to generate real DDoS attacks. "Genuine DDoS data is very hard to come by, because internet service providers and computer companies don't want to talk about attacks, and won't release information about them."

So he collected internet traffic data by means of what is known as a honeypot – a website specifically established to lure malicious hackers into attacking it. "In our analysis of the data we have been looking for different ways to distinguish between malicious and legitimate traffic," Ashley says. "Our research works in conjunction with the Australian Honeypot Project, which collects and maintains a variety of malicious attack programs."

As a result, Ashley now has several useful datasets, which he hopes to make available through the web to researchers worldwide to use in their own studies.

Ashley's research is supported by two Geelong businesses: Belmont Computer Centre and Sunet Corporation.

FURTHER INFORMATION:

School of Information Technology
Principal supervisor: Professor Wanlei Zhou
E: wanlei.zhou@deakin.edu.au
www.deakin.edu.au/scitech/it