Researchers simulate cyber soldiers for sale

October 26 2010

(PhysOrg.com) -- Researchers, who are mimicking the debilitating attacks of cyber robot armies to help defend the Australian and Indian governments, will discuss their work tomorrow (October 27) at Queensland University of Technology (QUT).

Dr Desmond Schmidt, from QUT's Information Security Institute (ISI), said infected home computers, called bots, could unknowingly be harbouring malicious software which had the ability to turn the humble PC into a soldier for sale on the cyber black market.

Dr Schmidt is taking part in the $5 million, three-year Australia-India project Protecting Critical Infrastructure from Denial of Service Attacks, which is investigating internet-based attacks designed to overload government and corporate websites with traffic and information, and prevent them from operating.

"This can bring services, such as water and electricity, to a halt and shut down military and other government websites. It's almost like terrorism," Dr Schmidt said.

"By simulating these 'denial of service' (DoS) attacks on a test bed, we can investigate how they affect computers and software, and develop tools for mitigating and defending against the threat."

Dr Schmidt will discuss his work at ISI Day, an institute event featuring its latest research tomorrow, October 27 in Brisbane.

He has worked with Indian and Australian researchers to create a test bed with computers and servers in which different types of DoS attacks could be let loose to discover their effect in a supervised environment.

"It's difficult to monitor a computer or program under attack because its systems shut down, but we've created tools that can track what happens in detail," he said.

Dr Schmidt said governments around the world were concerned about the effects DoS attacks could have on their services.

He said that DoS attacks could involve millions of bots, or zombies. These zombies were typically ordinary home computers infected with malicious software, usually without the knowledge of their owners.

"Behind these zombies are controlling machines, and well-hidden behind these are the people directing them," he said.

"Those in control of the zombies may threaten businesses or governments with attack for extorting money, they may offer the network of zombies for sale, or undertake attacks for a range of malicious reasons."

Dr Schmidt said significant DoS attacks had already taken place in several locations, including in Georgia, where an attack, thought to have originated from Russia, brought the nation's websites to a halt.

He said the ISI test bed was one of only a few in the world, and for safety reasons it was isolated from the internet.

It can be reconfigured to simulate various types of attack, including stealth attacks that transmit only small amounts of carefully crafted data, but which can still have a devastating effect on services.

Provided by Queensland University of Technology