Denial of service denial: New filtering system could protect networks from zombies

September 30 2009

A way to filter out denial of service attacks on computer networks, including cloud computing systems, could significantly improve security on government, commercial, and educational systems. Such a filter is reported in the *Int. J. Information and Computer Security* by researchers from Auburn University in Alabama.

Denial of Service (DoS) and distributed Denial of Service (DDoS) attacks involve an attempt to make a computer resource unavailable to its intended users. This may simply be for malicious purposes as is often the case when big commercial or famous web sites undergo a DDoS attack. However, it is also possible to exploit the system's response to such an attack to break system firewalls, access virtual private networks, and to access other private resources. A DoS attack can also be used to affect a complete network or even a whole section of the Internet.

Commonly, attack involves simply saturating the target machine with external internet requests. In the case of a DDoS attack the perpetrator recruits other unwitting computers into a network and uses a multitude of machines to mount the attack. The result is that the resource, whether it is a website, an email server, or a database, cannot respond to legitimate traffic in a timely manner and so essentially becomes unavailable to users.

Methods for configuring a network to filter out known DoS attack software and to recognize some of the traffic patterns associated with a mounting DoS attack are available. However, current filters usually rely

on the computer being attacked to check whether or not incoming information requests are legitimate or not. This consumes its resources and in the case of a massive DDoS can compound the problem.

Now, computer engineers John Wu, Tong Liu, Andy Huang, and David Irwin of Auburn University have devised a filter to protect systems against DoS attacks that circumvents this problem by developing a new passive protocol that must be in place at each end of the connection: user and resource.

Their protocol - Identity-Based Privacy-Protected Access Control Filter (IPACF) - blocks threats to the gatekeeping computers, the Authentication Servers (AS), and so allows legitimate users with valid passwords to access private resources.

The user's computer has to present a filter value for the server to do a quick check. The filter value is a one-time secret that needs to be presented with the pseudo ID. The pseudo ID is also one-time use. Attackers cannot forge either of these values correctly and so attack packets are filtered out.

One potential drawback of the added layer of information transfer required for checking user requests is that it could add to the resources needed by the server. However, the researchers have tested how well IPACF copes in the face of a massive DDoS attacks simulated on a network consisting of 1000 nodes with 10 gigabits per second bandwidth. They found that the server suffers little degradation, negligible added information transfer delay (latency) and minimal extra processor usage even when the 10 Gbps pipe to the authentication server is filled with DoS packets. Indeed, the IPACF takes just 6 nanoseconds to reject a non-legitimate information packet associated with the DoS attack.

More information: "Modelling and simulations for Identity-Based Privacy-Protected Access Control Filter (IPACF) capability to resist massive denial of service attacks" in *Int. J. Information and Computer Security*, 2009, 3, 195-223

Source: Inderscience Publishers (news : web)