Self-learning security system for computer networks

July 9 2009

Cyber attacks on computer networks are becoming increasingly commonplace. To counter the threat, they are protected by so-called network intrusion detection systems. But these fail to identify some attacks, or do not spot them until it is too late. To improve matters, Damiano Bolzoni of the University of Twente (The Netherlands) has developed a system which paves the way for a new generation of network security. This forms the subject of his doctorate, awarded by the Faculty of Electrical Engineering, Mathematics and Computer Science on 25 June.

A network intrusion detection system (NIDS) is like a kind of virus scanner, but for an entire network rather than a single computer. There are two types. The first draws upon a database of all known attacks, such as those attempted by computer hackers. It works by recognizing the 'signatures' of methods previously used. But this means that it will not at first spot a new and as yet unknown method.

The second kind of NIDS uses anomaly detection. In other words, it learns how the network is normally used and if it spots a deviation from this standard pattern it will alert the system administrator so that the suspected attack can be investigated. In practice, however, this type is not widely used because no really good systems are yet available commercially.

Bolzoni has been trying to change that by developing a new anomaly detection NIDS, which he has named SilentDefense. His system is based

upon self-learning algorithms, which make it far more accurate than existing systems of this kind. Moreover, the chance of 'false positive' alerts is about 1000 times lower than in the systems currently available.

The system is now being further developed by SecurityMatters, the company recently founded by Bolzoni and fellow researchers Emmanuele Zambon and Sandro Etalle. They expect to launch SilentDefense commercially in mid-2010.

In Bolzoni's view, the ideal NIDS is not of one type or the other but combines the two. For that to be possible, however, a good system based upon anomaly detection first needs to become available.

Provided by University of Twente (news : web)