



Network Vulnerability Analysis

Background

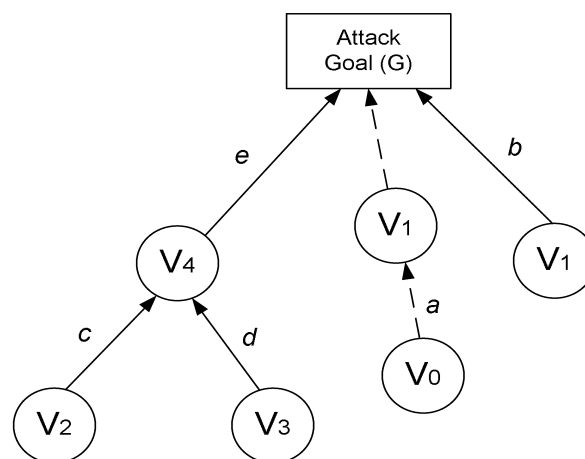
Network security is becoming more and more important as people spend more and more time connected. Compromising network security is often much easier than compromising physical or local security, and is much more common.

Administrators of large networks typically use network analysers or network monitors to identify threats to the network so that mitigation strategies can be implemented. These are mostly graph-based methods that generate attack trees (or graphs which show modes of hacking into the network) to cover all possible sequences of vulnerabilities. These become very cumbersome as the size and complexity of networks increase.

New System

A new method for network vulnerability analysis has been developed by Swinburne researchers in the Centre for Advanced Internet Architectures. Their method directly analyses and eliminates less critical vulnerabilities without building the actual attack graph. In other words, it is a top down approach in contrast to existing methods which are a bottom up approach, resulting in a significantly more efficient analysis by focusing on the priority areas which can do most damage.

The patent-pending tool can be used to identify security issues and to improve/compare network security for any computer network.



Market

The target market for this system is network administrators wishing to keep their network secure or to improve network security.

Opportunity

The Swinburne researchers are building industry alliances to further develop and implement this new system. They are keen to broaden the base of development partners, or investors.

Further information

Dr Bruce Whan

Director, Swinburne Knowledge

Swinburne University of Technology

T: +613 9214 5979

E: bwhan@swin.ed.au

W: www.swinburne.edu.au/knowledge

