Realtime Identification and Prevention of Network Attacks

Delio Brignoli

Allied Telesis plans to support and develop its current range of commercially sold security applications through the development of new algorithms or a new system design that has the capability and flexibility to detect and prevent a wider range of computer network attacks.

Current methods of security involve perimeter security; however there has been a general trend towards developing a new more holistic approach to network security that does not simply look at attacks through specified perimeters but takes a zone based approach. Current firewalls developed by Allied Telesis provide extensive detection securities however new attacks and attack methodologies are always being developed. Hence steps must be taken to develop new systems and techniques to mitigate these attacks.

This project involves initially understanding and then testing contemporary technologies employed (both theoretically and physically with real data) to identify and prevent network attacks. Using this information will aid in the development and thoroughly test a new algorithm or system that will withstand an extensive range of attacks. This is more speculative or leading edge research to develop technology currently outside mainstream firewall technology.

This work in this project takes a more exploratory approach in determining attack detection and prevention. The new algorithm or methodology developed will be integrated into Allied Telesis’ hardware security products and applications as a sentry feature making new devices less susceptible to attack and provide greater reliability. A successful new system derived from this project will propel Allied Telesis to the forefront of these new technologies.