Institute for Integrated and Intelligent Systems (IIIS) and School of Information and Communication Technology (ICT)

Is pleased to present the **SEMINAR** on

"Man-in-the-Middle and Wormhole Attacks in Wireless Networks"

**Steve Glass**

**Time**  11.00am - 1.00pm  
**Date**  Friday 18th September 2009  
**Venue**  G05 3.43 Gold Coast campus Griffith University.

**Abstract:**  The man-in-the-middle attack represents one of the most difficult problems in network security. In this attack the legitimate users of the network communicate with each other via a hostile adversary but without their knowledge or consent. The man-in-the-middle attack puts the hostile adversary in complete control of communications and they are able to inject, delay, modify, delete and re-order message traffic as they see fit. Such attacks have been successfully deployed to bypass authentication mechanisms, cryptographic defenses and cause widespread loss of service in the network.

In this presentation we will discuss a variant of the man-in-the-middle attack known as the wormhole attack. Wormholes pose a very serious threat to the integrity of wireless sensor networks, mobile ad hoc networks and wireless mesh networks. In these attacks the man-in-the-middle connects geographically distant points in the network and tunnels traffic between these points. Such an attack can have a significant effect on the network topology and lead to large scale network outages. We will discuss some of the countermeasures including protocols devised by the author to detect and prevent man-in-the-middle and wormhole attacks.

**Bio:**  Steve Glass is a NICTA-sponsored PhD candidate studying the problems of securing wireless networks. Prior to his PhD studies Steve worked in industry with IBM, Experian and Marconi in fields as varied as telecommunications network management, credit reference and operating system security. He obtained his first degree and Masters degree with the Open University in the UK.