



Assured Information Security, Inc.

245 Hill Road
Rome, NY 13441

Press Release

June 27, 2007

For Immediate Release

Assured Information Security, Inc. Hosts Presentation at Griffiss Institute

On Friday, June 29th, at 10 am, Assured Information Security, Inc. will host two presentations at the Griffiss Institute, 725 Daedalian Drive, Griffiss Business & Technology Park, Rome. Dr. John Marsh from Assured Information Security, Inc. presenting on malicious cryptography and Paul Ratazzi from AFRL presenting on information assurance and wireless networks. The event is open to the public.

Here are summaries of the presentations:

1. Exploiting the Physical Layer for Wireless Network Security

Presenter: Paul Ratazzi, Principal Engineer AFRL

Abstract:

Wireless network security is especially challenging due to the fact that communication is done on a shared medium - the airwaves. Activities counter to all aspects of information assurance, including availability, confidentiality, integrity, authentication, and non-repudiation are much easier to engage in when network traffic is accessible beyond the normal physical boundaries that protect our wired networks. This talk will explain how the physical layer, normally considered to be a liability for wireless networks, can be leveraged to form a very strong foundation for a comprehensive defense in depth strategy. In some cases, a wireless network that takes advantage these security enhancements, unique to the wireless realm, can be more secure than its standard wired counterparts.

2. Malicious Cryptography

Presenter: Dr. John Marsh

Abstract:

This short talk will review the book "Malicious Cryptography" by A. Young and M. Yung (Wiley, 2004). Topics to be covered include the application of asymmetric cryptography for cryptoviral attack, the importance of random numbers in cryptography, and subliminal channels. Some specific topics that will be touched upon include symmetric vs. asymmetric cryptography, the one-half virus, computational intractability, provably secure pseudo-random number generators (such as Blum-Blum-Shub), Santha and Vazirani's entropy extraction algorithm, the Von Neumann unbiasing algorithm, and the Trotter-Johnson unranking algorithm.

###