

**THURSDAY
FEBRUARY 7, 2008**

**Scaife Hall Auditorium
Room 125**

4:30 p.m.
Refreshments—4:00 p.m.

VIRGIL GLIGOR
CARNegie MELLON
UNIVERSITY



Virgil D. Gligor received his B.Sc., M.Sc., and Ph.D. degrees from the University of California at Berkeley. He has been at the University of Maryland between 1976 and 2007. He is currently a Professor of Electrical and Computer Engineering here at Carnegie Mellon University. He is an Editorial Board member of the ACM Transactions on Information System Security, and several IEEE Transactions (i.e., Dependable and Secure Computing, Computers, and Mobile Computing).

Over the past three decades, his research interests ranged from access control mechanisms, penetration analysis, and denial-of-service protection to cryptographic protocols and applied cryptography.

He was awarded the 2006 National Information Systems Security Award jointly given by NIST and NSA in the US for his contributions to security research.

ECE Seminar Hosts:
Radu Marculescu,
radum@ece.cmu.edu
Yi Luo,
y1827@andrew.cmu.edu
Bruno Sinopoli,
brunos@andrew.cmu.edu

Handling New Adversaries in Wireless Ad-hoc Networks

A common threat in many wireless ad-hoc networks is the capture of network devices by an adversary. Stajano's "big stick principle," which states that whoever has physical control of a device is allowed to take it over, suggests that such an adversary is substantially more powerful than the traditional Dolev-Yao and Byzantine adversaries, and hence difficult to counter. Protecting device secrets (e.g., cryptographic keys) via physical security mechanisms, which currently range from those employed by smartcards (very little tamper resistance), to IBM 4764 crypto co-processors (highest FIPS 140 evaluation), and to Physically Unclonable Functions (very good but not perfect physical security) will continue to require network security measures. I argue that "good-enough" measures in the face of node capture by adversaries can be obtained by using emergent properties. Intuitively, these are properties that cannot be provided by individual network nodes -- no matter how well-endowed nodes might be -- but instead result from interaction and collaboration among multiple nodes. Such properties can be used to detect, often probabilistically, the presence of an adversary within a network and to pinpoint with reasonable accuracy the affected network area (e.g., identify a specific captured node, a particular property of captured nodes). I illustrate a new simple probabilistic protocol that avoids the effects of node capture by detecting adversaries' attempts to access a node's internal state. I will also present several research directions that could lead to better network protection against a variety of new attacks such as those launched by an insider.