



## Fall 2009 CIS Colloquium Series

# Ethical Hacking and Information Security

**Robert Lai**

(Science Application International Corporation (SAIC))

*11am-Noon, Thursday, Sept. 17, 2009*

*Tuttleman 300AB*

**Abstract:** According to data in the latest edition of the IT Skills and Certifications Pay Index published by Foote Partners, Certified Ethical Hacker (CEH) certification pay was up 40% in the last quarter of 2008. The demand for ethical hacking or penetration testing is growing. Ethics is the key differential factor to define black-hat hacker and white-hat hacker. Programming is an art; hacking is a dark art. Understand the malicious hacker's mindset will make it easier to counter the attack. Skill profile of ethical hacking will be briefed during the presentation.

According to 2009 Data Breach Investigations Report by the Verizon Business RISK Team, 285 million records were compromised in 2008. The actual financial lost due to the leaks is hard to quantify, but the average data breach cost per record is \$202.00 in 2008. In summary, these security breaches are due to: (1) insecure software architected, designed, developed, and deployed; (2) improper or inadequate configuration of software security control; (3) unsatisfactory physical security control; (4) lack of layered security defensive measures at the perimeter, hosts, and applications; and (5) insufficient data protection during transit or at rest. The convergence of computer and Internet brings the benefit of faster information exchange for commerce, communication, entertainment, education, finance, and health care than ever before. Unfortunately, the dark side of the explosive internet revolution comes with cyber security that has an impact not only on the individual, but also on society since the critical infrastructure of the U.S. that includes the financial network, communication, the internet, Supervisory Control and Data Acquisition System (SCADA) controlled water and power grids, and the defense network are vulnerable to cyber attack. Sun-Tzu's first principle has stated, "warfare is the greatest affair of state, the basis of life and death, the Way (Tao) to survival or extinction. It must be thoroughly pondered and analyzed." Security should be implemented throughout the software development life cycle (SDLC) as built-in instead of add-on.

**Bio:** Robert Lai, CISSP-ISSAP, ISSEP, CAP, CEH, CSSLP is an Information Systems Security Professional with broad knowledge of cyber security, security test and evaluation, and penetration testing. Mr. Lai works as an Information Assurance Engineer for the Landforce Operation of Science Application International Corp (SAIC), which he is responsible as service integration lead of Network Management System, Cross Domain Solution, and Information Assurance for the Army's Future Combat Systems. He is a frequent item writer for the CAP, CISSP, CSSLP, ISSAP, and ISSEP certification exams. He was one of the contributors who were instrumental in developing the Certified Secure Software Lifecycle Professional (CSSLP) certification. Since 2008, he has been the chairperson of the scheme committee for EC-Council (certification body of Certified Ethical Hacker).

*Refreshments will be served!*