Seminar Series
Computer Science

Early Adopters: A Model for Correlating Internet Web Browsing With Compromise Events

Alex Kent, Los Alamos National Labs

Sep 11th Tuesday, 12:30 to 1:30pm

209 Comp. Sci. Bldg.

Abstract - Downloading information content from the Internet is a primary activity for most networked computers and it provides a basis for behavior characterization and association to malicious activity. Using web traffic (HTTP) logs, aggregated antivirus detection logs, and information security incident response tickets from Los Alamos National Laboratory's network over a six month period involving over 24,000 computers and almost 4 million unique Internet content locations, this talk will present an analysis of Internet web surfing behavior in combination with detected malicious activity. The talk will then present a model of risk behavior based on the concept of early and independent adopters of content from the Internet showing a useful and novel correlation between potential computer compromise and Internet access behavior.

Brief Bio - Alex Kent is a research scientist at Los Alamos National Laboratory (LANL); his work is primarily focused on applied cyber security research, including distributed intrusion detection systems, dynamic trust models, authentication systems, and ethology-inspired cyber defense models. Alex was previously the program director responsible for LANL's non-Department of Energy (DOE) cyber security work and the director of LANL's Advanced Computing Solutions (ACS) organization, centered on solving current and forward-looking cyber security problems with a cross-disciplinary and applied R&D emphasis. Prior to ACS, as deputy division leader over LANL's computing, telecommunications, and networking organization, Alex was responsible for overseeing the Laboratory's site-wide classified and unclassified IT environments, services, and security, including LANL's computer incident response capability. Alex has led and developed a number of high-impact, successful LANL cyber security projects, including an integrated physical-cyber security protection system, a USB-port protection system, a heterogeneous network host quarantine system, and a scalable two-factor authentication system. Alex has been a member of the technical staff at LANL since 1997, working in areas relating to cyber security and IT management. He is also an adjunct staff researcher with the Institute for Defense Analysis at the Center for Computing Sciences. Alex has been presented with three Distinguished Performance Awards for his various technical contributions and has also received a patent for work in network authentication. He is currently a PhD Candidate at New Mexico Tech.