Improving cyber attack detection through computer modeling

November 30 2012

A new study shows computer network security analysts are not prepared for drawn out cyber attacks.

Cyber attacks that have long caused major work disruption and theft of private information are becoming more sophisticated with prolonged attacks perpetrated by organized groups. In September 2012, Bank of America, Citibank, the New York Stock Exchange, and other financial institutions were targets of attacks for more than five weeks. Defense Secretary Leon E. Panetta warned that the United States was facing the possibility of a "cyber-Pearl Harbor" and was increasingly vulnerable to foreign computer hackers who could disrupt the government, utility, transportation, and financial networks.

Key to protecting online operations is a high degree of "cyber security awareness," according to human factors/ergonomics researchers Varun Dutt, Young-Suk Ahn, and Cleotilde Gonzalez. In their *Human Factors* article, "Cyber Situation Awareness: Modeling Detection of Cyber Attacks With Instance-Based Learning Theory (http://bit.ly/VjVs7M)," they developed a computer model that presented 500 simulated cyber attack scenarios to gauge simulated network security analysts' ability to detect attacks characterized as either "impatient" (the threat occurs early in the attack) or "patient" (the threat comes later in the attack and is not detected promptly). Their model was able to predict the detection rates of security analysts by varying the analysts' degree of experience and risk tolerance as well as an attacker's strategy (impatient or patient attack).

The authors found that experienced, risk-averse analysts were less accurate at detecting threats in patient than in impatient attacks. "In a patient attack, when the attacker waits until the end to generate threats, the experiences in the analyst's memory that indicate an attack" are not as readily retrieved, says Dutt, which "makes it difficult to correctly detect patient attacks."

"Application of our results include the design of training tools that increase competency and the development of decision-support tools that improve defenders' on-the-job performance in detecting cyber attacks." The authors suggest that employers evaluate an analysts' risk tolerance before employment and/or manipulate tolerance levels during training to better identify threats.

As cyber warfare strategies and tactics evolve, the authors plan to further investigate the trend of drawn-out attacks and new intrusion detection software.

Provided by Human Factors and Ergonomics Society