An Approach to Incorporating Uncertainty in Network Security Analysis

Submitted by David Nicol on Tue, 03/07/2017 - 9:23pm. Contributors: Hoang Hai Nguyen Kartik Palani David M. Nicol

ABSTRACT: Attack graphs used in network security analysis are analyzed to determine sequences of exploits that lead to successful acquisition of privileges or data at critical assets. An attack graph edge corresponds to a vulnerability, tacitly assuming a connection exists and tacitly assuming the vulnerability is known to exist. In this paper we explore use of uncertain graphs to extend the paradigm to include lack of certainty in connection and/or existence of a vulnerability. We extend the standard notion of uncertain graph (where the existence of each edge is probabilistically independent) however, as significant correlations on edge existence probabilities exist in practice, owing to common underlying causes for dis-connectivity and/or presence of vulnerabilities. Our extension describes each edge probability as a Boolean expression of independent indicator random variables. This paper (i) shows that this formalism is maximally descriptive in the sense that it can describe any joint probability distribution function of edge existence, (ii) shows that when these Boolean expressions are monotone then we can easily perform uncertainty analysis of edge probabilities, and (iii) uses these results to model a partial attack graph of the Stuxnet worm and a small enterprise network and to answer important security-related questions in a probabilistic manner.

Hoang Hai Nguyen is a graduate student in the Department of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign (UIUC). Before joining UIUC, he was a software engineer at the Advanced Digital Sciences Center, a Singapore-based research center established and led by UIUC. His research interest is in the modeling and analysis of computer networks and networked control systems with the primary focus on cyber-security.

Kartik Palani is a second year graduate student in Computer Engineering at the University of Illinois at Urbana-Champaign, advised by Prof. David Nicol. He is affiliated to the Trustworthy Cyber Infrastructure for the Power Grid group and the Information Trust Institute at the Coordinated Science Laboratory. He also works closely with Prof. Sean Smith and his students at the Trust Lab at Dartmouth College. His research focuses on security for the smart power grid and the Internet of Things. He works on developing scalable security architectures for these critical applications. Being a systems engineer by heart he has a particular affinity towards designing and building reliable and secure large scale systems.

David M. Nicol is Professor of Computer and Electrical Engineering at the University of Illinois, Urbana-Champaign, and Director of the Information Trust Institute. Previously he held faculty positions at the College of William and Mary, and Dartmouth College. His research interests include high performance computing, simulation modeling and analysis, and security. He was elected Fellow of the IEEE, and Fellow of the ACM for his contributions in these areas. He is co-author of the widely used textbook "Discrete-Event Systems Simulation", and was the inaugural awardee of the ACM Special Interest Group on Simulation's Distinguished Contributions Award, for his contributions in research, teaching, and service in the field of simulation.