Quantitative Evaluation of Security Metrics

William H. Sanders
Department of Electrical and Computer Engineering, Information Trust Institute, and Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
whs@illinois.edu

ABSTRACT

Making sound security decisions when designing, operating, and maintaining a complex system is a challenging task. Analysts need to be able to understand and predict how different factors affect overall system security. During system design, security analysts want to compare the security of multiple proposed system architectures. After a system is deployed, analysts want to determine where security enhancement should be focused by examining how the system is most likely to be successfully penetrated. And when several security enhancement options are being considered, analysts would like to evaluate the relative merits of each. In each of these scenarios, quantitative security metrics should provide insight on system security and aid security decisions. Quantitative metrics enable ranking the alternatives to determine the best option. Quantitative assessments of system security are also valuable for risk management trade-off decisions.

In this tutorial, we first survey existing approaches for quantitative evaluation of system security. These include NIST's Risk Management Guide for Information Technology Systems, Attack Graphs, and privilege graphs, among others.

The tutorial then describes an approach that we have developed called the ADversary VIew Security Evaluation (ADVISE) method. To provide insight on system security and aid decision-makers, ADVISE quantitatively evaluates the strength of a system's security. To do this, the ADVISE method aggregates security-relevant information about a system and its adversaries to produce a quantitative security analysis useful for holistic system security decisions.

The ADVISE method for system security analysis consists of three main phases. Phase one is the characterization of the system and its adversaries and the specification of the desired security metrics. Phase two is the generation of a dynamic executable security model created from the characterization information in phase one. Phase three is the execution of the security model generated in phase two. Quantitative security metrics are produced as model outputs. This approach makes four contributions:

- a precise adversary characterization format that enables simulation of how a particular adversary is likely to attack a system,
- a precise system characterization format that describes the possible attack paths into a system and includes security-relevant system details,
- simulation algorithms for computing adversary attack decisions and the probability that an attack attempt will be successful, and
- executable models that produce mission-relevant quantitative security metrics.

In addition to describing an approach for modeling a system and its advisories, we argue the importance of modeling the behavior of the users of the system when quantitatively evaluating security. In particular, we describe a methodology and framework for system analysis and modeling that can identify key human decisions and quantify their effects on overall security system security. This approach is illustrated through two case studies to provide insights into cyber security system performance trade offs. A simple case study illustrates how to analyze system security using the method. A tool is currently under development to facilitate this methodology.

ACKNOWLEDGMENT

This is joint work with Robin Berthier, Robert Cain, Douglas Eskins, Ken Keefe, Elizabeth (Van Ruitenbeek) LeMay, Carol Muehrcke, Simon Parkin, Donald Parks, Willard Unkenholz, and Aad van Moorsel.

BIOGRAPHY

William H. Sanders is a Donald Biggar Willett Professor of Engineering, the Director of the Information Trust Institute, and the Director of the Coordinated Science Laboratory at the University of Illinois. He is a professor in the Department of Electrical and Computer Engineering and Affiliate Professor in the Department of Computer Science. He is a Fellow of the IEEE and the ACM. He is currently the Director and PI of two centers at Illinois, the NSF/DOE/DHS Trustworthy Cyber Infrastructure for the Power Grid (TCIP) Center, and the DOE/DHS TCIPG Center, aimed at making the power grid resilient to attacks and failures. He is a co-developer of three tools for assessing computer-based systems: METASAN, UltraSAN, and Mobius.