

Network Security Analysis Using Attack Graphs

Anoop Singhal
Computer Security Division, NIST
Gaithersburg, MD 20899, USA
Email: anoop.singhal@nist.gov
Phone: 301-975-4432

Lingyu Wang and Sushil Jaodia
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444, USA

At present, computer networks constitute the core component of information technology infrastructures in areas such as power grids, financial data systems and emergency communication systems. Protection of these networks from malicious intrusions is critical to the economy and security of our nation. Having a standard way to measure network security will bring together users, vendors and researchers to evaluate methodologies and products for network security.

In the past, there has been some progress in standardizing security metrics such as those by NIST. However, a widely accepted metrics for network security is still unavailable. Typical issues currently addressed in the area of network security are:

- Topological Vulnerability Analysis
- Network Hardening
- Attack Response

The current focus is on qualitative aspects rather than a quantitative study of network security. To measure the overall security of a network one must first understand the vulnerabilities and how they can be combined to construct an *attack*. Recent advances using *attack graphs* can be used to measure quantitatively the security of a network. Instead of measuring individual vulnerabilities and then wondering about their combined effect, we can now measure the overall security of a network based on the context provided by the attack graph. Our vision is that *attack graphs* can be used to measure the damage that can be caused by an attack, the cost of reconfiguration and the amount of resistance to an attack. Network hardening and attack response will be guided by the pursuit of an optimal solution in terms of available metrics, rather than using an arbitrary solution.

This research is based on our experience with attack graph generation and analysis. Central to the framework are two types of composition operators that correspond to the case of serial and parallel connectivity between hosts. It is our belief that our research will lead to both theoretical results and practical advances in the design of network security metrics. It will also have a positive impact on the study of vulnerability analysis, network hardening and attack response.

References

1. L. Wang, C. Yao, A. Singhal and S. Jajodia, Interactive Analysis of Attack Graphs using Relational Queries, In *Proceedings of 20th IFIP WG 11.3 Working Conference on Data and Application Security (DBSEC 2006)*, pages 119-132, 2006.
2. L. Wang, A. Singhal and S. Jajodia, Measuring the Overall Security of Network Configurations Using Attack Graphs, Accepted for Publication In *Proceedings of 21st IFIP WG 11.3 Working Conference on Data and Application Security (DBSEC 2007)*