

Automated Generation and Analysis of Attack Graphs

O. Sheyner*, J. Haines**, S. Jha ***,
R. Lippmann**, J. M. Wing *

*CMU, ** MIT Lincoln Laboratories,
***U. Wisconsin

Presented by: Maria Calle

Information Assurance
PhD Seminar – Summer 2006

Overview

- Authors created and implemented a technique for Attack Graph Generation
- Attack graph represents all possible attacks in the network
- Manually is tedious, error prone and impractical for hundred nodes* or more
- Two techniques to help decide cost-effectiveness of attack protection

2

Definitions

- Network is a finite state machine
- State transitions are atomic attacks
- Path in the graph is a series of atomic attacks, leading to bad state
- Technique is:
 - Exhaustive: covers all possible attacks
 - Succinct: contains only network states from which the intruder can success
- Desired security property (no root access). Intruder wants to violate this property
- Graph is produced with a modified version of NuSMV (software for formal verification of finite state systems: ITC (Istituto Trentino di Cultura) and CMU)
- Network may be represented using XML

3
