UNIVERSITÉ Concordia UNIVERSITY

Concordia University ENCS Engineering & Computer Science

M.A.SC. THESIS EXAMINATION

CONCORDIA INSTITUTE FOR INFORMATION SYSTEMS ENGINEERING

Notice of Thesis Defence

TO: Faculty, Graduate Students, Guests

FROM: Dr. A. Hammad, Graduate Program Director,
Concordia Institute for Information Systems Engineering

DATE: February 18, 2009

You are invited to attend the following M.A.Sc. (Information Systems Security) thesis examination:

Candidate: **Tao Long**

Thesis Title: **Attack Graph Compression**

Date & Time: Friday, March 6, 2009 @ 2:00 P.M.

Location: EV003.309

Examining Committee:

Dr. Z. Tian	Chairman
Dr. L. Wang	Supervisor
Dr. B. Zhu	CIISE Examiner
Dr. D. Qiu	External Examiner (ECE)

ABSTRACT:

Attack graph has emerged as a useful tool for defending against multi-step network attacks involving correlated vulnerabilities. However, most current representations of attack graphs are not scalable. Even the attack graph of a reasonably large network is usually incomprehensible to the human eyes. For realistic networks with tens of thousands of hosts and hundreds of vulnerabilities, even computing the attack graph may become infeasible. On the other hand, an attack graph of a real-world network usually has much redundancy due to the presence of hosts with similar configurations, such as those in an office or computer lab. To our best knowledge, existing work can at best hide such scalability issues through visualization techniques but cannot remove the redundant information, which does not comprise real solutions. This thesis presents a scalable representation of attack graphs for removing such redundancy. The representation is based on a well known compression technique, namely, reference encoding. We start with simple cases where hosts have identical connectivity and vulnerabilities. We then study more realistic cases where hosts may have different connectivity and vulnerabilities. We show that in some cases small differences are better hidden in textual rules while in other cases the differences are better handled by leaving the involved hosts outside the compression model. To evaluate the proposed compression model, we will describe a case study and show experimental results based on random network topologies generated by existing tools. Both results confirm that our model can significantly reduce the complexity of attack graphs.