THE UNIVERSITY OF TULSA

THE GRADUATE SCHOOL

HYBRID ATTACK GRAPHS FOR MODELING CYBER PHYSICAL SYSTEMS SECURITY

by

George Robert Louthan IV

A thesis submitted in partial fulfillment of
the requirements for the degree of Master of Science
in the Discipline of Computer Science

The Graduate School
The University of Tulsa

2011

THE UNIVERSITY OF TULSA

THE GRADUATE SCHOOL

HYBRID ATTACK GRAPHS FOR MODELING CYBER PHYSICAL SYSTEMS SECURITY

by
George Robert Louthan IV

A THESIS

APPROVED FOR THE DISCIPLINE OF

COMPUTER SCIENCE

By Thesis Committee

______________________________, Chairperson
John C. Hale

____
Mauricio Papa?

____
Peter Hawrylak?

ABSTRACT

George Robert Louthan IV (Master of Science in Computer Science)

Hybrid Attack Graphs For Modeling Cyber Physical Systems Security

Directed by John C. Hale

7 pp., Chapter 1: Conclusions

(75 words)

As computer systems' interactions with the physical world become more pervasive, largely in safety critical domains, the need for tools to model and study the security of these so-called cyber physical systems is growing. This thesis presents extensions to the attack graph modeling framework to permit the modeling of continuous, in addition to discrete, system elements and their interactions, to provide a comprehensive formal modeling framework for describing cyber physical systems and their security properties.

ACKNOWLEDGEMENTS

Thanks to Evan Mackay and my family for their constant support.

More acknowledgments go here.

This material is based on research sponsored by DARPA under agreement number FA8750-09-1-0208. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, or DARPA or the U.S. Government.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

CHAPTER 1

INTRODUCTION

1.1 Introduction

As computer systems become pervasive across a variety of domains, not only are their interactions with people becoming more frequent; computer systems are also increasingly interacting with the physical world and with each other.

1.2 Hybrid Systems

Systems that include both continuous and discrete components are termed *hybrid systems*. When linked together with a significant network component, these systems are sometimes called *cyber physical systems*, which have been targeted as a key area of research. Such systems are becoming pervasive in safety-critical domains such as medical, critical infrastructure, automotive, and others, and their security is an important area of research and the topic of this thesis.

1.3 Modeling Frameworks

Existing frameworks for modeling and analysis of computer networks are inappropriate for use in these systems because of their inability to capture the continuous domain. Likewise, existing methods for studying hybrid systems fall short when it comes to modeling the sometimes complex networks that are hallmarks of cyber physical systems.

1.4 Scope

This thesis presents an extension of the attack graph modeling framework, typically used for studying network security, into the continuous domain to enable it to be used for studying cyber physical systems.

The remainder of this thesis is structured as follows. Chapter 2 provides background in hybrid systems and their modeling methods, introduces past work in attack graphs, and presents a set of case studies in both the hybrid and discrete domains to be used throughout this work. Chapter 3 introduces in detail the basic attack graph framework to be used as the basis for the hybrid extensions. Chapter 4 introduces the extensions themselves. Chapter 5 delivers some results from this modeling methodology, and Chapter 6 draws conclusions and suggests further work.

CHAPTER 2

BACKGROUND

2.1 Hybrid Systems

2.2 Attack Graphs

2.3 Case Studies

CHAPTER 3

ATTACK GRAPHS

3.1 Definition

3.2 Working Lexicon

3.3 State Predicates

3.4 State Aggregation

CHAPTER 4

HYBRID EXTENSIONS

4.1 Introduction

4.2 Definition of New Syntax

4.3 Time

4.4 Time State Aggregation

CHAPTER 5

RESULTS

CHAPTER 6

CONCLUSION AND FUTURE WORK