T H E   U N I V E R S I T Y   O F   T U L S A

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

9 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

LIST OF TABLES

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.

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. This thesis is concerned with modeling the security of these systems and their interactions with each other and the physical world.

1.2 Modeling Frameworks

An excellent argument that touches on the need for new research directions in modeling cyber physical systems is due to Lee in a 2006 position paper in the National Science Foundation Workshop on Cyber-Physical Systems, a prelude to the NSF's research initiative on cyber physical systems:

> Cyber-Physical Systems (CPS) are integrations of computation with physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect compu- tations and vice versa. In the physical world,

> the passage of time is inexorable and concurrency is intrinsic. Neither of these properties is present in today's computing and networking abstractions. [2]

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; they also lack a robust, let alone "inexorable" notion of time. 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.

1.3 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 goal is to combine the best of both worlds: hybrid systems modeling frameworks, particularly hybrid automata, which best describe systems in relative isolation; and computer network security modeling frameworks, particularly attack graphs, which excel at capturing the complex interrelationships and interdependencies between assets and attacks.

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 Cyber Physical Systems

2.1.1 Hybrid Systems

A system with both continuous (frequently physical) components and discrete (frequently digital) components is said to be a *hybrid system*, named for its characteristic blending of the two domains. Examples of hybrid computer systems abound in industrial controls, for example, although hybrid systems may also be fully physical (e.g., a bouncing ball experiences continuous behavior when rising and falling and discrete behavior when colliding with a surface).

The term hybrid system is an older one that was coined as researchers began to study the newly pervasive reactive systems that arose as programmed control of the physical world became widespread. [1] For several reasons it does not suffice to describe precisely the types of systems with which this work is concerned: a subset of hybrid systems that incorporate a significant computer and networking component.

Nevertheless, the modeling of hybrid systems is well studied and provides a sufficient body of relevent knowledge from which to draw to warrant its inclusion. This chapter includes background on a particularly relevent modeling framework for hybrid systems called the hybrid automata, which is used in this thesis as the standard benchmark against which to compare hybrid modeling techniques.

2.1.2 Cyber Physical Systems

A newer, better term for the systems investigated in this thesis is *cyber physical systems*. Put simply, a cyber physical system is a networked hybrid system: a networked computer system that is tightly coupled to the physical world.

The term arose in 2006 when the National Science Foundation identified cyber physical systems as a key area of research.

2.1.3 Hybrid Automata

A valuable formalism for modeling hybrid systems in isolation

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

BIBLIOGRAPHY

[1] R. Alur, C. Courcoubetis, T. Henzinger, and P. Ho. Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems. *Hybrid systems*, pages 209–229, 1993.

[2] E.A. Lee. Cyber-physical systems-are computing foundations adequate. In *Position Paper for NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*. Citeseer, 2006.