Overview of the Afternoon

Session 1 (2:30 – 3:30): STPA-Sec
Overview – STPA within Secure Systems Engineering (and Cyber Security)
• Introduction
• Observations on Cybersecurity today
• System Thinking and Security
• STPA-Sec overview
• Summary and Conclusion

Session 2 (3:30 – 5:00): STPA-Sec Practice
• Overview
• Concept Analysis
• Architectural Analysis
• Design Analysis
• User Q&A
• Summary and Conclusion

To Maximize the Available Time, I Will Assume Basic Familiarity With STAMP, STPA and Will Leverage John Thomas’s Example from this Morning
System-Theoretic Process Analysis for Security (STPA-SEC):
Secure Systems Engineering, Cyber Security and STPA

William Young Jr, PhD

2019 STAMP Conference
Boston, MA

March 25, 2019
Disclaimer:

The views expressed in this presentation are are those of the presenters and do not reflect the official policy or position of the United States Air Force, Department of Defense, Air Combat Command, MIT Lincoln Laboratory, Syracuse University, or the U.S. Government
Introduction
Introduction

- Losses are growing and current approaches to securing complex, software intense, designed physical systems do not appear to be working as well as desired

- Origins of losses fall into at least one of two categories:
  - Disruption prevents engineered system from fulfilling its designed purpose
  - Disruption does not necessarily prevent the engineered system from fulfilling its primary purpose, but it produces an unacceptable “by-product”

- The side with individuals best able to conceptualize the most creative ways to exploit device/designed system functionality has competitive advantage (tactics)
Introduction

Design = Secure System Engineering
Construction = Secure System Development
O & M = Protect Data and IT Components

Ref: System Engineering For Intelligent Transportation Systems

Current Approaches Do Not Address Safety & Security Errors that lead to Losses When it is Most Effective and Cheapest to Do So
Observations on Cybersecurity

Today
Threat Based Approach to Developing a “Secure” Architecture

Threat Modeling

Security Policy / Requirements

Select Security Mechanism / Controls

Current Security Analysis Depends on Identifying the Right Threat (Tactics), But Does Not Help Address the Larger Mission Assurance Goal (Strategy)

Ref: (Anderson, 2010; Shostack, 2014; Swiderski & Snyder, 2004)

William.Young.3@US.AF.Mil  WYOUNG@MIT.EDU  © Copyright William Young, Jr, 2019
Schneier’s Attack Tree Model is the Intellectual Foundation of Most Thinking on Cybersecurity

“Clearly, what we need is a way to model threats against computer systems. If we can understand all the different ways in which a system can be attacked, we can likely design countermeasures to thwart those attacks...Security is not a product - it's a process. Attack trees form the basis of understanding that process.”

Schneier Based His Security Attack Trees on Fault Trees He Saw Used for Safety

Ref; Dr. Dobb's Journal, December 1999

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU © Copyright William Young, Jr, 2019
Cybersecurity Through Today’s Analytic Lenses

The System Vulnerabilities are Driven by Threat Capability
Current Security Analysis

“When you ask an engineer to make your boat go faster, you get the trade-space. You can get a bigger engine but give up some space in the bunk next to the engine room. You can change the hull shape, but that will affect your draw. You can give up some weight, but that will affect your stability. When you ask an engineer to make your system more secure, they pull out a pad and pencil and start making lists of bolt-on technology, then they tell you how much it is going to cost.”

- Prof Barry Horowitz, UVA
What We Need to Get to

“The first thing we need in this process is the ability to state computer security requirements clearly and precisely... so that a competent professional can study it for a reasonably short amount of time and, say, "Oh, yes, I agree. If you build that particular system to that particular requirement, it's secure enough for that particular purpose."

- Donald Good "The Foundations of Computer Security, We Need Some"
SYSTEM THINKING & SECURITY
Relooking Schneier’s Words

“Clearly, what we need is a way to model threats against computer systems. If we can understand all the different ways in which a system can be attacked, we can likely design countermeasures to thwart those attacks...Security is not a product -- it's a process. STPA-Sec will form the basis of understanding that process.”

STAMP and STPA-SEC Provide us a Different Way to Understand (and Control) the Security Process
Cyber Security Through Different Analytic Lenses

In Systems Engineering, Threats are Just One of Many Trades

William.Young.3@US.AF.Mil  WYOUNG@MIT.EDU  © Copyright William Young, Jr, 2019
New Approach: Secure Form Simply Realizes Secure Function

• “Form follows function” is a central tenant of system engineering and architecture

• Generate secure Business & Mission Systems by first defining the secure functionality to be realized

• Get to security via
  • Identify functionality required to solve the problem at hand (But we must understand problem)
  • Implement all required functionality securely based on understanding problem and context

• Architecture Defined (Crawley)
  • The embodiment of concept, and the allocation of physical/informational function to elements of form, and definition of interfaces among the elements and with the surrounding context
New Approach: Secure Form Simply Realizes Secure Function

• “Form follows function” is a central tenant of system engineering and architecture

• Generate secure Business & Mission Systems by first defining the secure functionality to be realized

• Get to security via
  • Identify functionality required to solve the problem at hand (But we must understand problem)
  • Implement all required functionality securely based on understanding problem and context

• Architecture Defined (Crawley)
  • The embodiment of concept, and the allocation of physical/informational function to elements of form, and definition of interfaces among the elements and with the surrounding context

We Can Use STAMP Model to Help Craft the Security Concept
STAMP Model & Security

• Focuses on function, not threat to guide realization (form)
  • Separates problem space from solution
  • Allows us to reason about function (and critique a proposed functional decomposition based on security related concerns)
• Provides a means to define and specify secure function clearly, unambiguously, and in context of the mission
• Functional Control Structure is simply a means to help envision how the necessary functionality can be implemented in a way that prevents losses identified
"Security" Losses Can Be Reframed as (Functionality) Control Problems

**Cause a Mid Air Collision**
- Process Model
- Control Algorithm

- Aircraft must maintain minimum safe separation

**Cause Friendly Fire Loss**
- Process Model
- Control Algorithm

- Only hostile forces must be engaged

**Steal Customer PII**
- Process Model
- Control Algorithm

- PII must only be exposed to authorized entities

ENFORCE: Safe Separation
ENFORCE: Engagement Rules
ENFORCE: Data Access Policy
From Systems Analysis to Secure Systems Analysis

“A systematic examination of a problem of choice in which each step of the analysis is made explicit wherever possible.”


Secure Systems Analysis

Systems Analysis

Security Engineering

Systems Engineering

STPA-Sec Allows the Systems Analysis Framework to be Applied to Security
STPA-Sec

• Analysis process to generate a security concept and framework

• Examines a functional process through a security lens to gain insights and craft artifacts to enable additional reasoning

• Threats are just another environmental hindrance to function
  • In fact, the threats themselves don’t really matter…it’s the functional disruption they can deliver
  • We can engineer our systems to handle the most important functional disruptions

• Analysis methodology supports learning and facilitates stakeholder debates and trades (can imagine “what might be”)
STPA-Sec Extends STPA

- Synthesize (frame) the security problem
- Define purpose of the analysis
- Model the Control Structure
- Identify unsafe/unsecure control actions
- Step 2: Identify loss scenarios
- Wargame
Summary and Conclusion

• Security engineering and underlying systems thinking offers an alternative to address the challenge and bring strategy to bear.

• Growing realization that security engineering must begin before architecture development...but we need a Security Engineering Analysis methodology:
  • All analysis is based on models, so we require a model of how losses occur.
  • Default model today is “threats cause our security-related losses” (but we don’t generally get to control the threats).

• STPA-Sec applies the STAMP model to provide a methodology to place security within a systems engineering context:
  • Define “secure” functionality.
  • Guide the development of an architecture to realize the functionality.
  • We DO get to control our systems engineering.

We Must Ensure That We Are Defining and Solving the Right (Engineering) Problem.
Concluding Thoughts from Sun Tzu

The opportunity to secure ourselves against defeat lies in our own hands.

The supreme art of war is to subdue the enemy without fighting.

Strategy without tactics is the slowest route to victory.
Tactics without strategy is the noise before defeat.
My Contact Information

WYOUNG@MIT.EDU – Personal Email
William.Young.3@US.AF.Mil – Government Email
(for 6 more months)