SYNOPSYS®
Silicon to Software™

Threat Modeling Primer

Dan Lyon
Senior Principal Consultant
dlyon@synopsys.com

Agenda

- Why Security is a Systems Problem

- Introduction to Threat Modeling
  - Understanding and Decomposing the system
  - Modeling Assets
  - Modeling Controls
  - Modeling Threat Agents
  - Interpreting the Model

About Me

- Lead Embedded Consulting Practice
- Industry Participation
  - AAMI TIR 57 – Medical Device Security Risk Management
  - FDA and MITRE panels and working groups
  - CTA CEB33 co-chair Consumer Electronics – Security Program and Implementations
  - IEEE Center for Secure Design –
    - Building Code for Building Code
    - Automotive Secure Design
  - SAE and RTCA
- Prior to Synopsys
  - 18 years in product development building complex systems
  - Software, Systems and Security Engineering
  - DFSS Green Belt; Black Belt
- Industry Experience
  - Past Certifications: GSEC, GCIA, GCIH, GWAPT, GMOB, GCPM

Security Is A Systems Problem

Systems Engineering Owns Security

- Security is an emergent property
- Complexity creates emergent properties
- Complexity is managed by SE
- Therefore, Security is managed by SE
- SE most efficiently addresses

MITRE

NIST Special Publication 800-160

Initial Public Draft

Systems Security Engineering

An Integrated Approach to Building Trustworthy Resilient Systems

SYNOPSYS®

Introduction to Threat Modeling

What Is Threat Modeling?

Threat modeling (TM) is software design analysis that looks for security weaknesses by juxtaposing software design views against a set of threat agents:

- Identifies secure-design weaknesses
  - Missing security controls
  - Weak or inappropriate security controls
  - Potential vulnerabilities
- Finds weaknesses that cannot be found by other techniques
- Does not replace penetration testing, secure code review, or any other security activity

All models are wrong, but some are useful.

- George Box

Threat Modeling Vocabulary

Approaches to Threat Modeling

- Attack trees
- Microsoft Security Development Lifecycle
- Synopsys

Common theme … find flaws … potentially think outside of your comfort zone

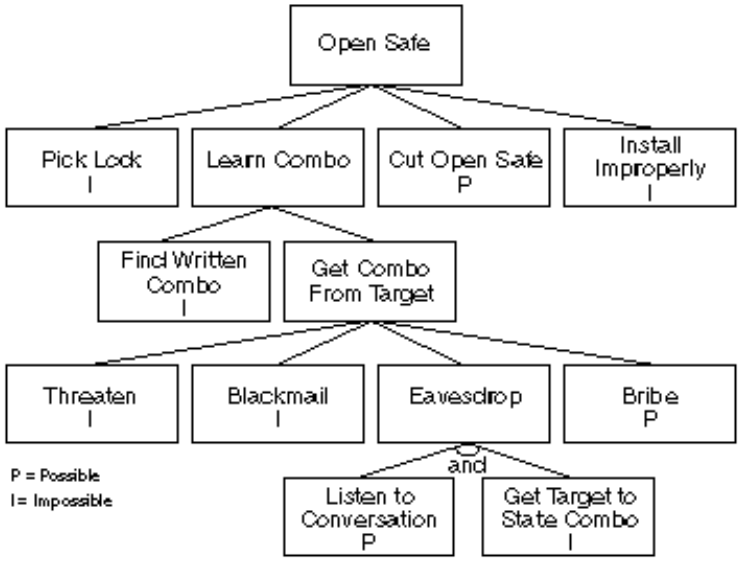
Attack Tree

- An attack tree has a root node, child nodes, and leaves
- Root node is the goal, or a component prompting the analysis
- Child nodes are refinements of the goal
- Leaf nodes are attacks that satisfy the condition described by the parent node
  - Sometimes **any** leaf node will satisfy the condition (OR)
  - Sometimes **all** leaf nodes will satisfy the condition (AND)

Attack Tree

Simple attack tree example from 1999 Schneier paper

– https://www.schneier.com/academic/archives/1999/12/attack_trees.html



Microsoft SDL

Microsoft's threat modeling methodology:

- One of cornerstones of Microsoft Security Development Lifecycle (SDL) that promotes its performance at design phase of the software development process
- Is highly dependent on data-flow analysis
- Uses the STRIDE risk categorization
  - Based on the fact that attackers interact with their targets via data
  - Therefore, understanding system entry points, exit points and internal data flows critical to identify vectors leading to potentially vulnerable system components

Microsoft provides a free, extensible, threat modeling tool.

STRIDE

- STRIDE is a risk categorization scheme:
  - **S**poofing
  - T**a**mpering
  - R**e**pudiation
  - I**n**formation Disclosure
  - D**e**nial of Service
  - E**s**calation of Privilege

- STRIDE is a subcomponent of Microsoft's threat modeling methodology—often confused with the methodology itself

Synopsys Threat Modeling Process

Threat Modeling Process

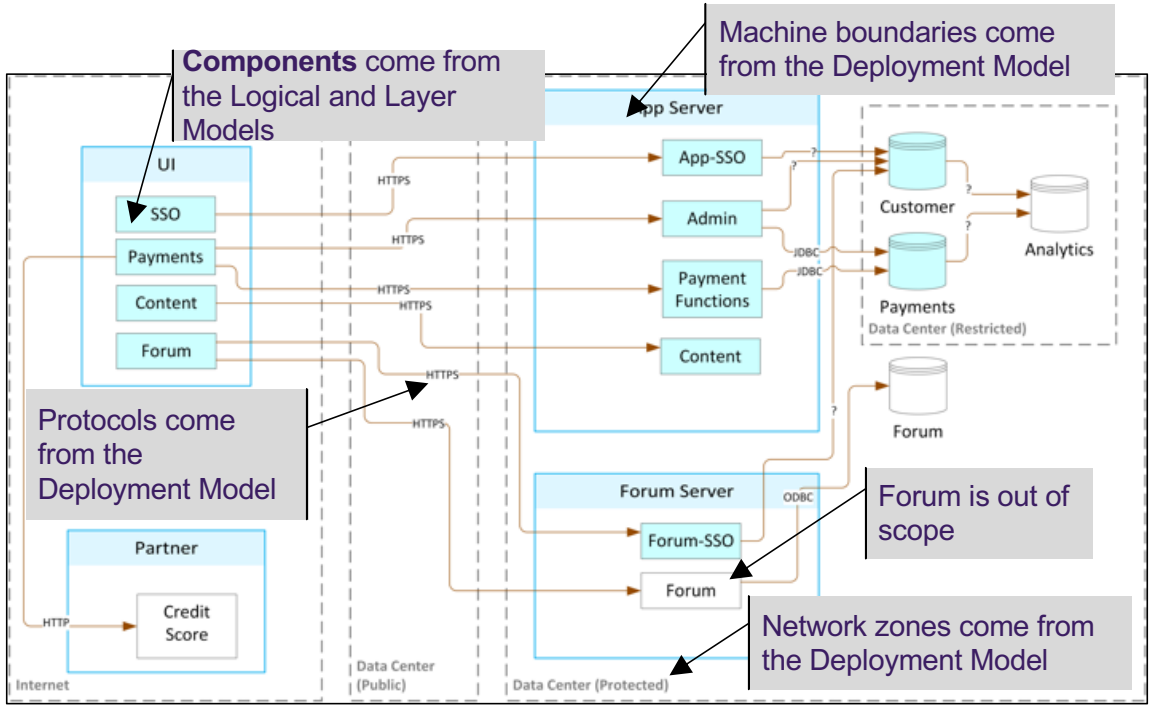
Threat modeling process includes the following steps:

- Define scope and depth of analysis
- Gain understanding of what is being threat modeled
  - Decompose and model the software
- Model the attack possibilities
  - Identify assets, security controls, and threat agents
  - Juxtapose attack possibilities and software model
- Interpret the threat model
  - Produce a list of attacks
- Create the traceability matrix for reporting the attacks
  - Propose mitigations

Decompose and Model the System

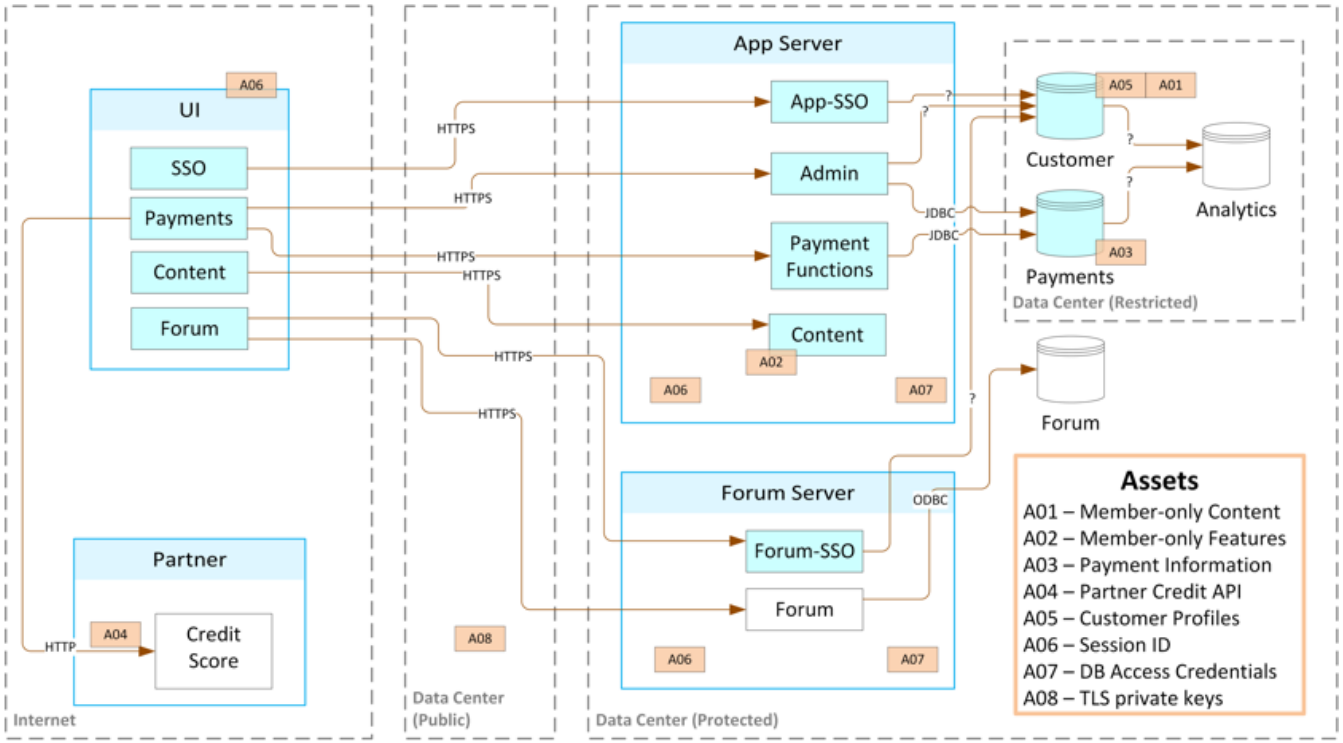
- Understand how the system works (before trying to break it)
  - Who uses the system
  - What are the business goals
  - What are the dependencies between systems
    - System depends on what inputs?
    - What outputs do other systems depend on?
- Review documents already created
  - Interface Control Documents
  - System Architecture
  - Subsystem Architecture/Requirements
- Cross-disciplinary team is key

Simplified System Model



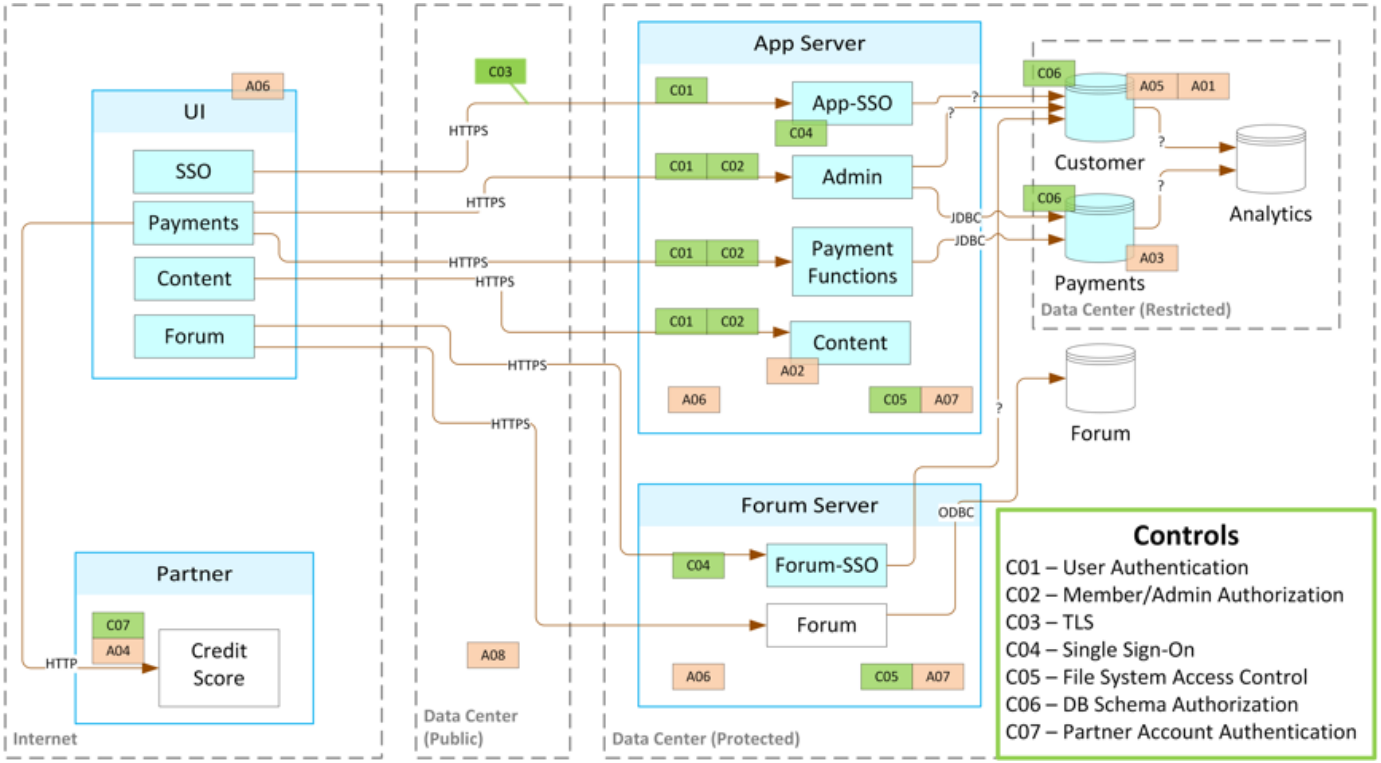
SYNOPSYS®

Model the Attack Possibilities: Assets



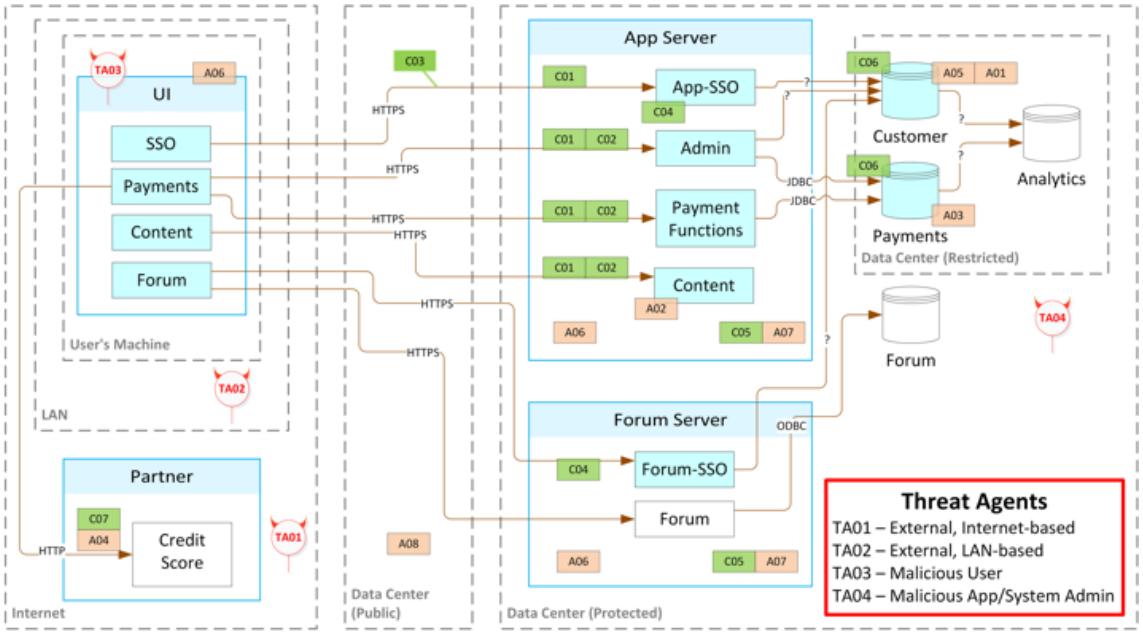
SYNOPSYS®

Model the Attack Possibilities: Security Controls



SYNOPSYS®

Model the Attack Possibilities: Threat Agents

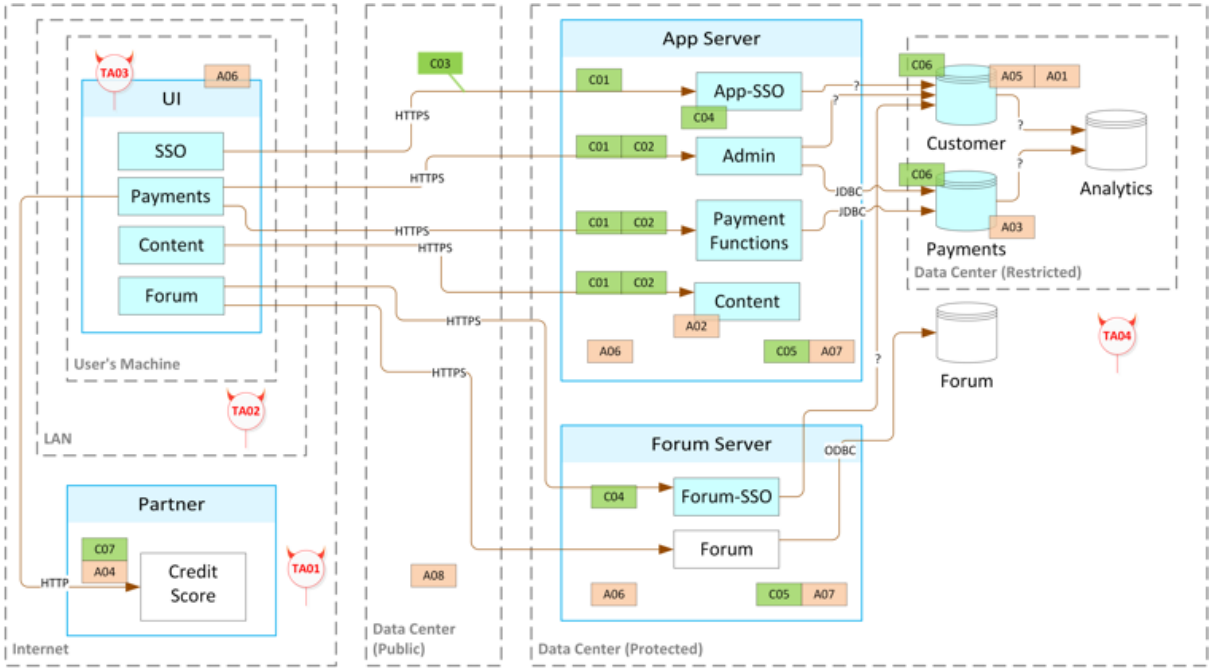


SYNOPSYS®

System Threat Model

Characteristics of the system threat model include:

- Provides holistic view of application's security posture
- Considers both application and infrastructure
- Builds roadmap for additional security activities



Interpret the Threat Model

To interpret the threat model, start with threat agent and follow flow-of-control paths to reach an asset:

- Is there any path where threat agent can reach asset without going through a control?

- For any security control along each of those paths:
  - What must threat agent do to defeat the control?
  - Can threat agent defeat the control?

Record missing or weak controls in the traceability matrix.

Traceability Matrix—In One Sentence

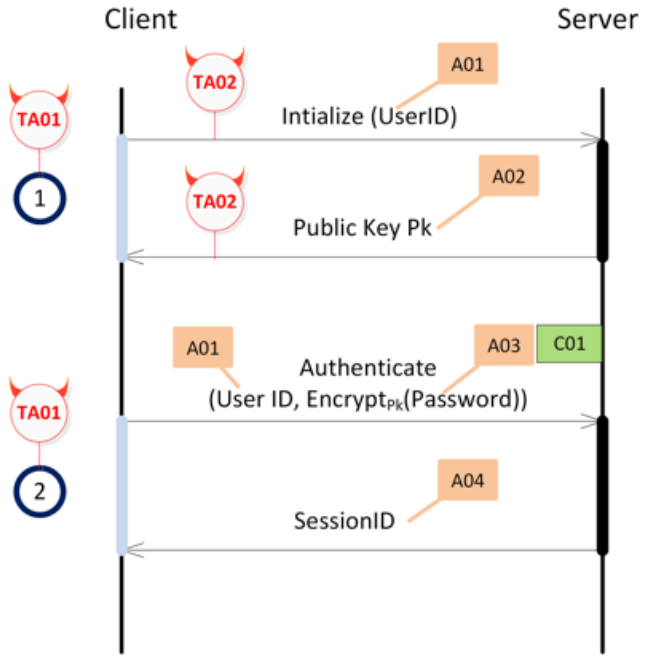
"A ***threat agent***, trying to compromise some ***asset***, using ***attack***, interacting via ***attack surface***, in order to achieve ***attack goal***, having ***impact***, mitigated to an acceptable risk level by ***security control.***"

Threat Agent	Asset	Attack	Attack Surface	Attack Goal	Impact	Security Control
Threat Agent	Asset compromised	Actual exploit	Entry point used by attacker	Goal of attack	Impact	Mitigation advice

Protocol/Sequence/API Threat Model

Characteristics include:

- Analysis of message structure and component interaction
- Importance of message order or flow



SYNOPSYS®

In Summary

- Understand different techniques used for threat modeling
- Understand the threat modeling process and methodology using the Synopsys method as an example
- Use Synopsys threat modeling approach for analyzing applications and systems