

Threat and Vulnerability Analysis: The Concept and a Methodology

John P. Pironti

CISA, CISM, CISSP, ISSAP, ISSMP

Principal Enterprise Solution Architect

Principal Security Consultant

Unisys Corporation

September 21, 2006

UNISYS

Imagine it. Done.

INTEROP
MAKES YOU
SUCCEED

Threat Analysis Overview

Agenda

- Threat Analysis Concept Overview
- Asset Identification & Required Information
- Key Elements of Threat Analysis
- OSI+ Threat Analysis Methodology
 - Who, What, When, Where, Why, and How
 - OSI + Layers
- Threat Level Assignment
- Intelligence
- Final Thoughts

Threat Analysis

Concept Overview

- Threat Analysis is an activity which models a particular solution against attack scenarios and known vulnerabilities to evaluate its ability to repel attacks
- The output of a threat analysis should produce information to create appropriate identification and countermeasure plans for identified attack scenarios
- Threat Analysis should also quantify risk of identified threat to organization
 - Likelihood of occurrence
 - Impact on organization

Why Is Security So Difficult?

- Adversaries have extraordinary resources
- Adversaries need to master only one attack
- Defenders constrained by ethics and laws
- Defenders must serve business goals
- Defenders must win all the time



Threat Analysis

General

- In order to protect a solution you must understand the threats that exist to the environment
 - What is the problem you are trying to solve?
- Each element of the solution will have individual threats as well as the overall threat to the solution
- Threat models will drive business and technical decisions for the overall security solution



Asset Identification

- All assets associated with solution need to be identified prior to threat analysis activity
- Both physical and logical assets need to be identified
- Third party elements need to be accounted for
 - Risks associated with these elements need to be documented



Asset Classification

- All identified assets need to be classified
 - Simple classification system most effective
 - Numeric or Level Systems Most Effective
 - 1 -5 (1 least sensitive 5 most sensitive)
 - Public, Confidential, Confidential-Restricted
- Classifications need to be understood by both humans and machines
 - Physical Marking – (Stamps, Tags)
 - Electronic Marking (XML, DRM tags)
- Classifications will define controls
 - Not all data created equally
 - Higher sensitivity levels typically require more controls
- Appropriate risk management can be applied with effective classification



CONFIDENTIAL

Threat Analysis Required Information

- Threat analysis activities require significant information from organization to be accurate and effective
 - Value to the organization
 - Regulatory and legal constraints
 - Sensitivity of data included in solution
 - Impact on third party activities
- Appropriate risk management decisions cannot be made without these considerations



Threat and Vulnerability Analysis Methodology Overview

OSI+ Threat and Vulnerability Assessment Methodology

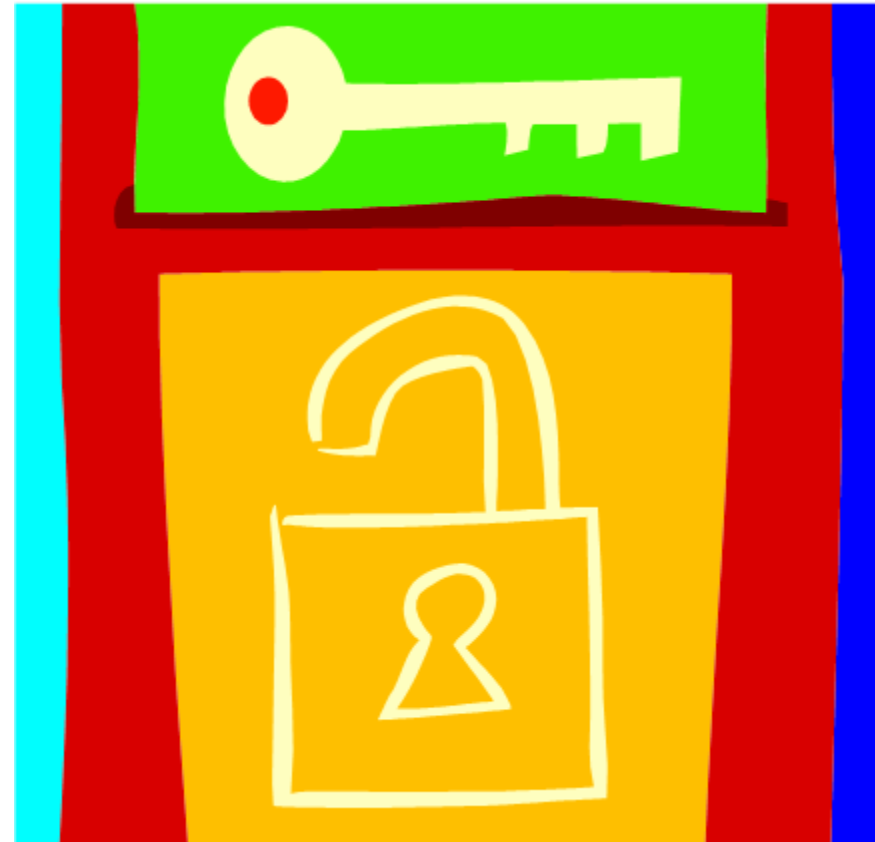
- Overview
- Who, What, When, Where,
Why, and How
- Countermeasure Plans
- Threat Level Assignment



Threat and Vulnerability Analysis

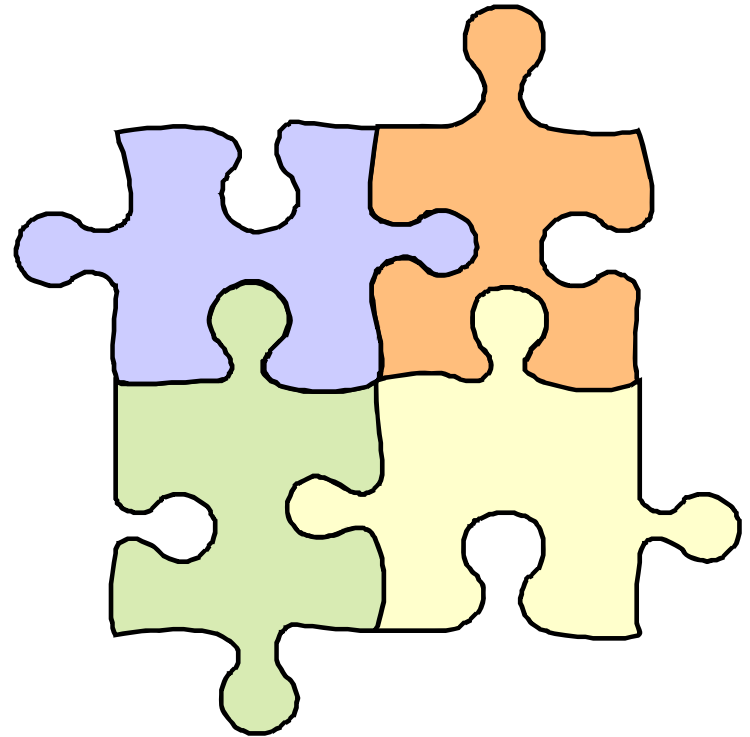
Threat Models

- Threat models should include:
 - Profiles of capabilities and knowledge of adversaries
 - Known vulnerabilities of utilized hardware and software and solution elements
 - Scenarios which describe how an attacker could compromise each element of the environment
 - Countermeasure plan for each attack scenario and attack profile



OSI+ Methodology Overview

- Skilled adversaries will use a combination of skills and techniques to attempt to compromise a solution
 - Technological attacks are not the only way an adversary will attack a solution
- The OSI+ model provides a framework for analyzing how an adversary can attack a solution
 - Identifies weaknesses in current solution
 - Systematic way to evaluate a solution
- Each element needs to be analyzed but not elements will be relevant for each solution



Threat Analysis – Who

Attacker Profiles

- **Newbies**
 - Beginners, Download Tools from Internet
- **Script Kiddies**
 - Basic Programming Skills
 - Customize Downloaded Tools
- **Coders**
 - Advanced Programming Skills
 - Write Tools for Newbies and Script Kiddies
- **Professionals**
 - Privately Funded Research
 - Advanced Capabilities and high levels of access to technology
 - Highly dedicated and resourceful
- **Spooks**
 - Government Agents
 - Unlimited Resources and Capabilities



Threat Analysis – Who

Competency Models

- Understanding of current and future capabilities of the adversary community
- Research of current education and knowledge programs for computer science and computer security
- Profiling of backgrounds and lifestyles of potential adversaries
- Profiling of adversaries required skills, knowledge, and tools

Threat Analysis

What

- Identification of the portion of the solution which the adversary will most likely attack
 - Typically area most easily accessible from external access point or with highest perceived value
- Skilled adversaries usually attack highest value solutions
- General adversaries will attack solutions which they have highest levels of access to
 - Web Access
 - Remote Access



Threat Analysis When

- Identification of most likely time an adversary will attack
 - Time of day when defenses at weakest
 - Time of year when defenses are at their weakest
- Skilled adversaries will attempt to attack when they believe security staff is distracted with other events
 - Business continuity and disaster recovery events
 - Recovery from known virus infections



Threat Analysis

Where

- Identification of the most likely points of attack of a solution
 - Remote access points
 - Third party access points
 - Web environments (HTTP attacks)
- Skilled adversaries will attempt to identify systems whose value is perceived to be low and will most likely have minimum security attributes
 - Print Servers
 - Backup Servers



Threat Analysis

Why

- What is the benefit to the of a successful attack to an adversary?
 - Financial
 - Political
 - Personal
 - Status Seeking
- Understanding of motivations will assist in the creation of appropriate countermeasures and risk identification



Threat Analysis

How

- Analysis of the tools and techniques an adversary will use to attack a solution and the solutions ability to counteract these tools and techniques
- Information will be required from multiple sources
 - Web sites
 - News feeds
 - IRC message boards
 - Intelligence activities
- OSI+ Methodology is one way to analyze how an adversary can compromise a solution
 - Aligns with Open Systems Interface (OSI) Model
 - Adds critical element of people, policy, process, and procedure to model



OSI+ - How Layers

Policy, Process, and Procedure
Application
Presentation
Session
Transport
Network
Data
Physical
People

Threat Models – *Attack Trees*

- Attack trees are graphical depictions of how an adversary could compromise a solution
 - Identifies roadmap of adversaries activities
- Useful in understanding system view of attack sequence and impact
- Provide valuable data to incident response and operations teams in identification and remediation of attacks



Threat Analysis Countermeasure Plans

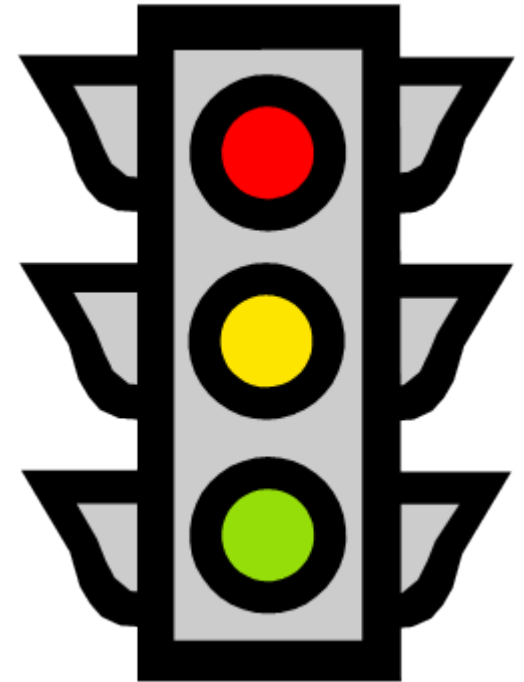
- Once threat analysis has been completed countermeasure plans should be created for identified scenarios
 - Threat identification
 - Procedures for threat and attack mitigation
 - Recognition of attack completion and successful mitigation



Threat Analysis Methodology

Threat Level Assignment

- Output of threat analysis should include threat level assignment
 - Required for risk management decisions by management teams
 - Should be communicated to all individuals with security responsibilities
- Threat levels need to be simple and easily understood
 - Red, Yellow, Green & 1 -5 designations work well
 - Simple designations allow for better awareness throughout organization
- Each designation needs to be defined from a business impact perspective



Vulnerability Management Intelligence

- Important to understand current trends and capabilities of attackers
- Knowledge base of known attacks and attackers should be created
- Trend analysis should be performed to be able to project future attacks and attack methods



Threat Analysis

Final Thoughts

- Threat Analysis activities are an essential tool in risk management programs
- Before you can solve a problem you must understand the problem
- Threat analysis is only a module in a overall security program
 - Does not solve the overall security problem
 - Require incident management and operations integration to be successful



Thank You For Your Time!

Contact Information...



John P. Pironti
CISA, CISM, CISSP, ISSAP, ISSMP
01-781-238-1375
John.pironti@unisys.com