Modeling Vulnerabilities

from buffer overflows to insider threat

Sophie Engle

NSF I/UCRC CIP MEETING

UC Davis Kemper Hall 1008 · Tuesday June 17 2008

Motivation

Motivation

What does it mean for a system to be secure?

Motivation

What does it mean for a system to be secure?

physically secure?

Motivation

What does it mean for a system to be secure?

cannot be misused by insiders?

Motivation

What does it mean for a system to be secure?

only authorized persons have access?

only authorized user accounts have access?

Motivation

What does it mean for a system to be secure?

no buffer overflow bugs?

no buffer overflow vulnerabilities?

Motivation

What do all of these examples have in common?

Motivation

What do all of these examples have in common?

POLICY

Motivation

What does it mean for a system to be secure?

physically secure?

policy defines…
the physical requirements of the system

Motivation

What does it mean for a system to be secure?

cannot be misused by insiders?

policy defines…
how the system is *intended* to be used

Motivation

What does it mean for a system to be secure?

only authorized persons have access?
only authorized user accounts have access?

policy defines…
who is authorized for what type of access

Motivation

What does it mean for a system to be secure?

no buffer overflow bugs?
no buffer overflow vulnerabilities?

policy defines…
the difference between bug & vulnerability

Motivation

What does it mean for a system to be secure?

no vulnerabilities

where a *vulnerability* is a set of conditions
that may lead to a potential policy violation

Motivation

How do we define policy?

Background

Background

How do we define policy?

Unifying Policy Hierarchy

(*Adam Carlson, Master's Thesis*)

Unifying Policy Hierarchy

Oracle Policy

- Represents the intent and will of policy makers
- May not be explicitly specified

Example:

Xander is authorized to read file `readme.txt`

Unifying Policy Hierarchy

Feasible Policy

– Represents the intent and will of policy makers

– Takes into account the mechanics and available access controls of the system

Example:

User account `xander` is authorized to read file `readme.txt`

Unifying Policy Hierarchy

Configured Policy

– Represents the policy configured on the machine

Example:

All user accounts are authorized to read file `readme.txt`

Unifying Policy Hierarchy

Actual Policy

– Represents the policy currently in effect on the machine

Example:

No user can read file `readme.txt`

(potentially result of denial of service attack)

Unifying Policy Hierarchy

Oracle Policy

Captures policy maker's intent

Feasible Policy

Considers limitations of system

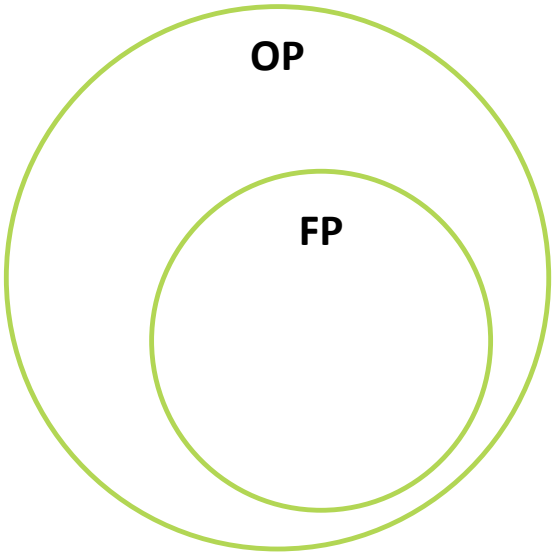
Configured Policy

Policy as configured on system

Actual Policy

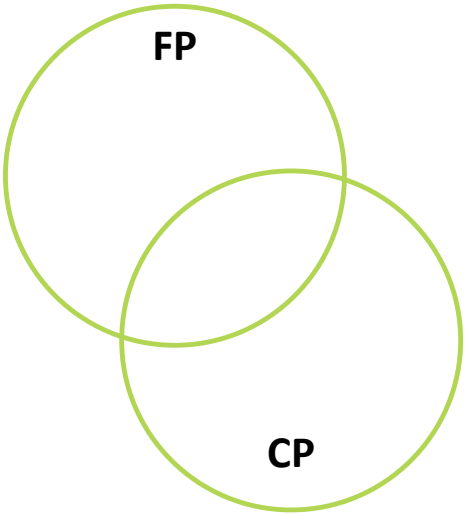
Policy currently in effect on system

Unifying Policy Hierarchy



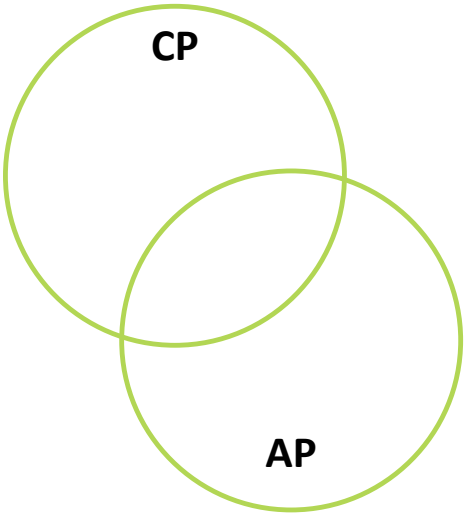
OP ≠ FP
Inherent Vulnerability

Unifying Policy Hierarchy



FP ≠ CP
Configuration Vulnerability

Unifying Policy Hierarchy



CP ≠ AP
Runtime Vulnerability

Proposal

Proposal

1. **Expand application of the hierarchy**

Proposal

1. **Expand application of the hierarchy**
   - Insider Threat
   - Social Engineering
   - Network Viewpoint
   - *And more…*

Proposal

Insider Threat

"exists whenever a lower policy level has *more* authorized privileges than a higher policy level"

Insider Threat

"exists whenever a lower policy level has *more* authorized privileges than a higher policy level"

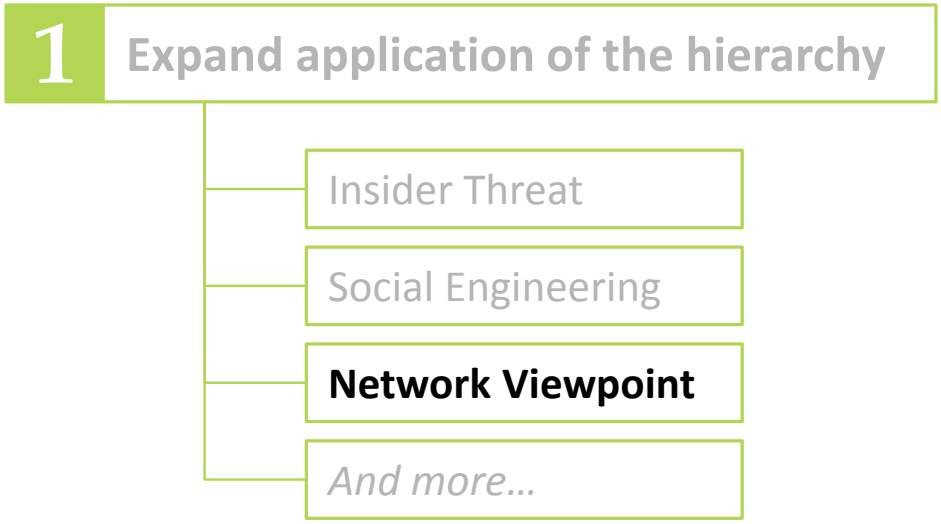
> OP: Yasmin may use the system to read medical records to treat patients.

Insider Threat

"exists whenever a lower policy level has *more* authorized privileges than a higher policy level"

> OP: Yasmin may use the system to read medical records to treat patients.
>
> FP: User account `yasmin` may use the system to read medical records.

Proposal



Network Viewpoint

In original approach, each system has its own associated policy hierarchy.

Network Viewpoint

In original approach, each system has its own associated policy hierarchy.

How do we expand this to a more network-based approach?

Proposal

1. Expand application of the hierarchy
2. **Use model to perform threat analysis**

Threat Analysis

"Gap Analysis"

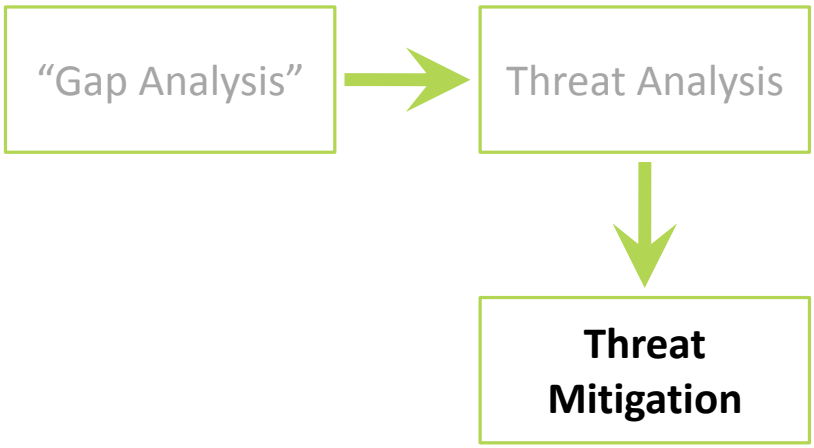
Examine the "gap" between levels of the policy hierarchy, i.e. everywhere two consecutive levels do not match.

Threat Analysis

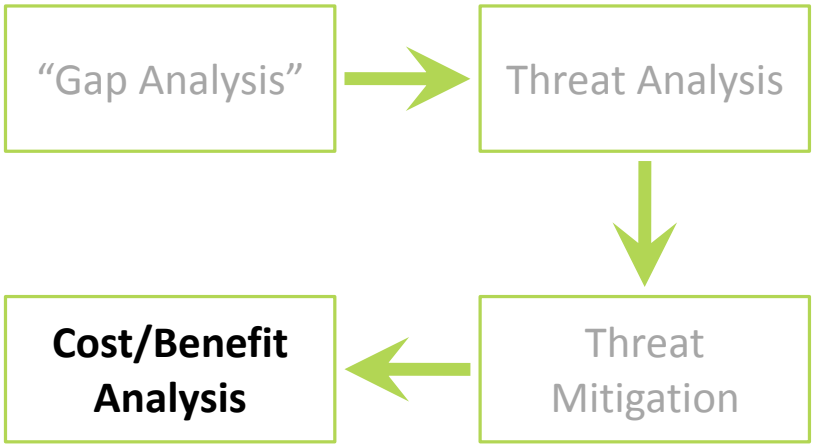
"Gap Analysis" → **Threat Analysis**

Next, determine the potential threat caused by these gaps.

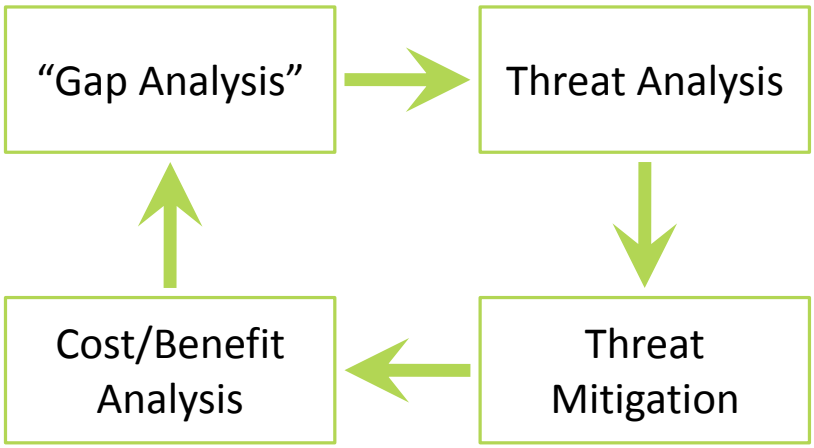
Threat Analysis



Threat Analysis



Threat Analysis



Proposal

1. Expand application of the hierarchy
2. Use model to perform threat analysis
3. **Present findings in a wiki format**

Questions?