SECURITY (COMP0141): THREAT MODELLING

UCL

define

How to ~~design~~ a secure system?

one that meets a specific security policy

How to define a security policy?

WHAT SHOULD POLICY ADDRESS?

Threats

Vulnerabilities

Likelihood

Impact

Protection

WHAT SHOULD POLICY ADDRESS?

Threats (who is the adversary?)

Vulnerabilities

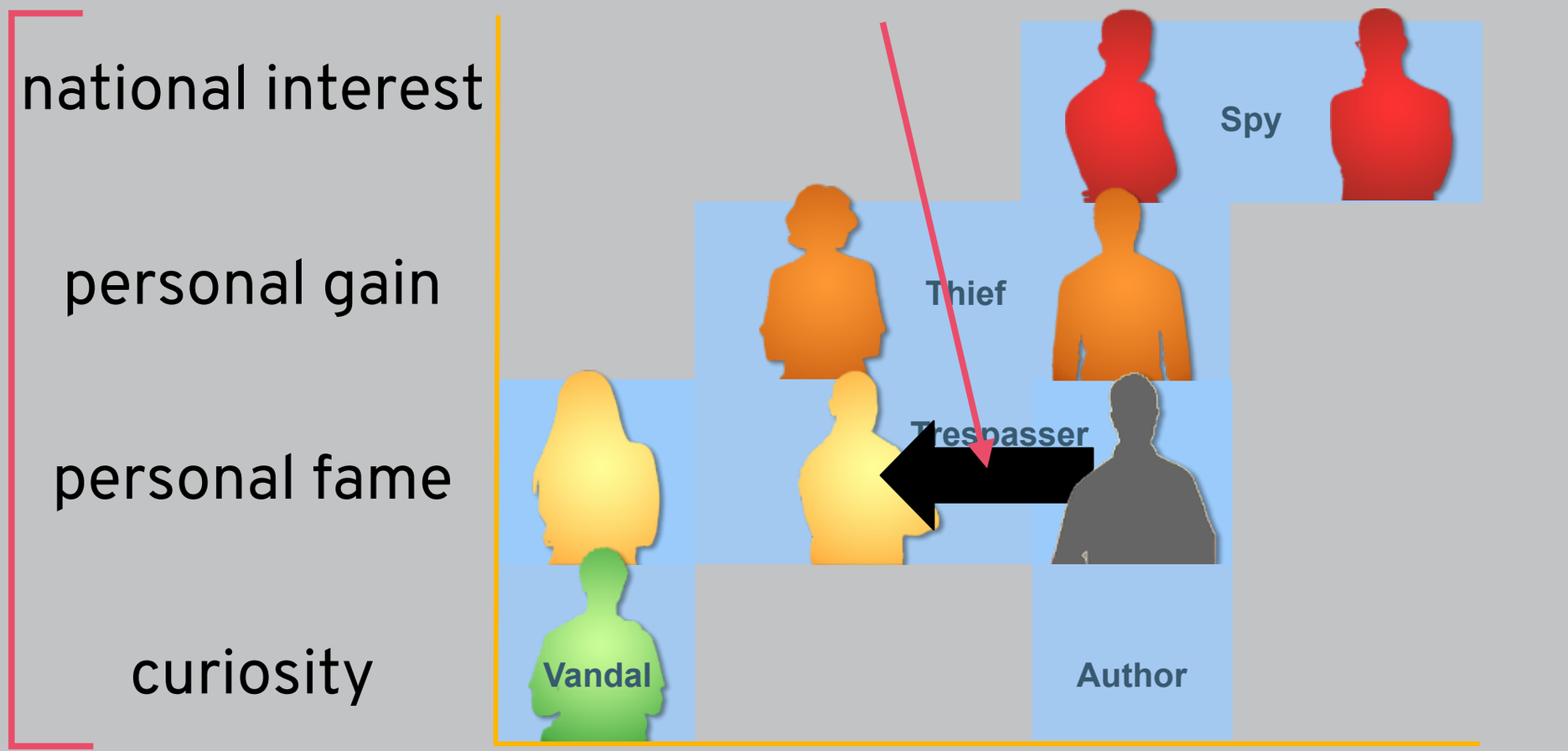
Likelihood

Impact

Protection

THREAT LANDSCAPE

tools created by experts now used by less-skilled attackers and criminals



(David Aucsmith, Microsoft)

“RESOURCEFUL STRATEGIC ADVERSARY”

What are the resources available to the adversary? What can they…

- Observe? (network connection)
- Corrupt? (router)
- Influence? (network configuration)
- Modify? (packet data)
- Control? (company employee)

An attack is some series of actions that allow the adversary to violate a given security policy

A strategic adversary chooses the **optimal** way to use their resources to mount an attack

STRIDE

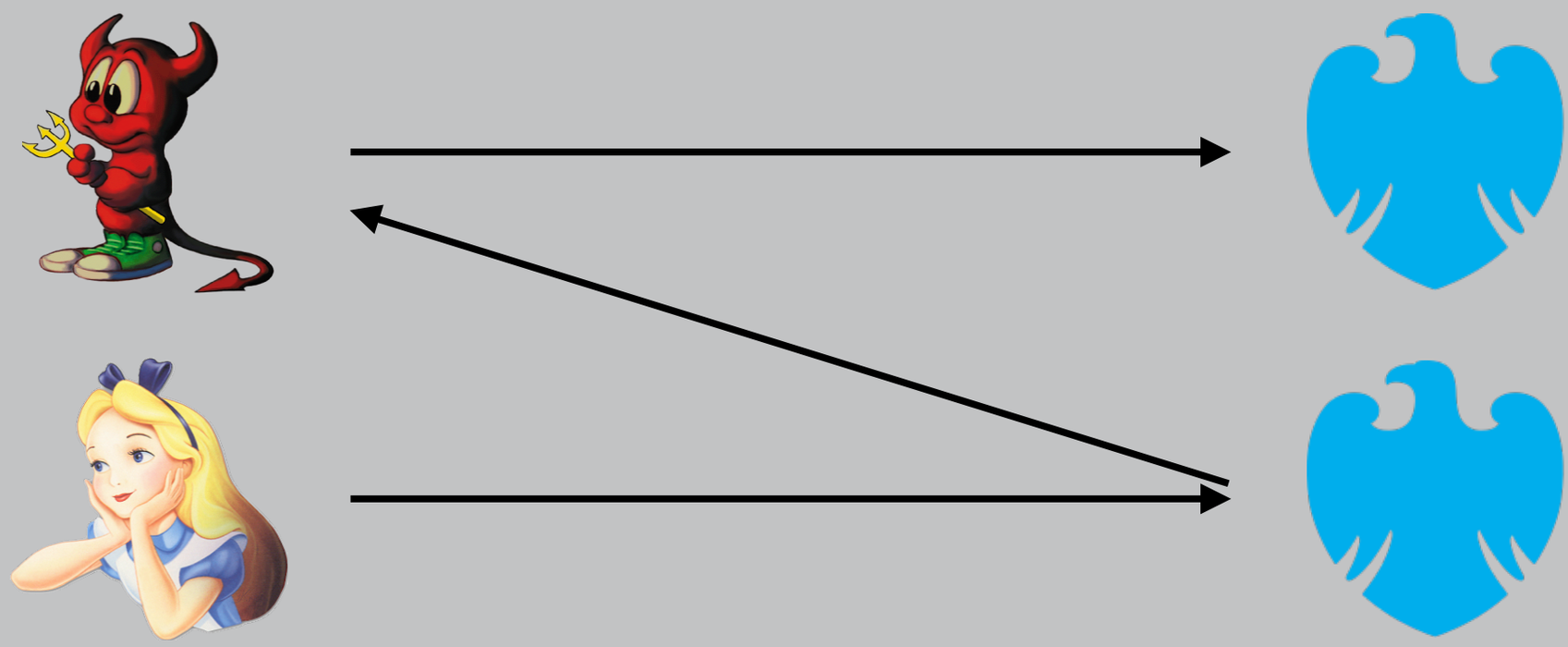
S*poofing* T R I D E

“It’s me, Alice!”

STRIDE

S T R I D E

Spoofing Tampering



STRIDE

S Spoofing

T Tampering

R Repudiation

I

D

E

“It’s me, Alice!”

“It wasn’t me!”

STRIDE

S T R I D E

Spoofing
Tampering
Repudiation
Information disclosure

account info of users

STRIDE

S Spoofing

T Tampering

R Repudiation

I Information disclosure

D Denial of service

E

STRIDE

S Spoofing

T Tampering

R Repudiation

I Information disclosure

D Denial of service

E Elevation of privilege

"It's me!"

account info of users

WHAT SHOULD POLICY ADDRESS?

Threats

Vulnerabilities (where can system break?)

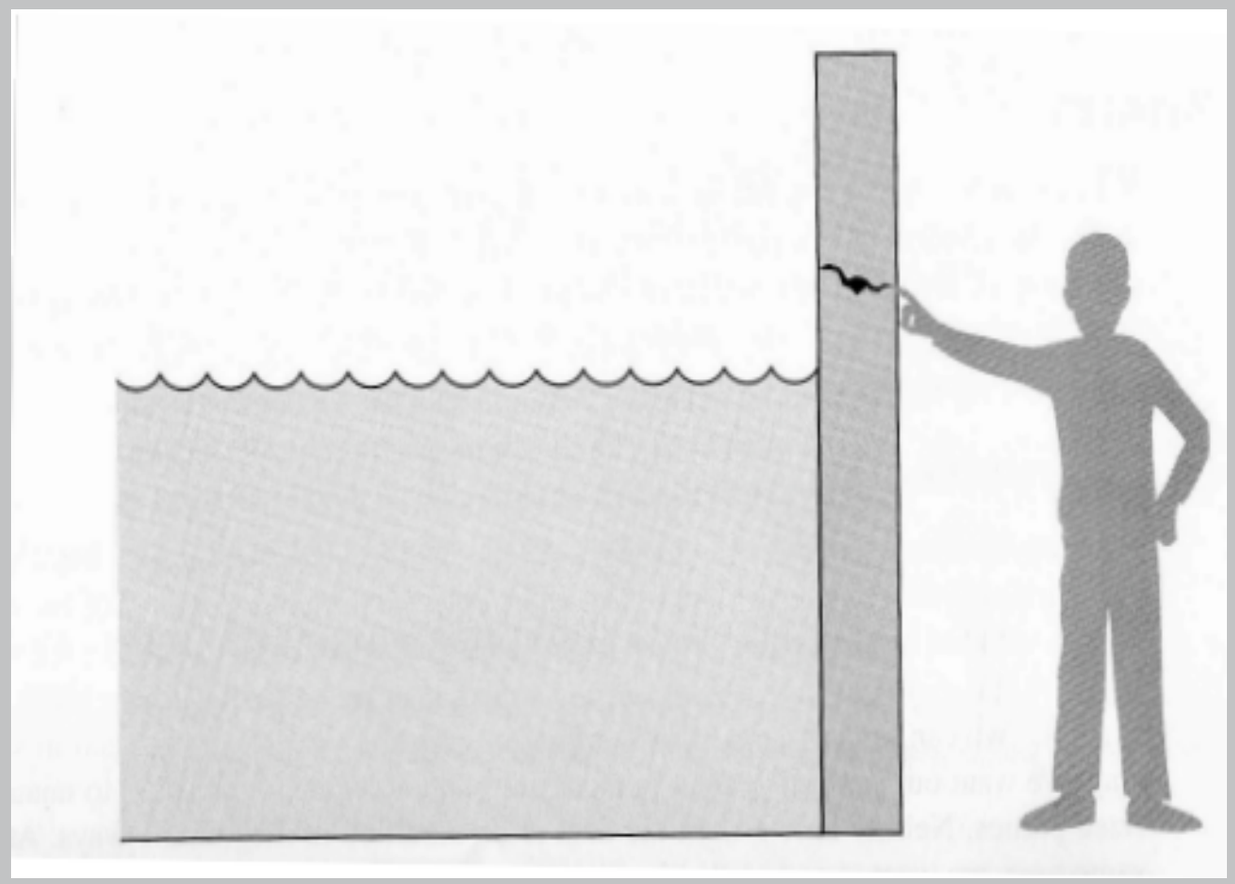
Likelihood

Impact

Protection

THREAT VS. VULNERABILITY

Threat? Water might overflow



Vulnerability? Crack

IDENTIFYING VULNERABILITIES

WHAT SHOULD POLICY ADDRESS?

Threats

Vulnerabilities

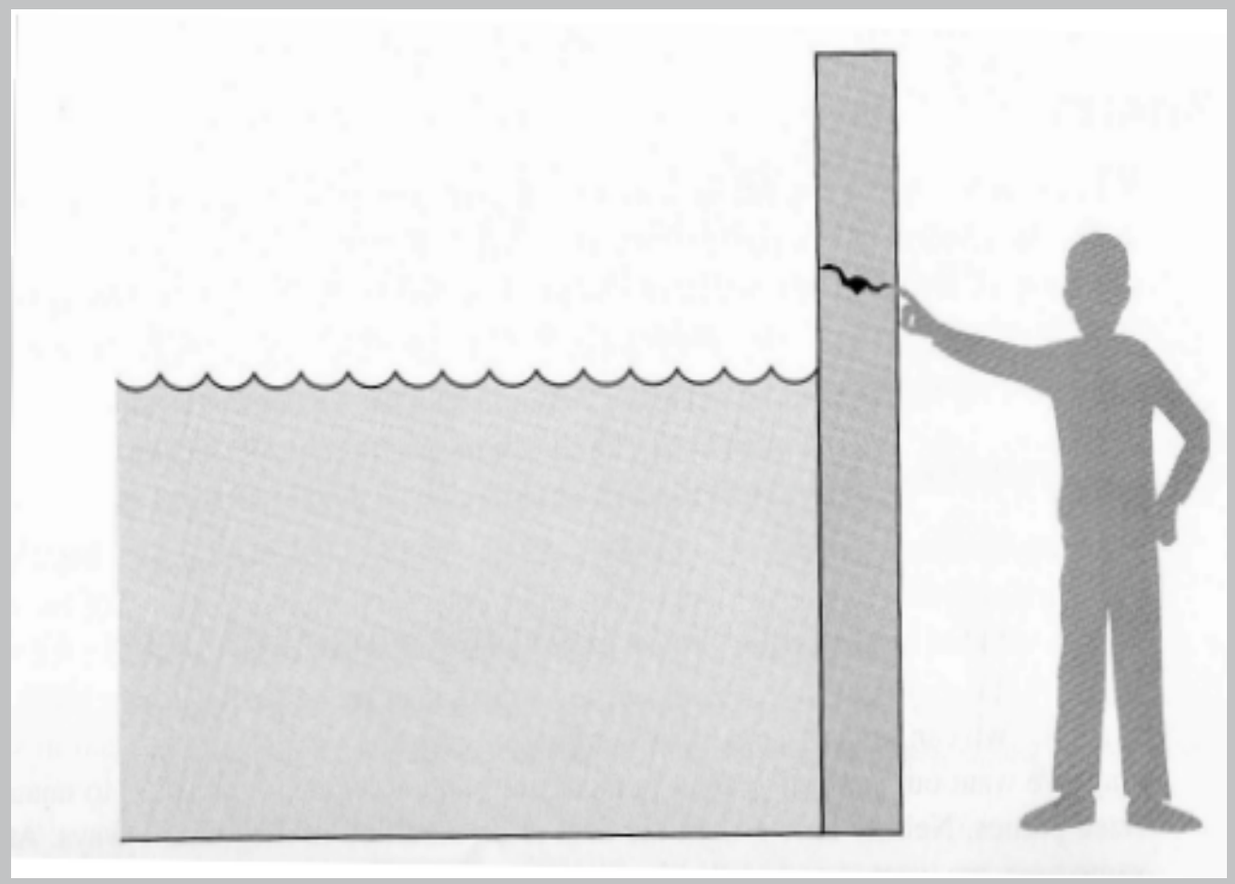
Likelihood (might this happen?)

Impact

Protection

VULNERABILITY VS. LIKELIHOOD

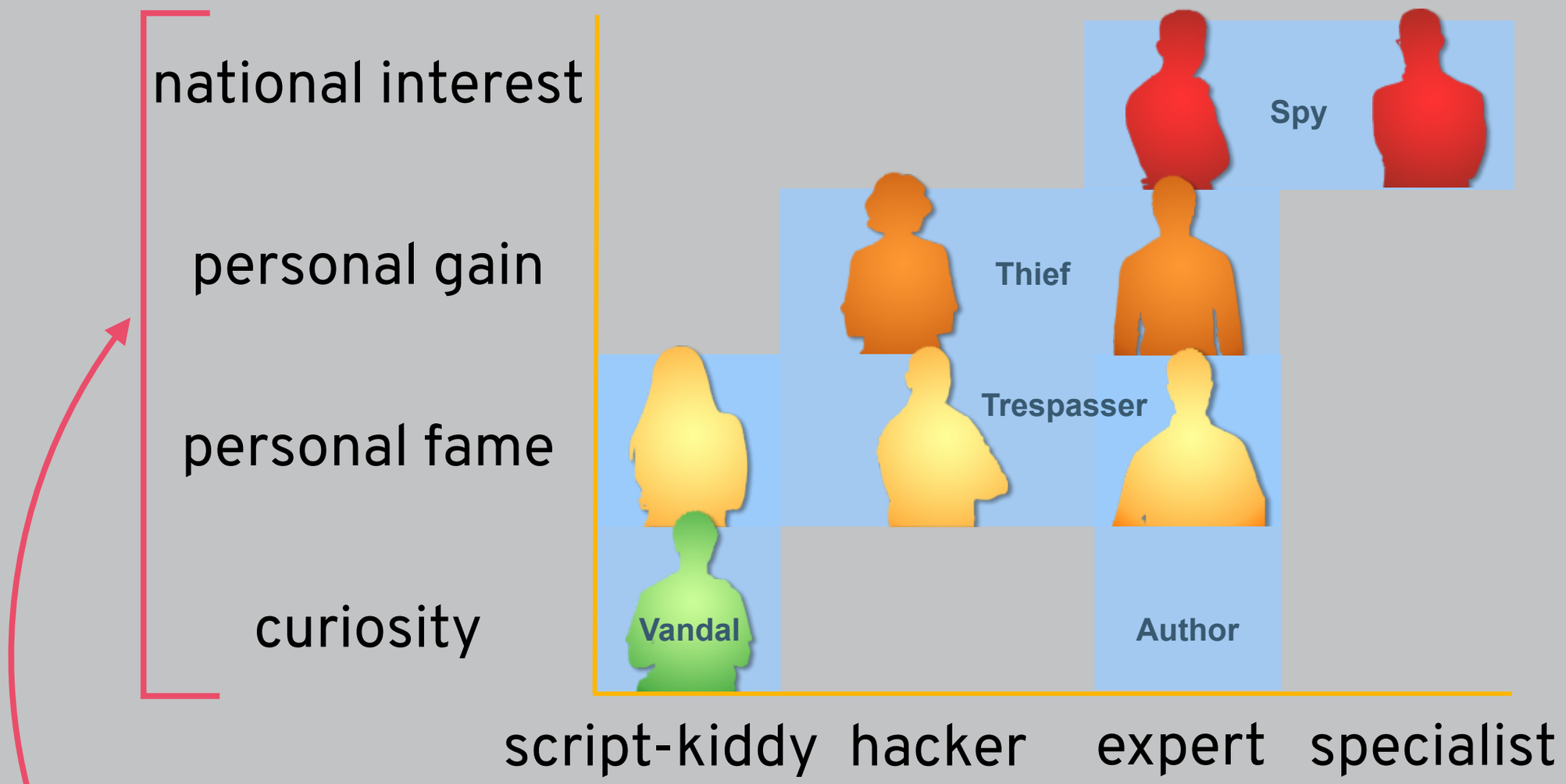
Likelihood? Zero if we never add water



Vulnerability? Crack

LIKELIHOOD

MOTIVATION



(David Aucsmith, Microsoft)

WHAT SHOULD POLICY ADDRESS?

Threats

Vulnerabilities

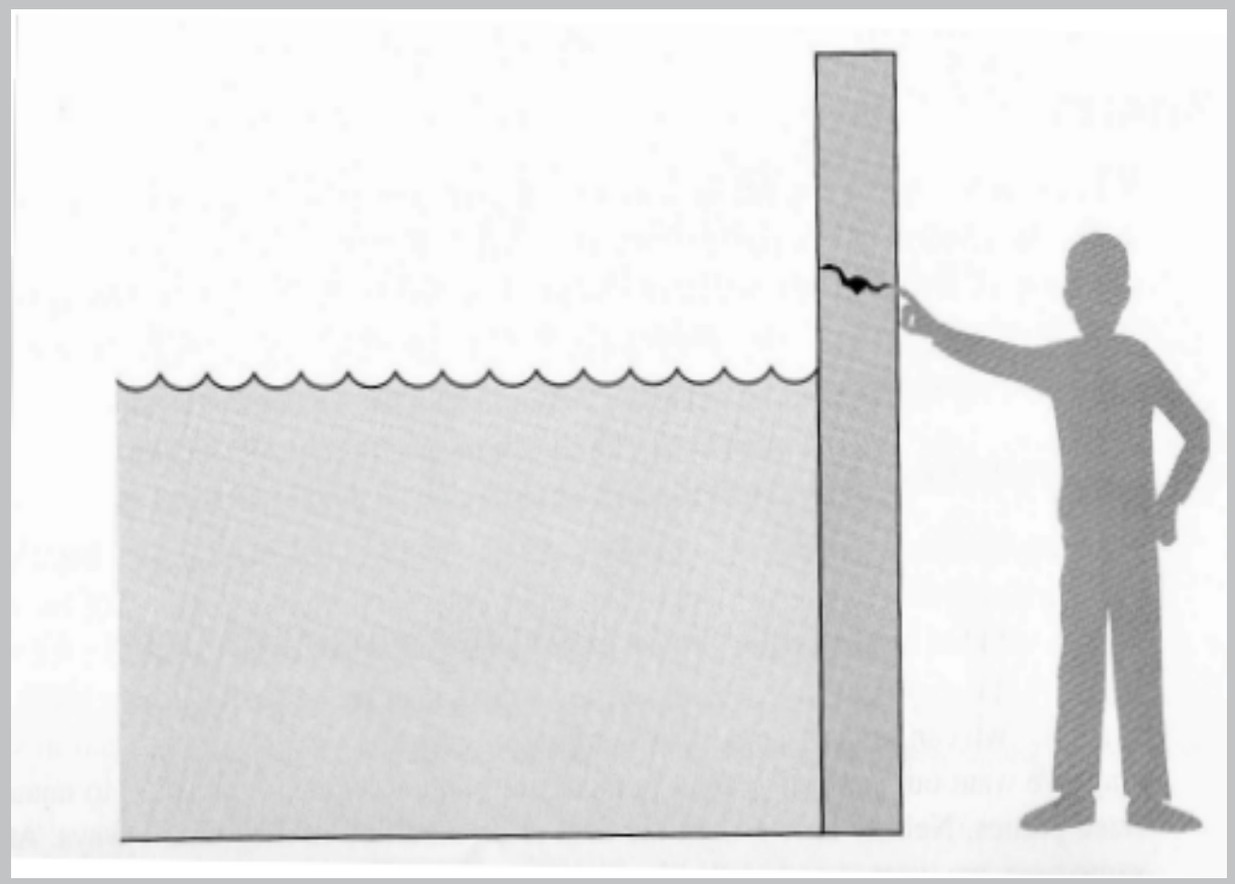
Likelihood

Impact (what if bad things happen?)

Protection

THREAT VS. IMPACT

Threat? Water might overflow



Impact? Depends on what's nearby

IMPACT/SCALE/COST

WHAT SHOULD POLICY ADDRESS?

Threats

Vulnerabilities

Likelihood

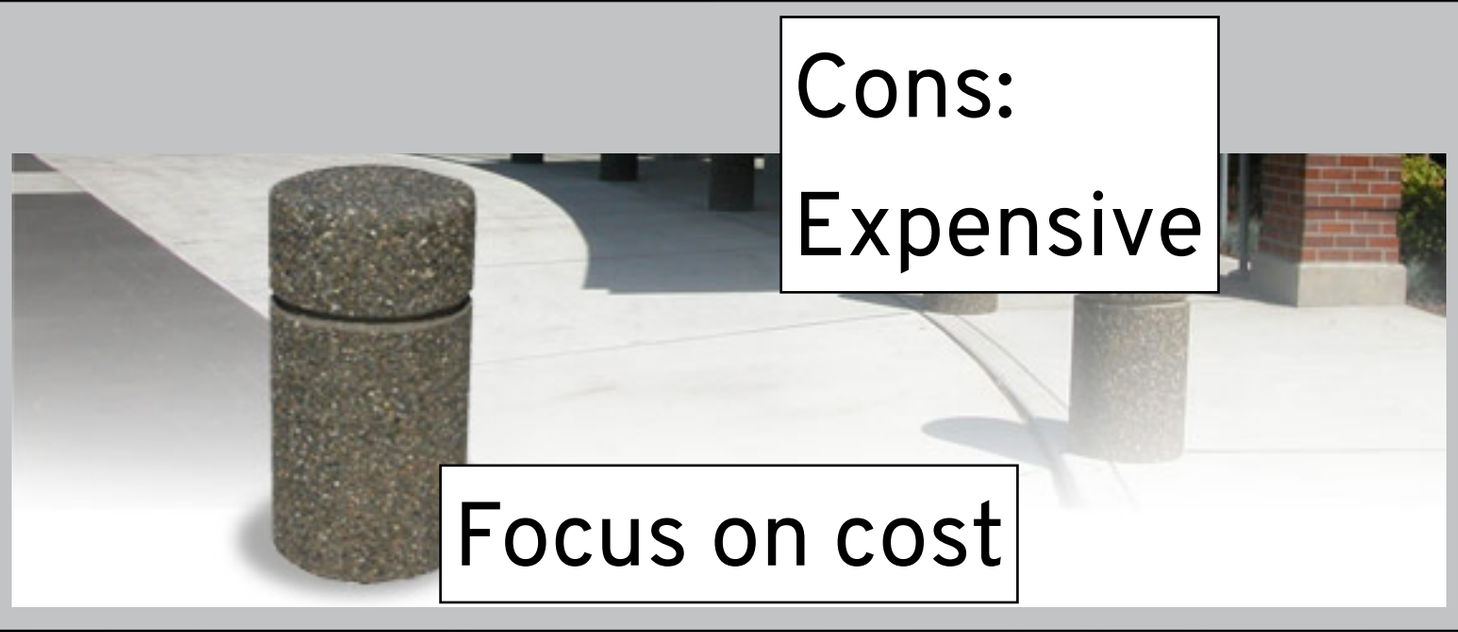
Impact

Protection (what does it cost?)

PROTECTION

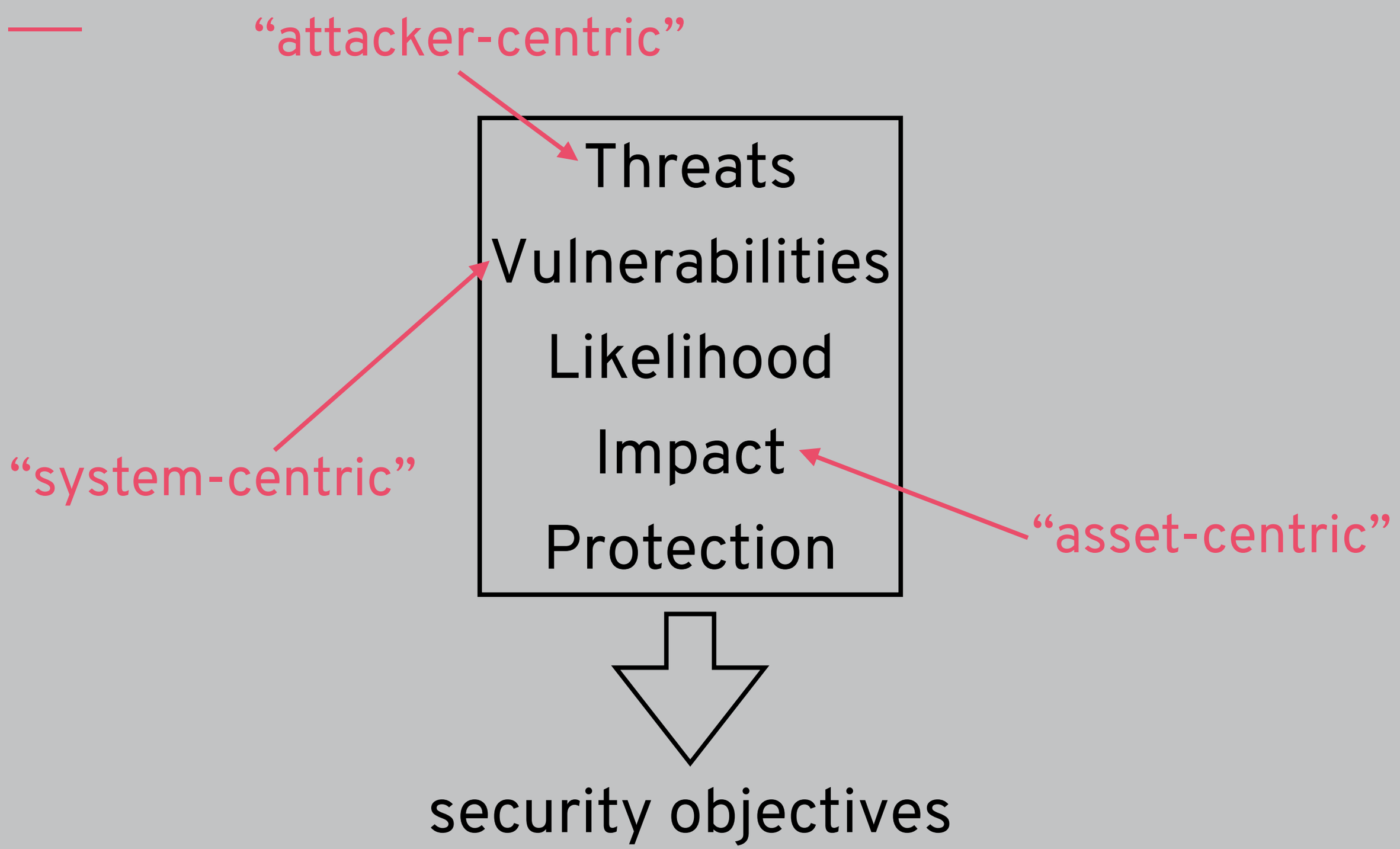
most of academic computer security is **protection**

secure	insecure



secure	insecure

THREAT MODEL



ATTACKER-CENTRIC THREAT MODEL

CAPABILITIES

The adversary can observe my connection
The adversary can corrupt my machine
The adversary controls a bank employee

MOTIVATION

The adversary wants to steal my money
The adversary wants to learn my password

VULNERABILITIES

The banking API is not protected
The password appears on my screen

IMPACT

The adversary steals my money
The adversary learns my password
The adversary blocks access to my bank account

define

How to ~~design~~ a secure system?

one that meets a specific security policy

How to define a security policy?

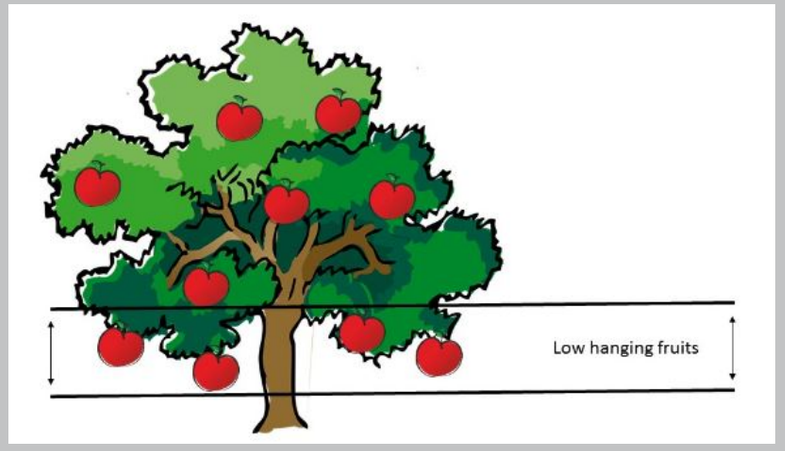
threats, vulnerabilities, likelihood, impact, and cost

used to create a **threat model**

ASYMMETRY: ADVERSARY VS. DEFENDER

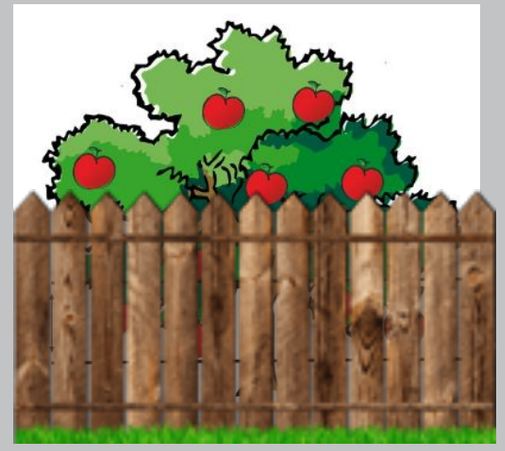
ATTACKER

*Just **one*** way to violate ***one*** security property is enough! (within the threat model)

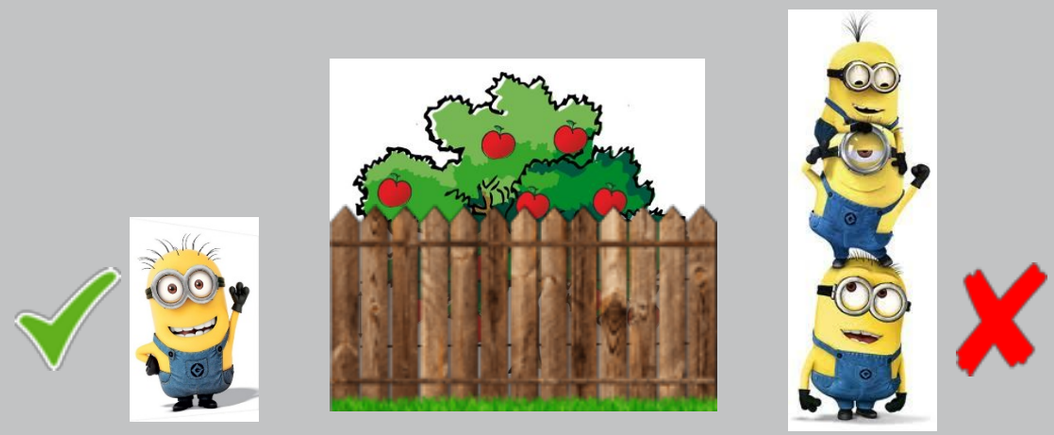


DEFENDER

No adversary strategy can violate the security policy



IS THE SYSTEM SECURE?



Need to instead ask: Is it secure under this threat model?

A system is “secure” if an adversary **constrained** by a **specific threat model** cannot violate the **security policy**

Again, binary models are brittle (if threat model is wrong you’re in trouble) and risk management ones may require many iterations

Observe systems around you and think: is the policy realistic? Is the threat model realistic? How/why could they fail?

SECURITY MECHANISM

A system is “secure” if there is a **security argument** that an adversary constrained by a **specific threat model** cannot violate the **security policy**

Security argument: rigorous argument that the **security mechanisms** are maintaining the security policy (subject to the assumptions of the threat model)

Security mechanism: Technical mechanism used to ensure that the security policy is not violated by an adversary operating within the threat model

SECURITY MECHANISM

Could be software, hardware, cryptography, or peoples and procedures — this is why we'll learn about all of these!

Example policy: a log cannot be changed by a single employee
Example mechanism: keep a copy of the log on multiple computers such that no one employee has access to all of them

Security mechanism: Technical mechanism used to ensure that the security policy is not violated by an adversary operating within the threat model