SECURITY (COMP0141): THREAT MODELLING

UCL

SECURITY DESIGN

define

How to ~~design~~ a secure system?

one that meets a specific security policy

How to define a security policy?

So a secure system is one that satisfies a security policy. But what's a security policy?

WHAT SHOULD POLICY ADDRESS?

Threats
Vulnerabilities
Likelihood
Impact
Protection

3

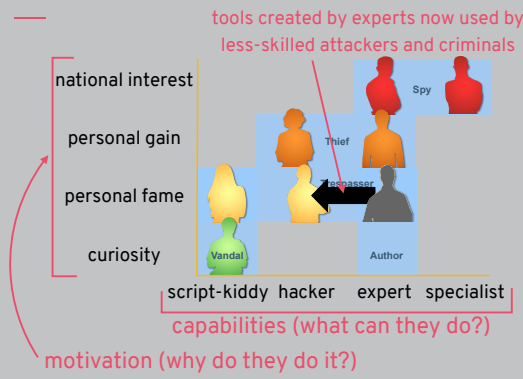
This is also considered a type of risk assessment

WHAT SHOULD POLICY ADDRESS?

Threats (who is the adversary?)
Vulnerabilities
Likelihood
Impact
Protection

4

THREAT LANDSCAPE



(David Aucsmith, Microsoft)

Consider adversary across two dimensions: capabilities and motivations

"RESOURCEFUL STRATEGIC ADVERSARY"

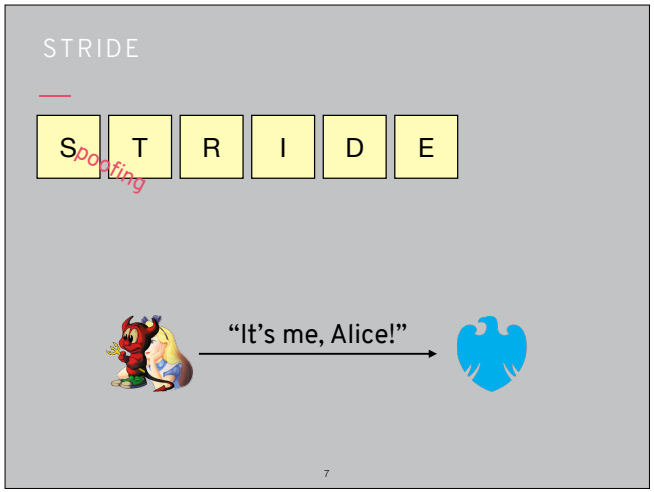
What are the resources available to the adversary? What can they…

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

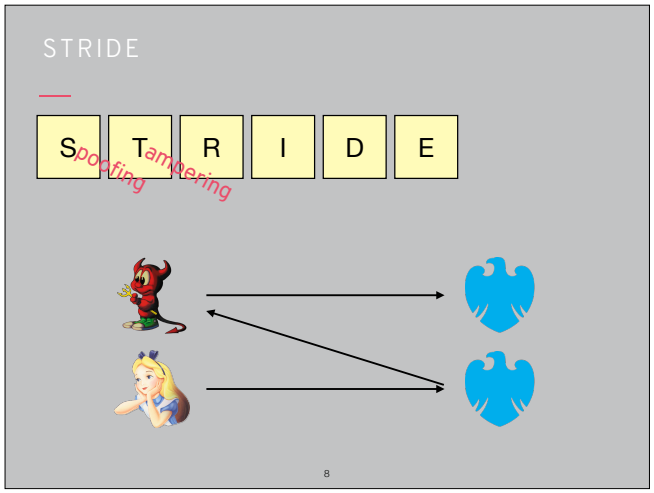
An attack is some series of actions that allow the adversary to violate a given security policy

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

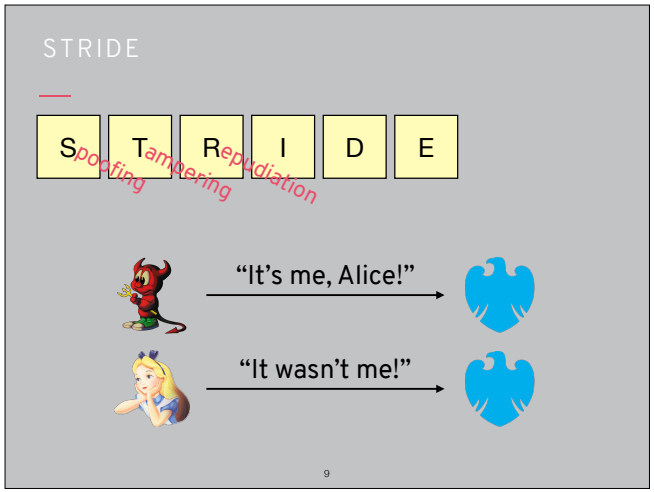
Can consider capabilities in terms of this idea of being resourceful and strategic



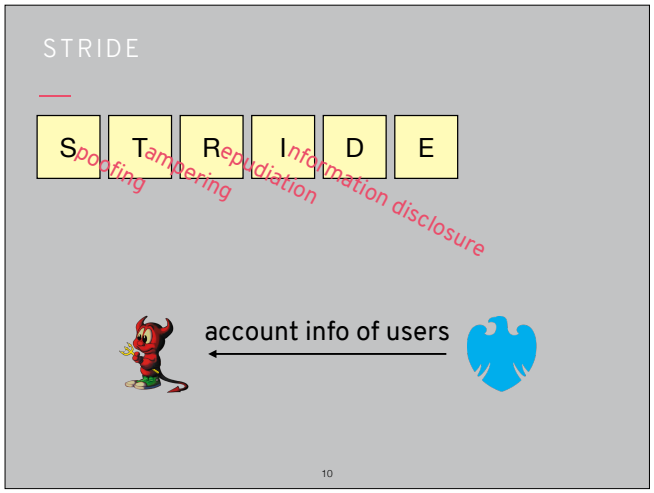
Spoofing is pretending to be someone else



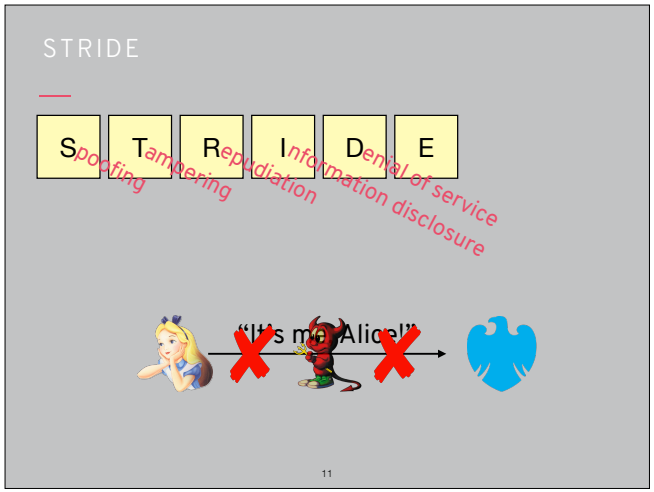
Tampering is altering someone else's interaction to give yourself some advantage



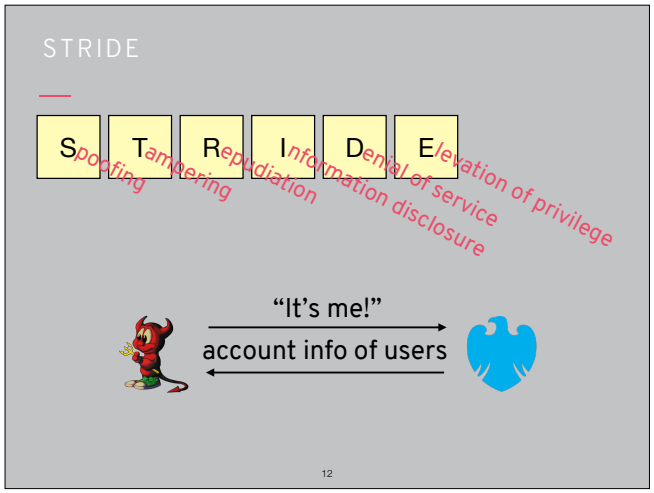
Repudiation is the (in)ability to resist framing



Information disclosure is getting access to something you shouldn't



Denial of service is stopping someone else's access



Elevation of privilege is doing more than you should be able to do

WHAT SHOULD POLICY ADDRESS?

Threats

Vulnerabilities (where can system break?)

Likelihood

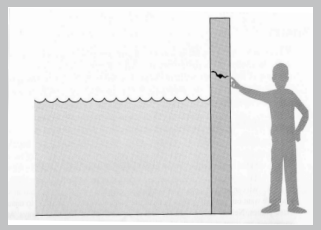
Impact

Protection

13

THREAT VS. VULNERABILITY

Threat? Water might overflow



Vulnerability? Crack

14

Often define vulnerabilities with respect to threats

IDENTIFYING VULNERABILITIES

15

How might someone break in despite this shiny lock?

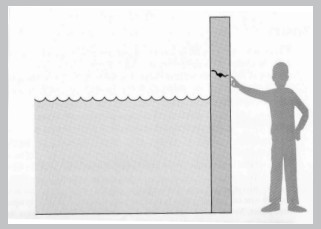
WHAT SHOULD POLICY ADDRESS?

Threats
Vulnerabilities
Likelihood (might this happen?)
Impact
Protection

16

VULNERABILITY VS. LIKELIHOOD

Likelihood? Zero if we never add water



Vulnerability? Crack

17

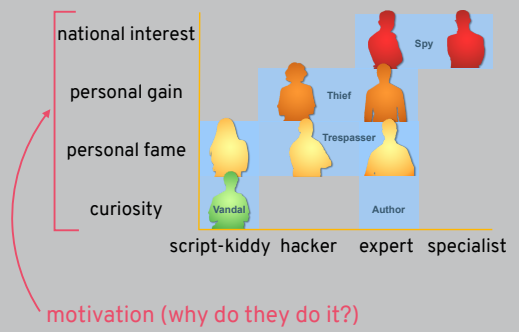
Often define likelihood with respect to vulnerability (need knowledge of overall system to assess)

LIKELIHOOD

18

Does someone actually want to exploit the vulnerability?

MOTIVATION



(David Aucsmith, Microsoft)

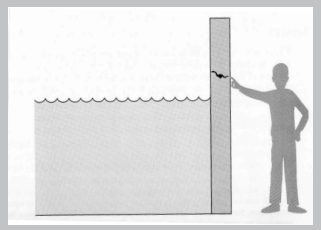
Goes back to the question of motivation

WHAT SHOULD POLICY ADDRESS?

Threats
Vulnerabilities
Likelihood
Impact (what if bad things happen?)
Protection

THREAT VS. IMPACT

Threat? Water might overflow

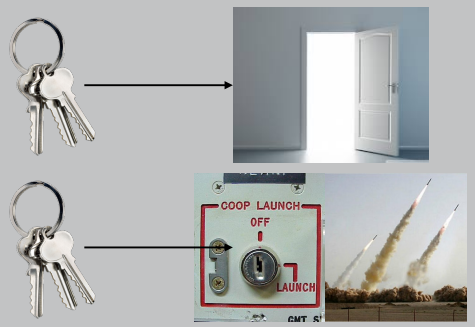


Impact? Depends on what's nearby

21

Often define impact with respect to threat

IMPACT/SCALE/COST



22

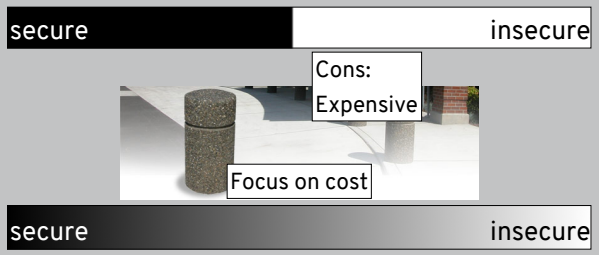
Again, impact is specific to the larger setting

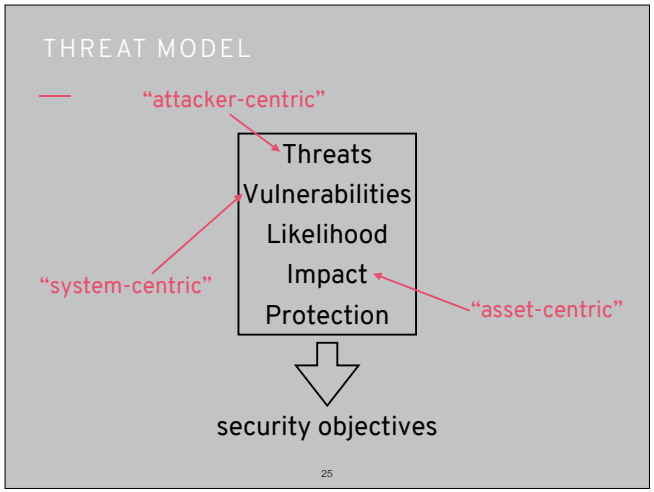
WHAT SHOULD POLICY ADDRESS?

Threats
Vulnerabilities
Likelihood
Impact
Protection (what does it cost?)

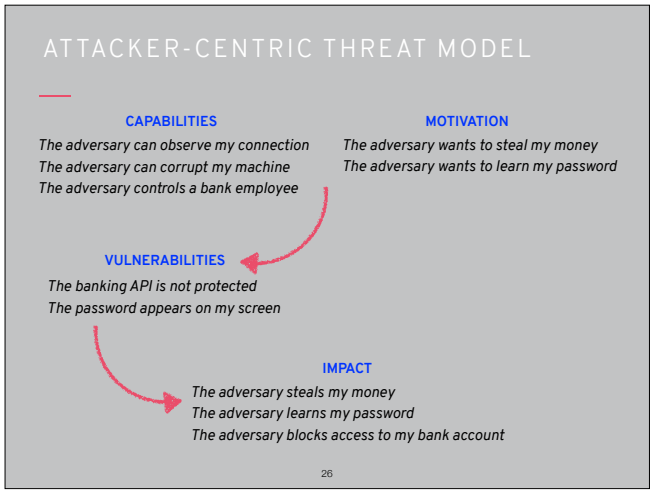
PROTECTION

most of academic computer security is **protection**





All of these factors produce a threat model with a given focus (depending on which factor is prioritised)



Here's an example of a threat model focusing on an attacker wanting to steal money stored in a bank account

SECURITY DESIGN

define

How to ~~design~~ a secure system?

one that meets a specific security policy

How to define a security policy?

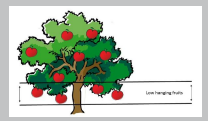
threats, vulnerabilities, likelihood, impact, and cost used to create a **threat model**

27

ASYMMETRY: ADVERSARY VS. DEFENDER

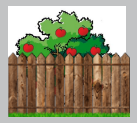
ATTACKER

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



DEFENDER

No adversary strategy can violate the security policy



28

Defender needs to thwart all possible adversaries, whereas attacker just needs to exploit one weakness

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 is not an absolute property, depends on having a good threat model that captures a range of adversarial behaviours

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

We'll be learning about a broad range of security mechanisms