SECURITY (COMP0141):
HUMAN-CENTRED SECURITY

UCL

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**

Let's do one more example of threat modelling, this time with a broad category: personal computing devices.

COMPUTING: THREATS

Threats (who is the adversary?)

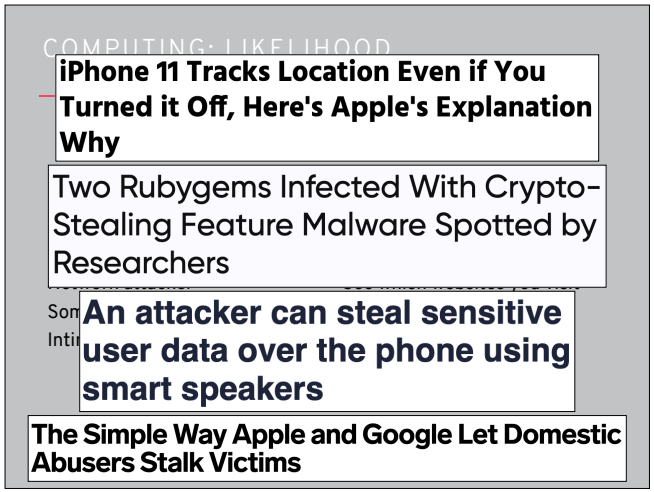
Capabilities?	Motivation?
Device manufacturer	Track your location
Software engineer	Steal your money
Network attacker	See which websites you visit
Someone in close proximity	Steal your credentials
Intimate partner	Stalk you

COMPUTING: VULNERABILITIES

Vulnerabilities (where can system break?)

Capabilities?		Vulnerabilities
Device manufacturer		Owning a computing device
Software engineer		App installation
Network attacker	⇨	Internet connection
Someone in close proximity		Human interaction
Intimate partner		Human interaction

The vulnerabilities here are quite fundamental!



These threats are all quite realistic, and in fact we see them happening frequently.

We could protect against these threats but doing so would have a serious impact on the actual functionality of the system.

DEFINITION OF USABILITY

What is usability?

> a measure of how well a **specific user in a specific context** can use a product/ design to achieve a **defined goal** effectively, efficiently and satisfactorily.

WHAT SHOULD POLICY ADDRESS?

Threats
Vulnerabilities
Likelihood
Impact
Protection
Goals (why are people using this system?)

What is missing here are the actual goals of the users of the system!

IS THE SYSTEM SECURE?

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

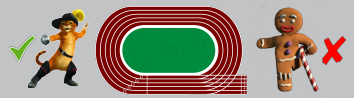
A system is “secure” if an adversary **constrained** by a **specific threat model** cannot violate the **security policy**

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?

Just like security, usability is not absolute.

IS THE SYSTEM USABLE?



Need to instead ask: Is it usable for this user with this goal?

Not all users are the same: employees at a university, older adults, children, women, blind people, refugees, journalists, etc.

Even the same user can act differently (busy, on their laptop, etc.)

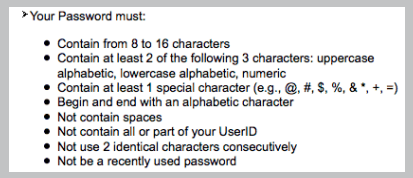
Not all goals are the same: employees use company devices for work, members of the public use mobile devices for social media, communication, gaming, navigation, etc.

USABILITY AND SECURITY

Systems can be “secure” but not usable, and thus insecure

Security policies can:

- Be too complex
- Provide the temptation to cut corners
- Fail to make it clear what the real threats and risks are
- Interfere with what users actually want to do



In fact, we often see that security and security policies might get in the way of the goals of users.

UNINTENTIONAL FAILURES

Security issues can happen due to unintentional failures

- Human error (people make mistakes)
- Non-compliance (“productivity first”)

Why do failures happen?

- Users lack intuition about complex computing devices
- Users are in charge of their own (complex) devices
- It is hard to estimate risks (have the wrong mental model)
- Security measures feel like they get in the way

This leads to security failures as users circumvent or otherwise violate the security policies.

HIDDEN COST: TIME

Security designers may assume that users:

- Can devote time and effort to security-related tasks
- Are motivated by security
- Need more knowledge or training in order to comply if they are not doing so already

These assumptions are all false!

EXAMPLE: BIOMETRIC AUTHENTICATION

EXAMPLE: BIOMETRIC AUTHENTICATION

To use these ePassport gates, users have to:

- Approach the device when the green light comes on
- Put down their bags
- Take their passport out of their bag or pocket
- Remove hats, glasses, etc.
- Insert their passport at (what they think is) the right page
- *Wait for their passport to be scanned and matched (retry if fail)*
- Get into (what they think is) the right position
- *Wait for their image to be captured and matched (retry if fail)*
- Put hat, glasses, etc. back on
- Pick up their bags
- Move away from the device before the gate closes

This all adds up, and takes even longer with infrequent use or for certain user groups

EVALUATING USABILITY

Cognitive walkthrough by usability experts

User studies

- Laboratory experiments
- Diary studies
- Interviews
- Observation of real usage

Data to collect

- Demographics
- Performance (time, success rate, errors)
- Opinions and attitudes
- Actions and decisions

HOW TO IMPROVE

Users lack intuition about complex computing devices →
Provide security education and training

Users are in charge of their own (complex) devices →
Make security invisible

It is hard to estimate risks →
Help users build more accurate mental models

Security measures feel like they get in the way →
Make security the path of least resistance

Just like with security, we'll see that there is no silver bullet and achieving any of these improvements is incredibly difficult to do in general.

QUIZ!

Please go to

`https://moodle.ucl.ac.uk/mod/quiz/view.php?id=2674312`

to take this week's quiz!