SECURITY (COMP0141): WHAT IS SECURITY?

UCL

DEFINITION OF SECURITY

What is security?

> **being** free from danger or threat

> **feeling** safe, stable, and free from fear or anxiety

What is security? Definition is fairly subtle (and it's not just a technical issue)

WHAT MAKES SECURITY SPECIAL?

Correctness: For a given input, a program should provide the correct output

Safety: Well-formed programs cannot have bad (wrong or dangerous) outputs, no matter the input

Robustness: Programs should be able to cope with errors in execution

These properties must hold even in the presence of a **resourceful** and **strategic** adversary

Security is different from other aspects of computer science

THE SECURITY MINDSET

The Security Mindset – Bruce Schneier

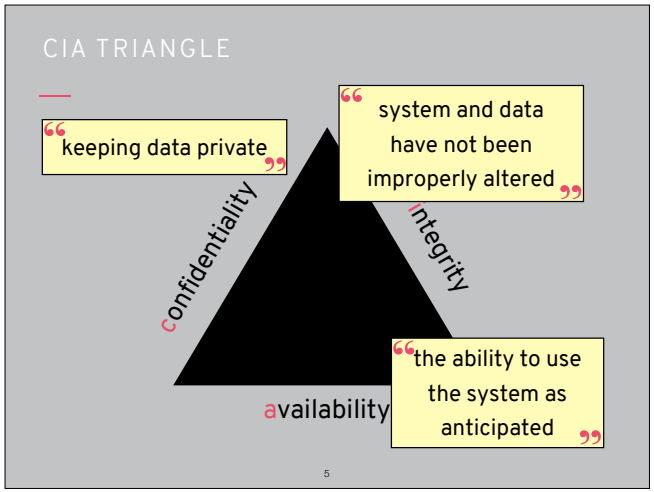
Uncle Milton Industries has been selling ant farms to children since 1956. Some years ago, I remember opening one up with a friend. There were no actual ants included in the box. Instead, there was a card that you filled in with your address, and the company would mail you some ants. My friend expressed surprise that you could get ants sent to you in the mail.

I replied: "What's really interesting is that these people will send a tube of live ants to anyone you tell them to."

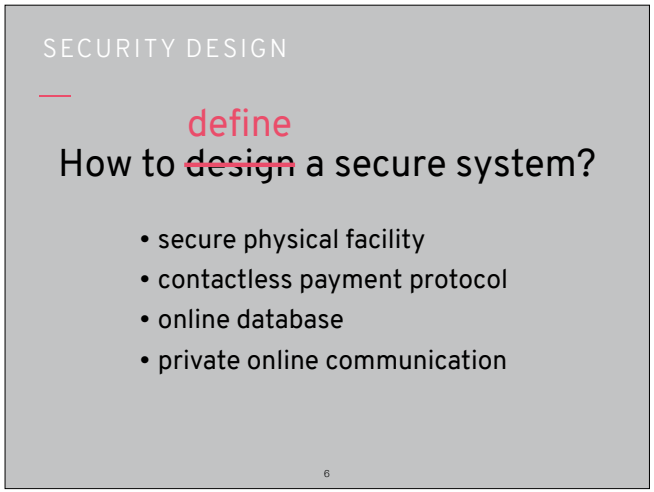
[…]

Good engineering involves thinking about how things can be made to work; ***the security mindset involves thinking about how things can be made to fail****. It involves thinking like an attacker, an adversary or a criminal. You don't have to exploit the vulnerabilities you find, but if you don't see the world that way, you'll never notice most security problems.*

Need to learn to think like an adversary



Most desirable security properties fit into CIA triangle



How to design a secure system? First we need to define a security system, and in particular a system. This term can refer to any member of a diverse set of things (places, protocols, computer resources, etc.).

COMPETING PHILOSOPHIES

7

Two competing philosophies for how to define security

BINARY MODEL

Cryptography

- Attacker has limitations X; define policy Y
- Secure if Y can't be violated without needing X
- E.g., Y = "only authorized users can access data" and X = "valid credentials"

8

BINARY MODEL

Pros:
Longevity

"right" answer gives strong guarantees

Cons:
Brittle
Expensive

hard to define "right"

hard to find "right"

9

RISK MANAGEMENT MODEL

Minimize biggest threats

Focus on cost

10

Consider example of someone driving a car into a building: concrete bollards can't provide perfect security but are cheap and pretty effective

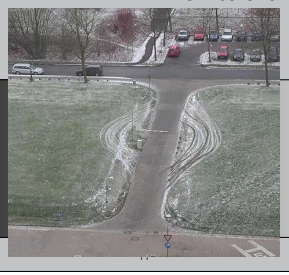
RISK MANAGEMENT MODEL

attack

defense

Pros:
Adaptive

Cons:
Arms race
How to evaluate?



secure

insecure

These solutions are usually quite reactive so lead to an arms race

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?