SECURITY (COMP0141):

WHAT IS SECURITY?

UCL

What is security?

> **being** free from danger or threat

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

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

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."

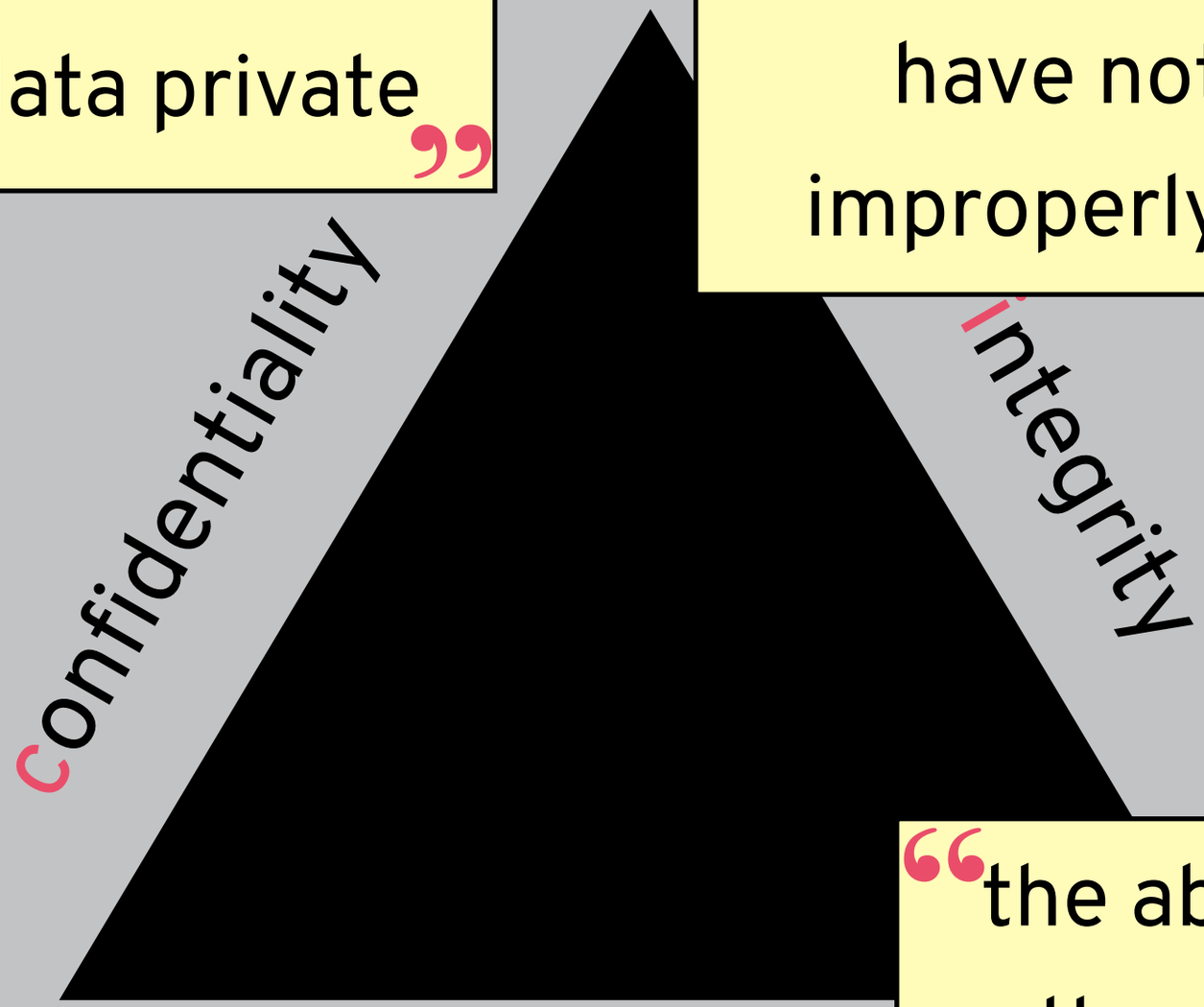
[…]

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*.

CIA TRIANGLE

"keeping data private"

"system and data have not been improperly altered"

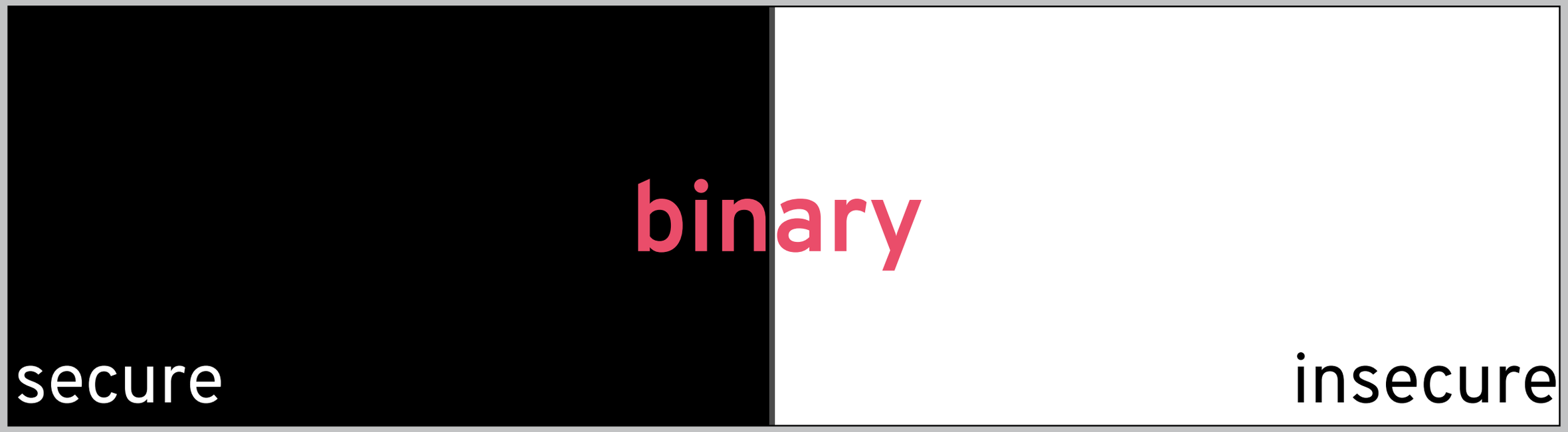


"the ability to use the system as anticipated"

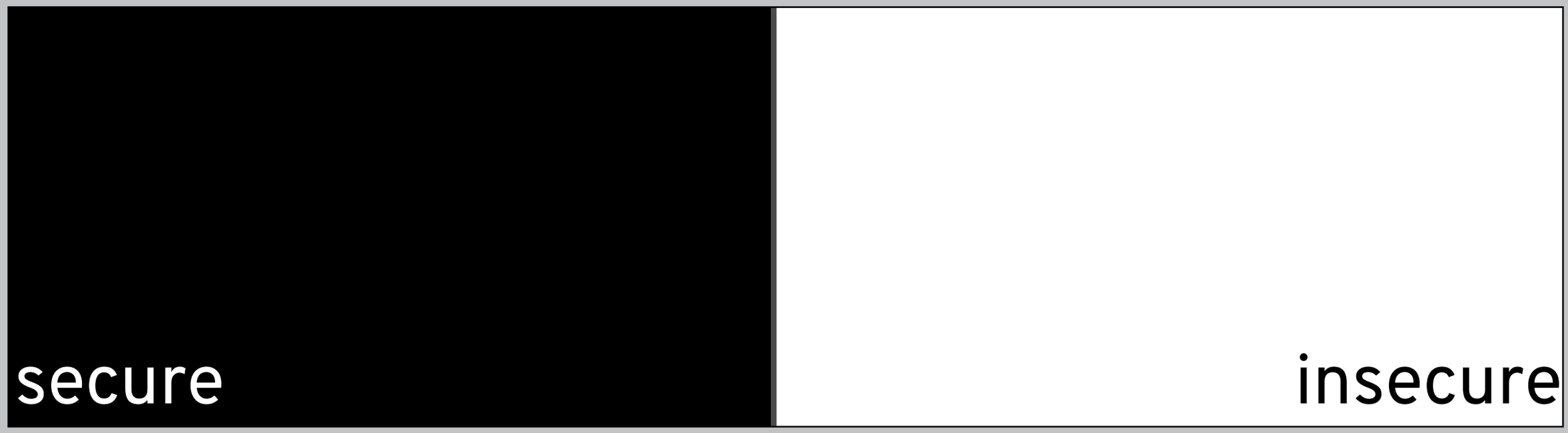
How to ~~design~~ define a secure system?

- secure physical facility
- contactless payment protocol
- online database
- private online communication

COMPETING PHILOSOPHIES



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"

BINARY MODEL

secure

insecure

Pros:

Longevity

"right" answer gives strong guarantees

Cons:

Brittle

Expensive

hard to define "right"

hard to find "right"

RISK MANAGEMENT MODEL

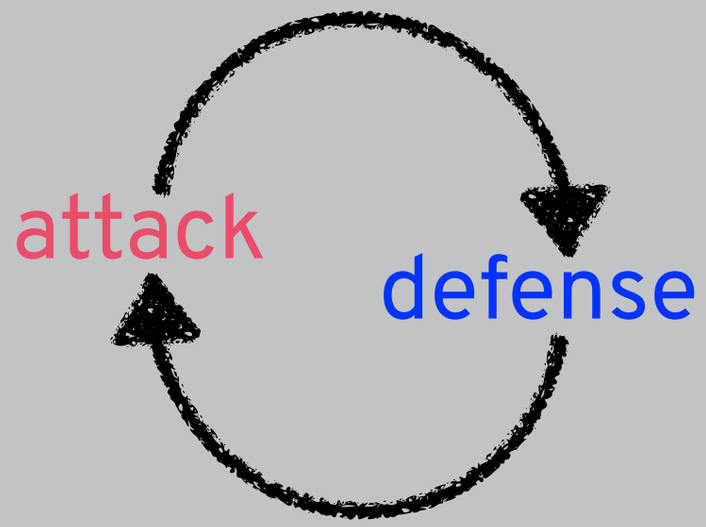
Minimize biggest threats

Focus on cost

secure

insecure

RISK MANAGEMENT MODEL



Pros:

Adaptive

Cons:

Arms race

How to evaluate?

secure

insecure

define

How to ~~design~~ a secure system?

one that meets a specific security policy

How to define a security policy?