SECURITY (COMP0141): DESIGN PRINCIPLES

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**

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

Exam

comp em

what makes security mechanisms good? bad?

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

DESIGN PRINCIPLES

Design principles laid out in a seminal paper: J. Saltzer and M. Schroeder. *The Protection of Information in Computer Systems.* SOSP 1973 (Introduction and Section 1)

(security mechanisms)

"The term 'security' describes **techniques** that control who may use or modify the computer or the information contained in it."

"Principles **guide** the design and contribute to an implementation without security flaws"

https://www.acsac.org/secshelf/papers/protection_information.pdf

DESIGN PRINCIPLES [SS'73]

Least privilege

Separation of responsibilities

Complete mediation

Fail-safe default

Defence in depth

Open design

Psychological acceptability

Economy of mechanisms

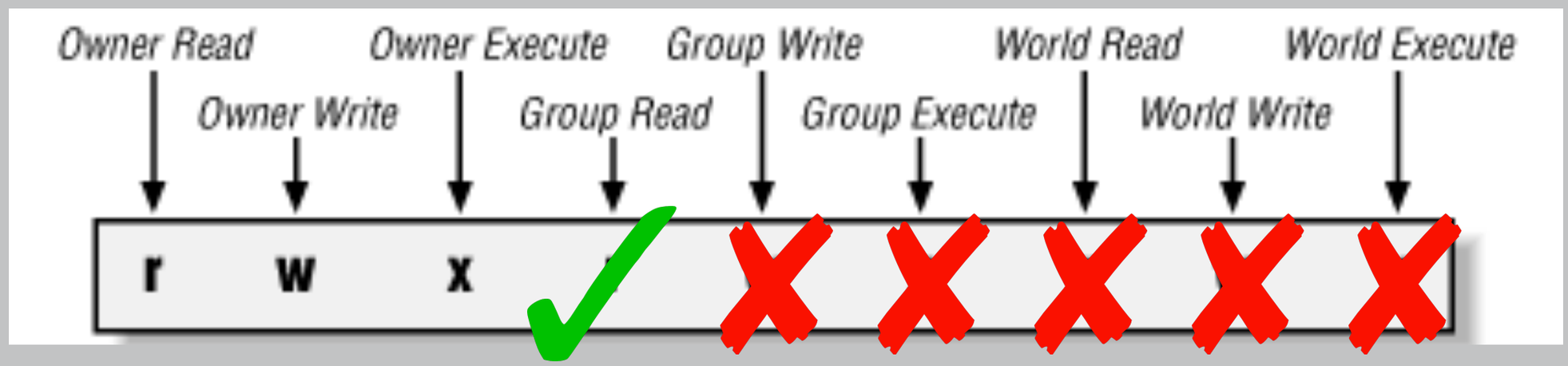
Least privilege

LEAST PRIVILEGE

What are the minimum privileges needed?

door entry

reading files



SEPARATION OF RESPONSIBILITIES

Least privilege

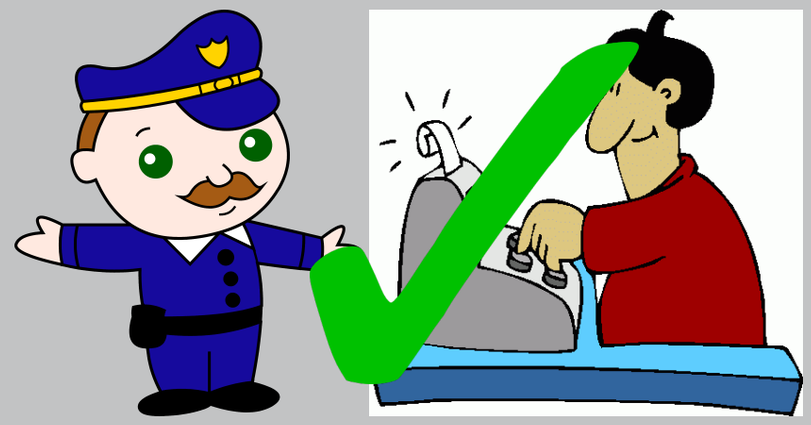
Separation of responsibilities

SEPARATION OF RESPONSIBILITIES

(accidentally or maliciously)

Can one person destroy the system's security?

shoplifting



system maintenance

database admin

=

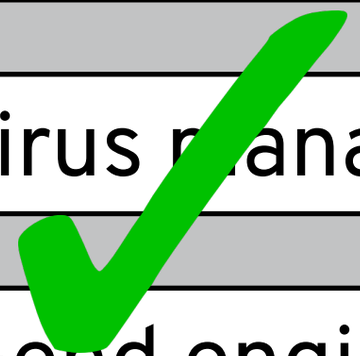
antivirus manager

front-end engineer

database admin

antivirus manager

front-end engineer



COMPLETE MEDIATION

Least privilege

Separation of responsibilities

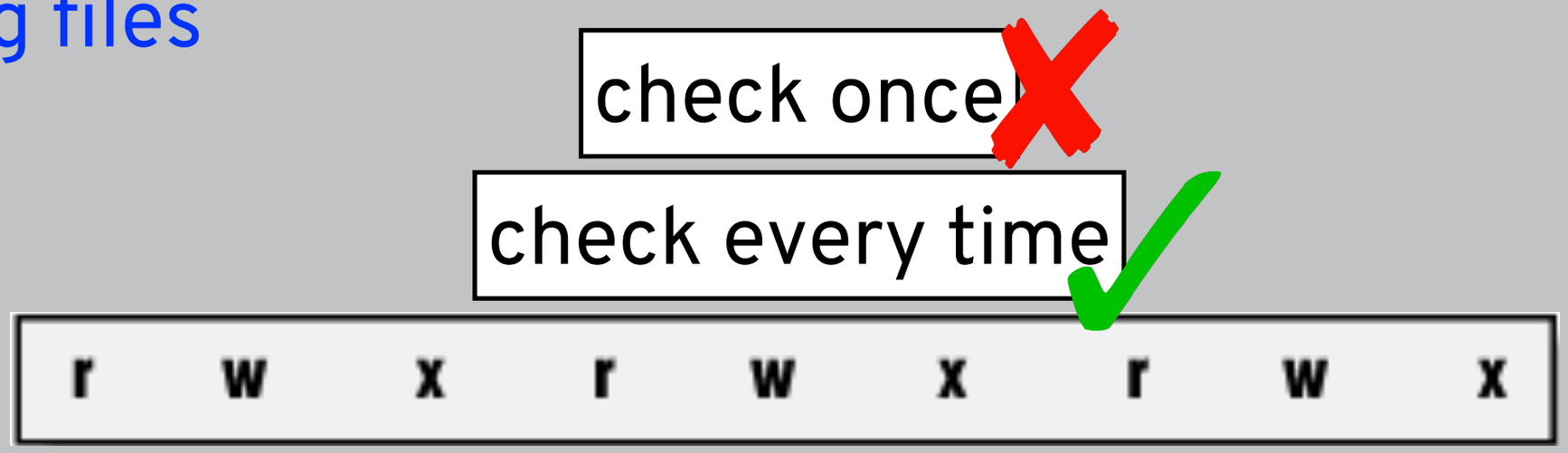
Complete mediation

COMPLETE MEDIATION

Can we tightly control access to objects?

entry point

reading files



FAIL-SAFE DEFAULT

Least privilege

Separation of responsibilities

Complete mediation

Fail-safe default

FAIL-SAFE DEFAULT

Is the default setting good for security?

luggage carts

accessing outside internet

Least privilege

Separation of responsibilities

Complete mediation

Fail-safe default

Defence in depth

DEFENCE IN DEPTH

Do we have more than one security measure?

door entry

browser extensions

(my opinion!)

OPEN DESIGN

Least privilege

Separation of responsibilities

Complete mediation

Fail-safe default

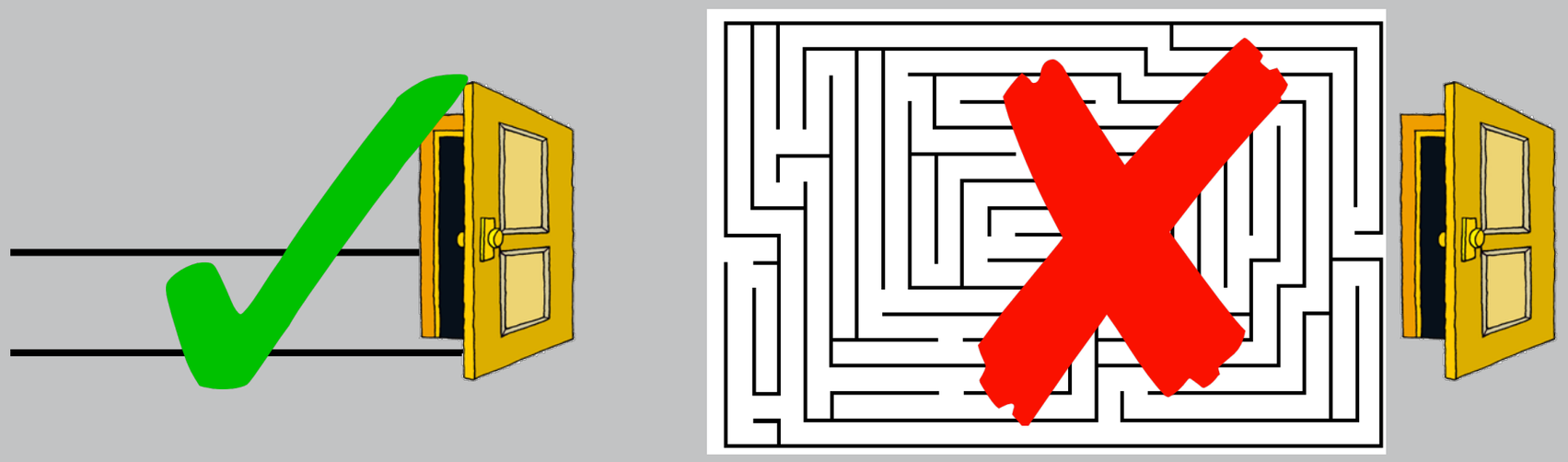
Defence in depth

Open design

OPEN DESIGN

Are we relying on “security by obscurity?”

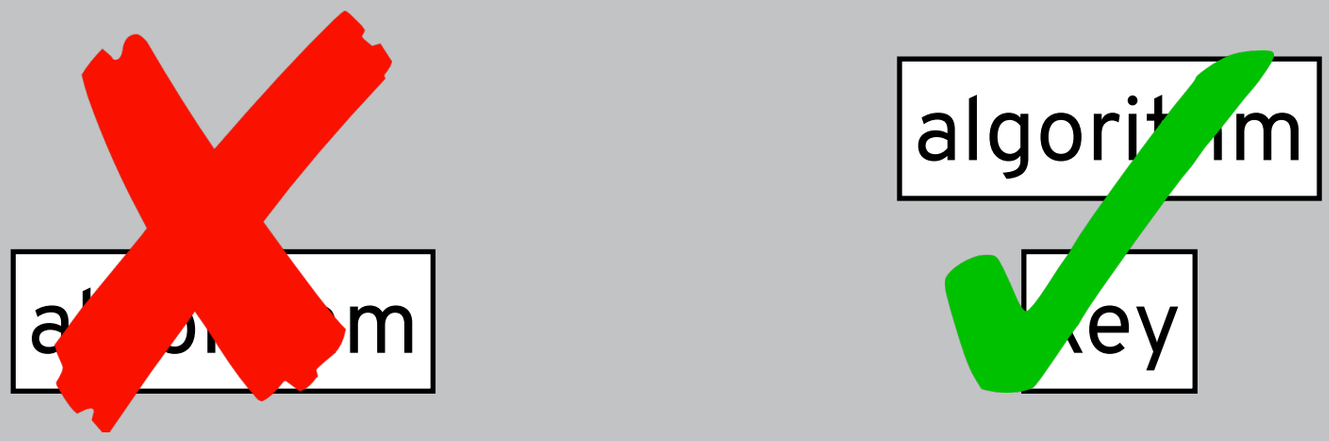
door entry



encryption

public:

secret:



PSYCHOLOGICAL ACCEPTABILITY

Least privilege

Separation of responsibilities

Complete mediation

Fail-safe default

Defence in depth

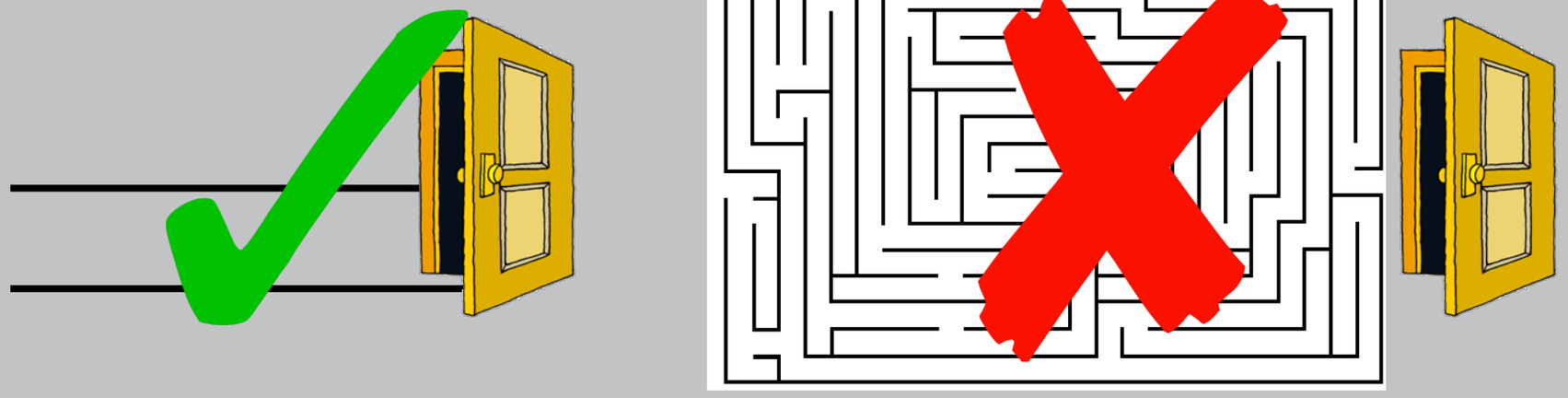
Open design

Psychological acceptability

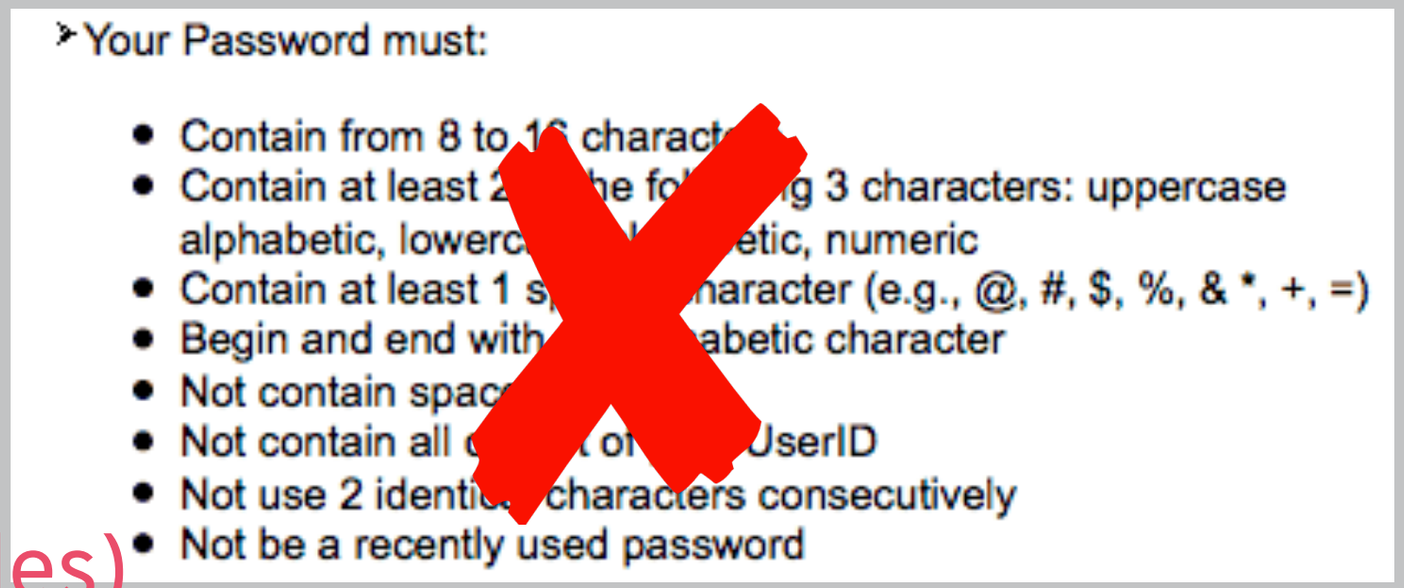
PSYCHOLOGICAL ACCEPTABILITY

Are users willing to follow security guidelines?

door entry



passwords



(tension between principles)

ECONOMY OF MECHANISMS

Least privilege

Separation of responsibilities

Complete mediation

Fail-safe default

Defence in depth

Open design

Psychological acceptability

Economy of mechanisms

ECONOMY OF MECHANISMS

KISS principle: Keep it simple, stupid!

(tension between principles)

TRUSTED COMPUTING BASE (TCB)

Trusted computing base (TCB) refers to every component of the system upon which the security policy relies (could be hardware, software, etc.)

In other words, if something goes wrong then the security policy may be violated

This needs to be kept small!

This is an example of economy of mechanisms (could just think of entire system as TCB but this is very unrealistic)

DESIGN PRINCIPLES [SS'73]

Least privilege

Separation of responsibilities

Complete mediation

Fail-safe default

Defence in depth

Open design

Psychological acceptability

Economy of mechanisms

DESIGN PRINCIPLES (UPDATED)

Least privilege

Separation of responsibilities

Threats

Vulnerabilities

Likelihood (might this happen?)

ediation (within reason)

efault (within reason)

depth (within reason)

~~Open design~~ Study of attacks

Psychological acceptability

Economy of mechanisms

DESIGN PRINCIPLES (UPDATED)

Least privilege

Separation of responsibilities

Complete mediation (within reason)

Fail-safe default (within reason)

Defence in depth (within reason)

~~Open design~~ Study of attacks

Psychological acceptability

Economy of mechanisms

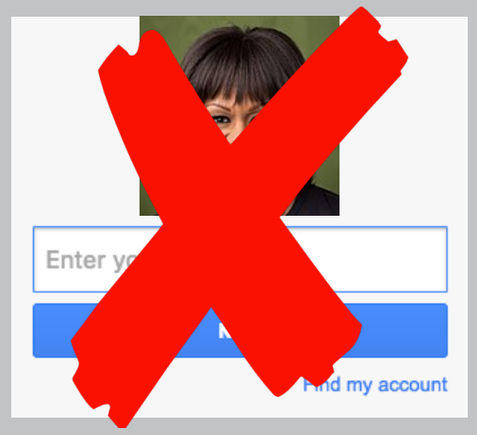
Prudent paranoia

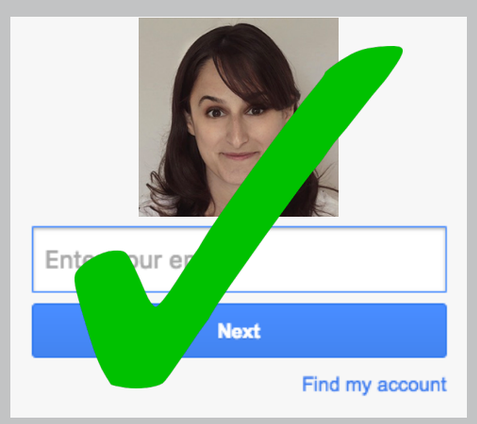
PRUDENT PARANOIA*

Don’t underestimate effort adversary will go to!

codebreaking

email security





*a.k.a. “Just because you’re paranoid doesn’t mean they aren’t after you.” (Joseph Heller, *Catch-22*)

DESIGN PRINCIPLES (UPDATED)

Least privilege

Separation of responsibilities

Complete mediation (within reason)

Fail-safe default (within reason)

Defence in depth (within reason)

~~Open design~~ Study of attacks

Psychological acceptability

Economy of mechanisms

Prudent paranoia

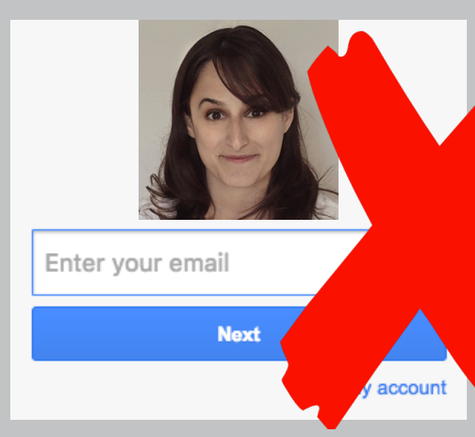
Privacy promotion

PRIVACY PROMOTION

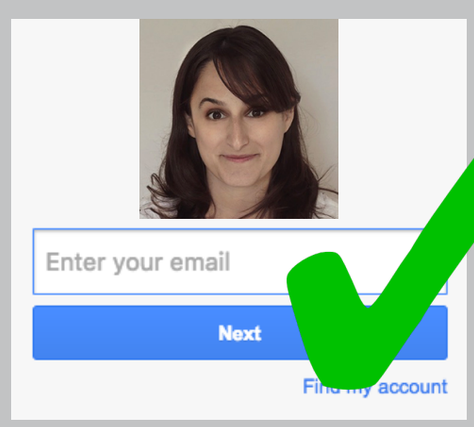
Don’t collect more data than strictly necessary

CCTV

site visitors

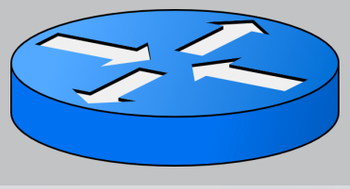


C ome
ondon
28.40.1.76
280 x 720
Mac OS X
English
…

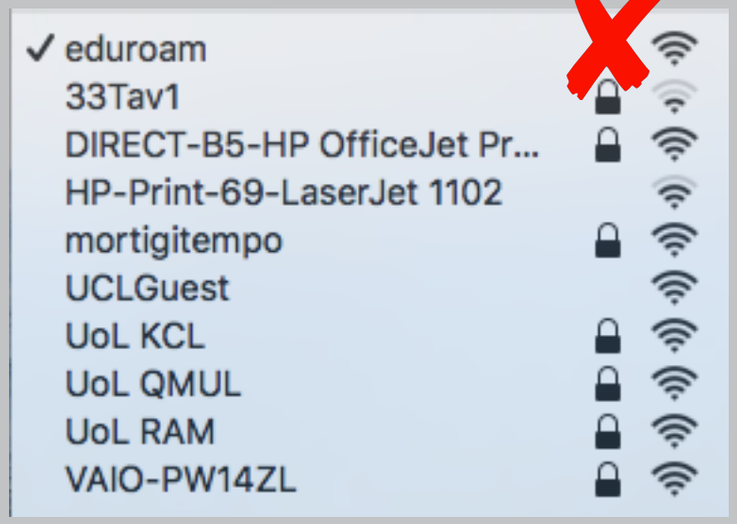


Lo don
28.40.1.76

CASE STUDY



(no WEP/WPA)



Least privilege

Separation of responsibilities

Complete mediation

Fail-safe default

Defence in depth

Open design

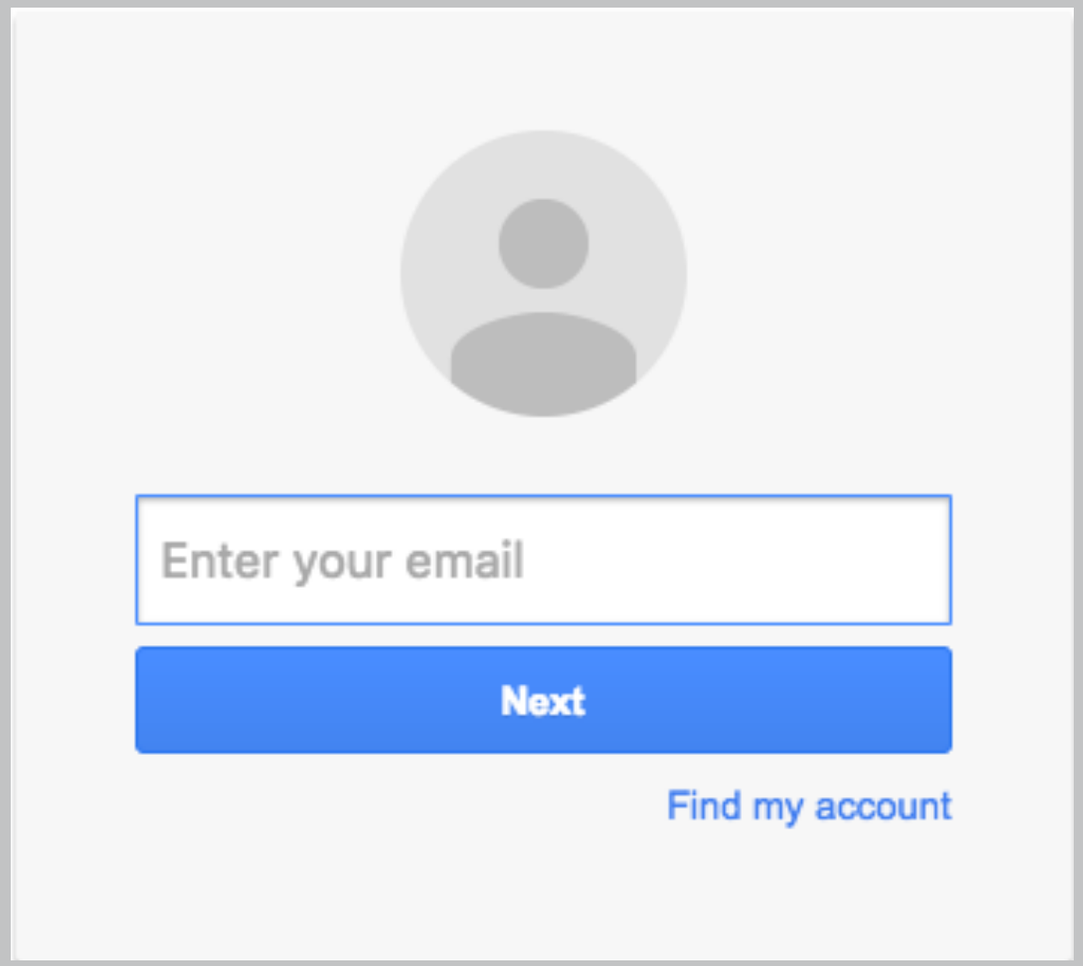
Psychological acceptability

Economy of mechanisms

Prudent paranoia

Privacy promotion

CASE STUDY



Defence in depth?

-lock out after too many attempts
-additional questions if unknown IP
-education about good passwords
-education about phishing
-two-factor authentication

Privacy promotion?

-strong protection on password file
-don’t store passwords in the clear
-don’t store list of all previous logins

DESIGN PRINCIPLES

Principles allow us to identify safe and unsafe patterns in the security engineering process

Do not use them as a blind checklist!

Need to re-assess whether or not principles are satisfied after composing security components together: new ones may increase security (defence in depth) or decrease it (“weakest link”)

Security + security ≠ security