SECURITY (COMP0141): DESIGN PRINCIPLES

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 go back and look at the question of how to design a security system

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

what makes security mechanisms good? bad?

em

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

Remember that last week we said security mechanisms were the way we achieved security. But what about their design?

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

We'll consider design principles laid out in a now-classic paper by Saltzer and Schroeder, which guide the choice of security mechanism

DESIGN PRINCIPLES [SS'73]

Least privilege
Separation of responsibilities
Complete mediation
Fail-safe default
Defence in depth
Open design
Psychological acceptability
Economy of mechanisms

We'll go through eight design principles from the paper. For each one we'll demonstrate them using physical and digital examples

LEAST PRIVILEGE

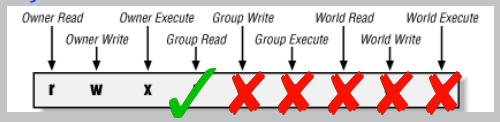
Least privilege

LEAST PRIVILEGE

What are the minimum privileges needed?

door entry

reading files



7

Least privilege says that every part of the system should have the minimum privileges need to operate. We'll see UNIX permissions (the digital example) later in the module

SEPARATION OF RESPONSIBILITIES

Least privilege

Separation of responsibilities

8

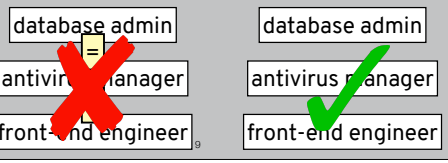
SEPARATION OF RESPONSIBILITIES

(accidentally or maliciously)

Can one person destroy the system's security?

shoplifting

system maintenance



9

Separation of responsibilities says that everyone should have a different job to do, otherwise there's a single point of failure that can take down the system

---

COMPLETE MEDIATION

Least privilege

Separation of responsibilities

Complete mediation

10

COMPLETE MEDIATION

Can we tightly control access to objects?

entry point

reading files

check once

check every time

r w x r w x r w x

Complete mediation says that we should be able to keep track of all accesses to sensitive objects in the system

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

Fail-safe default says that the default setting or behaviour should be one that's good for security

DEFENCE IN DEPTH

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!)

Defence in depth says that we have multiple forms of protection (so if one fails we're still okay)

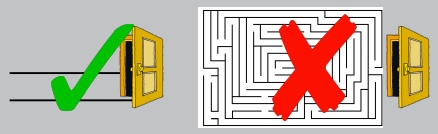
OPEN DESIGN

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: algorithm

secret: algorithm key

Open design says that we’re using established standards for protection, otherwise if we rely on secrets then we have no security left if someone
finds them out

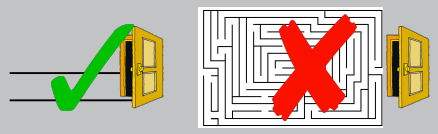
PSYCHOLOGICAL ACCEPTABILITY

Least privilege
Separation of responsibilities
Complete mediation
Fail-safe default
Defence in depth
Open design
Psychological acceptability

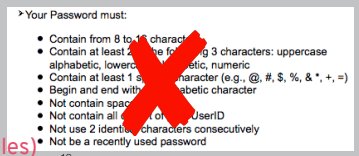
PSYCHOLOGICAL ACCEPTABILITY

Are users willing to follow security guidelines?

door entry



passwords



(tension between principles)

Psychological acceptability says that the measures can't be too cumbersome, otherwise people won't use them so we won't get security anyway. This is somewhat in contrast to other 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)

Economy of mechanisms says that we shouldn't make the system too complicated. This is also somewhat in contrast to other principles (e.g.,
defence in depth)

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)

Trusted computing base needs to be kept small

DESIGN PRINCIPLES [SS'73]

Least privilege
Separation of responsibilities
Complete mediation
Fail-safe default
Defence in depth
Open design
Psychological acceptability
Economy of mechanisms

23

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

24

In modern times, we want to consider updated versions of these principles and will add two more. First of all, there are now many "security" products out there, so we need to consider the likelihood of our system being attacked; we shouldn't spend millions to protect secrets worth hundreds (think about different passwords you use to manage different online accounts). Also, open design is not enough: we should actively try to attack existing standards and systems and use only measures that stand up to this

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

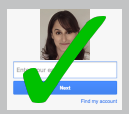
25

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*)

26

Prudent paranoia says that we shouldn't assume that our data/ accounts aren't valuable to someone, it's not all just conspiracy theories

DESIGN PRINCIPLES (UPDATED)

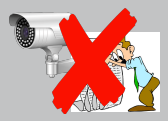
Least privilege
Separation of responsibilities
Complete mediation (within reason)
Fail-safe default (within reason)
Defence in depth (within reason)
~~Open design~~ Study of attacks
Psychological acceptability
Economy of mechanisms
Prudent paranoia
Privacy promotion

27

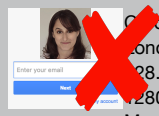
PRIVACY PROMOTION

Don't collect more data than strictly necessary

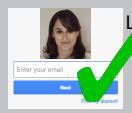
CCTV



site visitors



Chrome
London
28.40.1.76
1280 x 720
Mac OS X
English
…



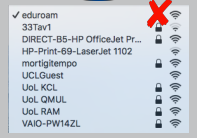
London
28.40.1.76

28

Privacy promotion is especially important today, and says that we should collect only the data that our system needs. Most existing systems do not do this

CASE STUDY

(no WEP/WPA)

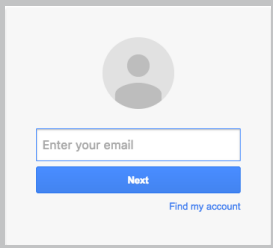


Least privilege
Separation of responsibilities
Complete mediation
Fail-safe default
Defence in depth
Open design
Psychological acceptability
Economy of mechanisms
Prudent paranoia
Privacy promotion

29

Example of unsecured wifi

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

30

Example of email login

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