FIT 1047

Introduction to computer systems, networks and security

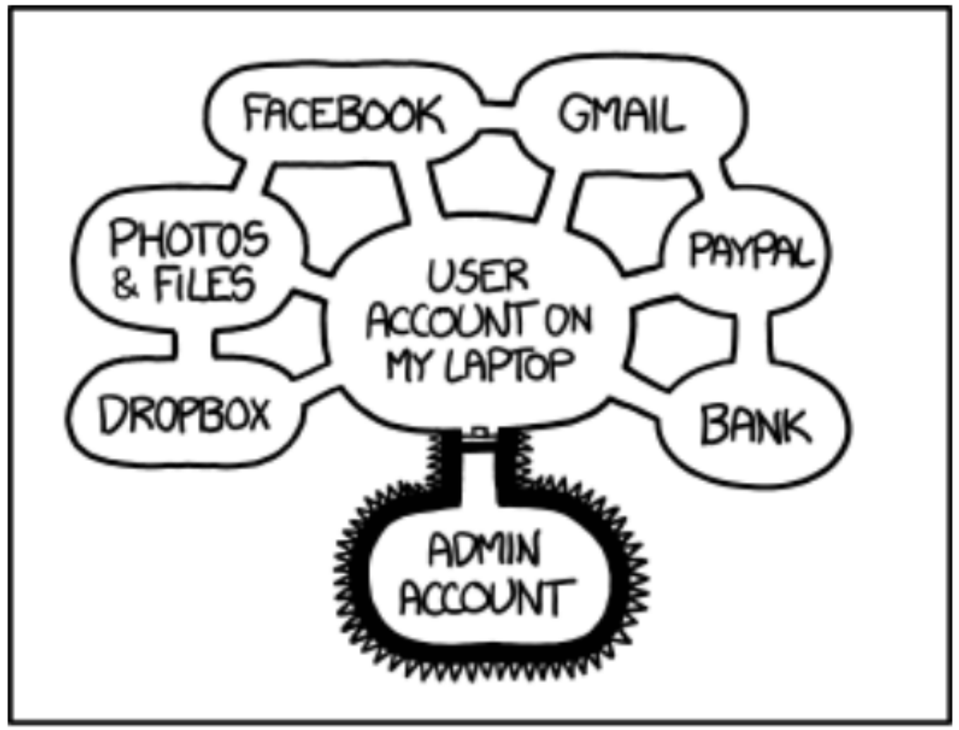
Space	Forward
Right, Down, Page Down	Next slide
Left, Up, Page Up	Previous slide
P	Open presenter console
H	Toggle this help

MONASH University

Assignment 1

- Upload one single zip file
- Deadline next week Friday September 7th 11:55pm
- Late submission is possible (with a penalty). One day late means minus 5 % of the mark.

Space	Forward
Right, Down, Page Down	Next slide
Left, Up, Page Up	Previous slide
P	Open presenter console
H	Toggle this help



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,

BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

(xkcd.org)

A central question in cyber security is about who (persons, processes, devices, etc.) has access to which resources in the system.

Resources: read files, execute programs, change data-base content, share data with others, etc.

ACCESS CONTROL

Questions

- How to identify who wants to use a device/service?
- How to protect files from being accessed / changed by users on the same device?
- How to protect transactions in an application?

How to authenticate a person?

- Identify at login
- Authenticate particular transactions

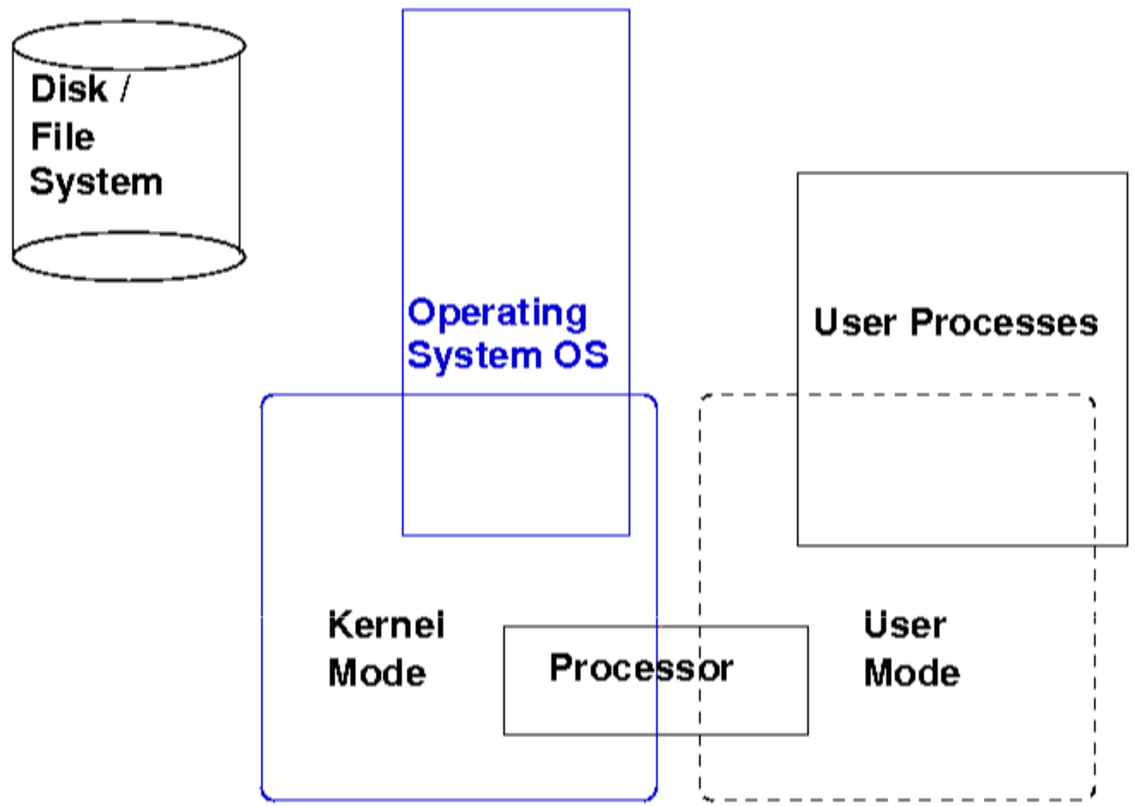
Identity -> Authentication:

Most common: password

Problems with passwords:

- Password re-use
- Weak passwords
- Can be stolen through Phishing / Malware
- Stored passwords
- Difficult to remember / reset processes

Lets look at the use of a password in a computer


Disk /
File
System
Operating
System OS
User Processes
Kernel
Mode
Processor
User
Mode

How not to store a password

- In cleartext

How not to store a password

- In cleartext
- As a hash value

Better ways to store a password

Use a salted hash

- The Password is the most commonly used way
- Multi-factor authentication combines different ways of authentication

(Wikimedia Commons)

Biometrics

- Fingerprints
- Voice recognition
- Iris scans
- Others

- Biometrics have high usability
- Not really secret information
- Cannot be revoked/replaced
- No pseudonymous/anonymous access

Hardware Tokens

- Separate device / additional security
- Note that even with secure authentication, the computer can still be attacked

(Wikimedia Commons)

Authentication of Transactions

- E.g. for money transfer in banking
- Tansaction numbers (TANs) are not linked to actual transaction
- SMS TAN can show info on transaction. Two devices need to be manipulated.
- TAN generator reads barcode from screen and generates TAN linked to transaction.

Access control on Operating System level

- Distinguish users, groups of users
- Controls access to files, ports, devices, and other resources
- User authentication (e.g. password, fingerprint)
- Allocate processes to users and enforce separation
- OSs can support complex policies for individual programs (e.g SELinux)

Basic file permissions (Linux)

- Main actions are read, write, execute
- Can be defined for owner, group, all users

Access rights:

- r permission to read
- w permission to write
- x permission to execute
- - no permission at all

xrwxr_x__ someuser somegroup some-file

- Owner (someuser): xrw
- Group (somegroup): xr_
- All users: x__

Access control on application level

- This is what user usually can see (and also configure)
- Often complex security policies
- Enterprise applications: Staff with various roles, and fine-grained access to transactions
- Social networks: Rules on who can see, copy, forward, search what data.

Access control in enterprise applications

- Can enforce protection properties.
- Controls access to resources, data-bases, transactions, etc.
- Can be role-based (not just user-based)

- Ticket or token-based access control.
- A central server checks authenticity and issues tickets.
- Ticket contains identity information and can also restrict capabilities (i.e. what is the user allowed to do)
- Example: Kerberos, Microsoft Active Directory

Single sign-on

- Just log in once and access many services (e.g. Monash University authcate)
- Very convenient. High usability
- Single point of failure. Needs secure implementation and high level of control.

- Main goal of access control: limit the damage that can be done by users, groups of users.
- Privilege escalation is a goal for attacks
- Many ways how access control can go wrong

What can go wrong?

- Weaknesses in software, interfaces, protocols
- Physical attacks
- Race conditions, feature interaction problems
- Connect devices (USB)
- Social engineering

Additional security mechanisms

- Hard disk encryption
- Virus protection
- Backups
- Security updates
- Trusted Computing (special security hardware)