COS30015 IT Security

Live Lecture Week 3

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

REFLECTION WEEK

SEMESTER 2
WEEK 3

TIME TO MAKE
DECISIONS

CENSUS DATE
31
AUG

Get help to make
informed decisions about
your studies before Census date

Drop-in sessions

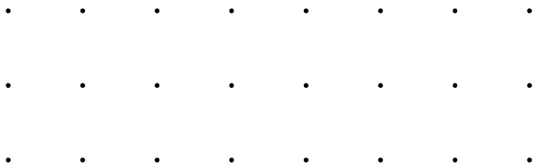
Tuesday 16 to Thursday 18 August
11am to 2pm daily
Atrium

LEARN MORE & FIND SUPPORT

swi.nu/reflect222

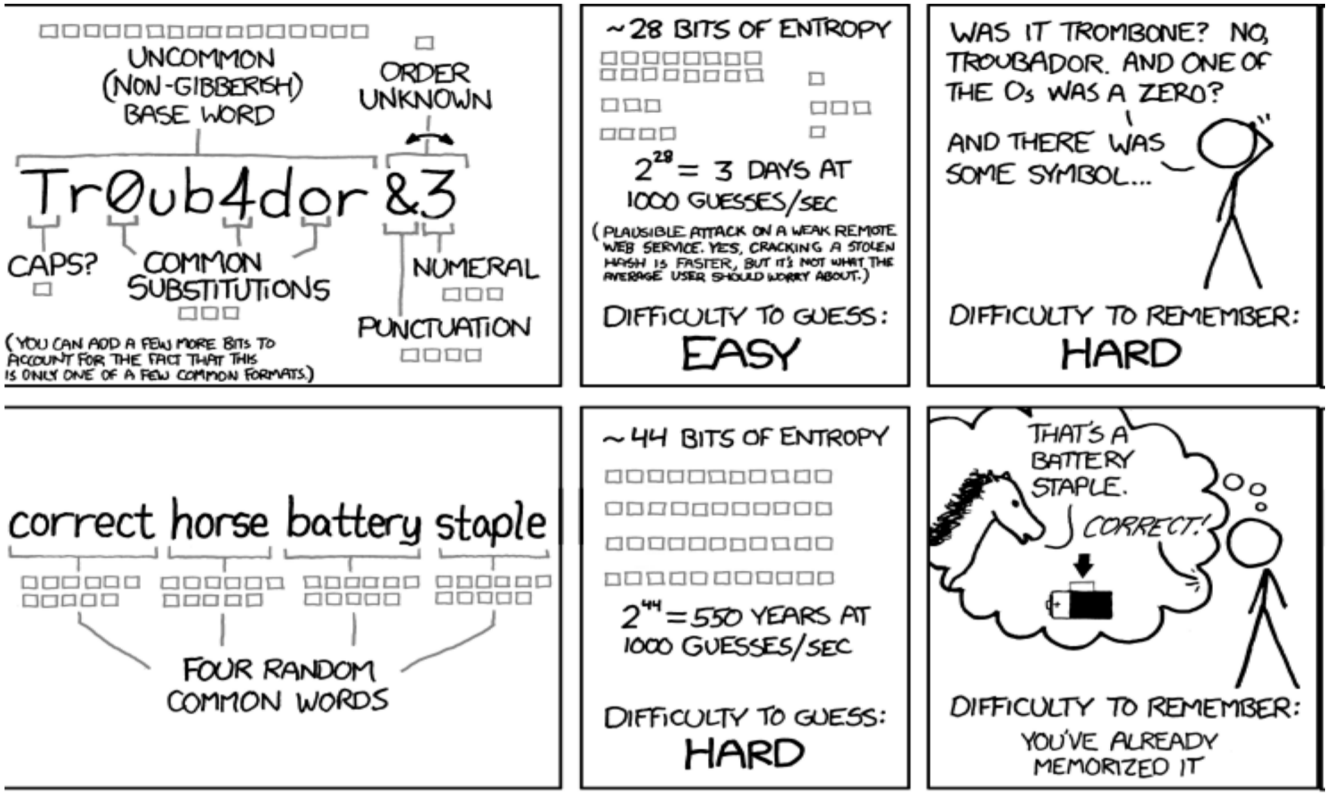
laurendobson@swin.edu.au

SWINBURNE UNIVERSITY OF TECHNOLOGY



Password-based Authentication

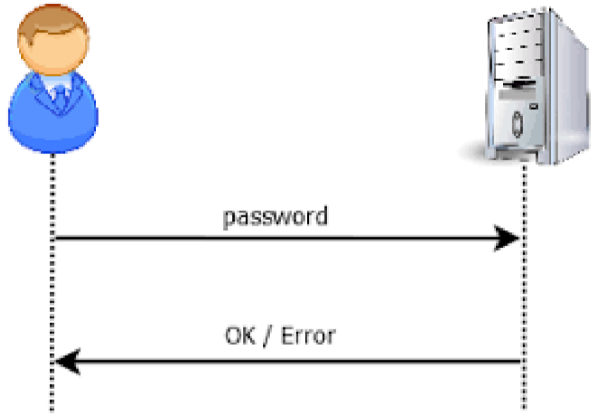
Password-based authentication



Password-based authentication

- Passwords are susceptible to *keylogging*, brute-force and dictionary attacks and can too often be obtained or guessed using social engineering techniques.

- The success of a brute-force attack depends on the size of the password/pin.
  - A 4-digit pin can be guessed after 5000 tries ((9999 – 0000)/2).
  - A 6-digit pin takes 500,000 guesses.
  - A 6 character password using lower-case letters takes 150 million guesses.



SWIN BUR NE
SWINBURNE UNIVERSITY OF TECHNOLOGY

Password-based authentication

- These passwords can be 'cracked' easily using existing software that automates the login process.

- Dictionary attack - SSH-brute.c
  - A 6-character password using upper and lower case letters, numbers and symbols (62 possible characters) will take about 28 billion guesses.
  - Increasing the number of characters to 8 improves things by a factor of 256,000 to 110,000 billion attempts needed.
  - Passwords of this size can still be guessed, but it takes an inconvenient time.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Password-based authentication

- If the password can be guessed, the speed of cracking increases dramatically.
- A dictionary attack may take as few as 85,000 guesses (171,000 words in the Oxford English Dictionary).
  - Try HashCat (in Kali VM)
  - Bad guys know how people "disguise" their passwords or append them to satisfy password policies. Most common modifications are scriptable.
- Most passwords are now 8 characters
  - Default passwords are by design easy to remember (short)!

SWINBURNE UNIVERSITY OF TECHNOLOGY

Password-based authentication

Don't write the password down.

http://www.theregister.co.uk/2005/08/10/kutztown_13/

If you really have to write it down, keep it in your wallet with your money. Don't write down what it's for.

Password storage?

SIMS synchronizes passwords for all accounts

- password re-use

Browsers store passwords

- in plain text

Password Managers

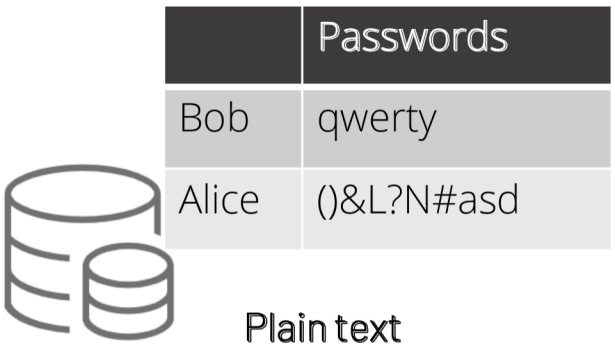
- only as safe as the master password.

Allow for *escrow*

PROTECT YOUR PASSWORDS

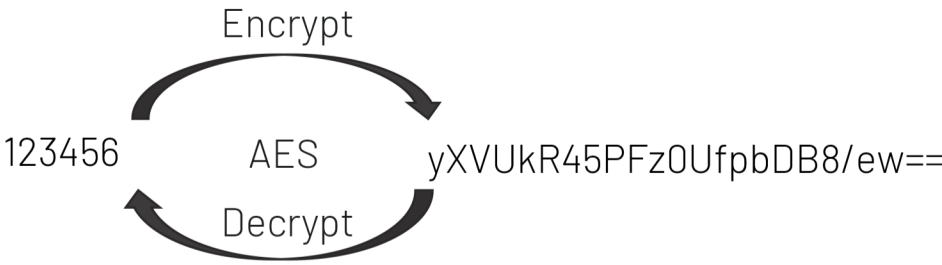
SWINBURNE UNIVERSITY OF TECHNOLOGY

Password-based authentication



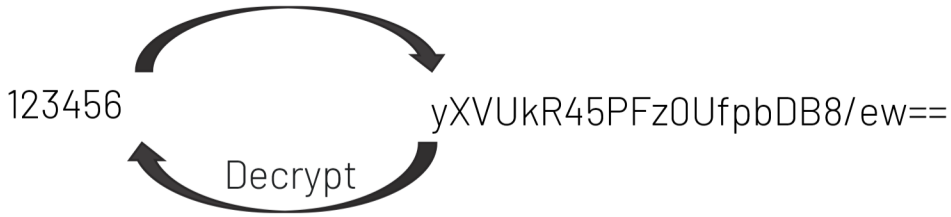
	Passwords
Bob	qwerty
Alice	()&L?N#asd

Plain text



Encryption

Password Salt



Hash

Username	Salt	Password
Bob	VNc4BdR20n	5ee235f4179b6da118c61b55d99caae88449d88a96f278a5e390e50ca424ff7b
Alice	zWQC6k6n1	fba3114d73562c3aac845b966689fa2e2c0704c6b702d2d6fca441e7a056682c

Completely different

Hash+Salt

https://emn178.github.io/online-tools/sha1.html

Password policy

- To minimise the risk of a password being guessed, each password should be
  - long,
  - random,
  - different.
- A password policy can be used to develop an algorithm for re-creating different passwords for each account:
- Mixtures of case and character substitution can be used as well.
  - e.g. mYPa55w0rd
- An entirely random password can be stored in a text file and copied into web forms as needed.

SWINBURNE UNIVERSITY OF TECHNOLOGY

What's in this week's lab?

- Lecture Topic --- Operation System Security
- Lab Task --- Buffer Overflow

SWIN BUR NE
SWINBURNE UNIVERSITY OF TECHNOLOGY

Task List for Week 3

- ❑ **Lecture Activity**
  - ❑ Video-streaming lecture
- ❑ **Complete this week's Lab Task**
- ❑ **ASSIGNMENT 1**
- ❑ **Suggest: external readings in Week 3 Module**

SWINBURNE UNIVERSITY OF TECHNOLOGY

Next Week --- Guest Lecturer

- **Topic: “Data Privacy Preservation”**
- **Guess Lecturer: Ding, Ming**
  - --- Senior Research Scientist at CSIRO