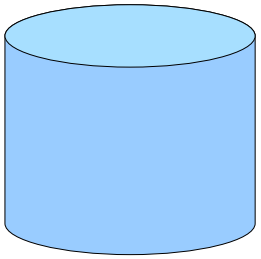
Integrity policies via a library in Haskell

Alejandro Russo
russo@chalmers.se

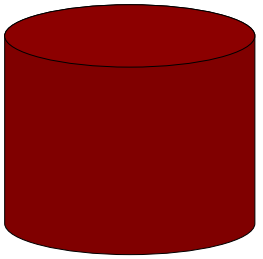
(joint work-in-progress with Albert Diserholt)

Password administrator

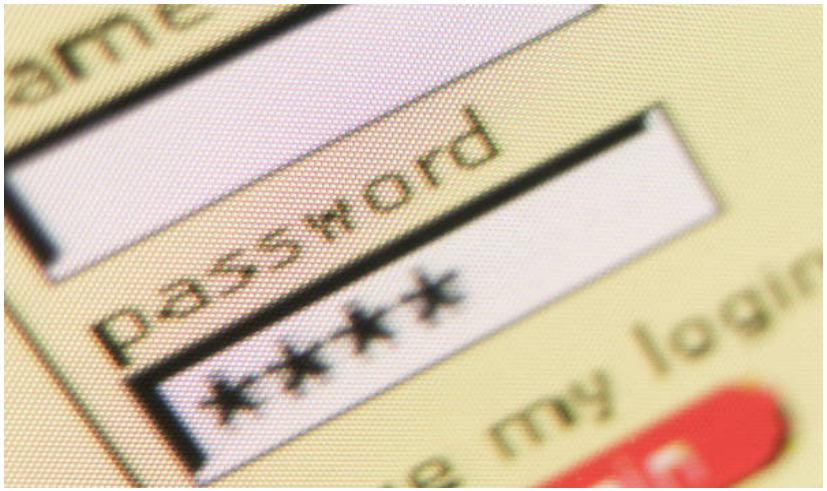
- Password administrators are commonly found in browsers, mobiles phones, desktop computers, etc.
- Inspired by Linux's Shadow Password Suite.
- Provide an API to manage passwords and perform authentication.
  - Root permission!



/etc/passwd



/etc/shadow



Challenges when designing the API

- Security concerns?
  - Confidentiality
  - Integrity
- Password should not be leaked.
  - Offline dictionary attacks
- Password can be destroyed or manipulated.
  - Denial of service attacks.
  - Facilitate penetration of systems.

Module	Confidentiality	Integrity
Login	Information to leak: comparation of password with user input. Otherwise, password must not be leaked.	File **passwd** and **shadow** can only be read.
Reset	Passwords must not be leaked.	File **passwd** can only be read, while **shadow** can be read and written. New password must be difficult to guess.
Backup	Password must not be leaked unless they are safely encrypted.	File **passwd** and **shadow** can only be read.
Encrypt	Passwords must not be leaked.	User input must not affect the generation of random numbers.

Module	Confidentiality	Integrity
Login	Information to leak: comparation of password with user input. Otherwise, password must not be leaked.	File **passwd** and **shadow** can only be read.
Reset	Passwords must not be leaked.	File **passwd** can only be read, while **shadow** can be read and written. New password must be difficult to guess.
Backup	Password must not be leaked unless they are safely encrypted.	File **passwd** and **shadow** can only be read.
Encrypt	Passwords must not be leaked.	User input must not affect the generation of random numbers.

Access Control

Module	Confidentiality	Integrity
Login	Information to leak: comparation of password with user input. Otherwise, password must not be leaked.	File **passwd** and **shadow** can only be read.
Reset	Passwords must not be leaked.	File **passwd** can only be read, while **shadow** can be read and written. New password must be difficult to guess.
Backup	Passwords must not be leaked unless they are safely encrypted.	File **passwd** and **shadow** can only be read.
Encrypt	Passwords must not be leaked.	User input must not affect the generation of random numbers.

Access Control

Data invariants

Module	Confidentiality	Integrity
Login	Information to leak: comparation of password with user input. Otherwise, password must not be leaked.	File **passwd** and **shadow** can only be read.
Reset	[illegible]	File **passwd** can only be read, while **shadow** can be read and written. New password must be difficult to guess.
Backup	[illegible] leaked unless they are safely encrypted.	File **passwd** and **shadow** can only be read.
Encrypt	[illegible]	User input must not affect the generation of random numbers.

Access Control

Data invariants

Information-flow