TÉCNICO LISBOA

PASSWORD GENERATION

RUI LIMA 94073

INTRODUCTION

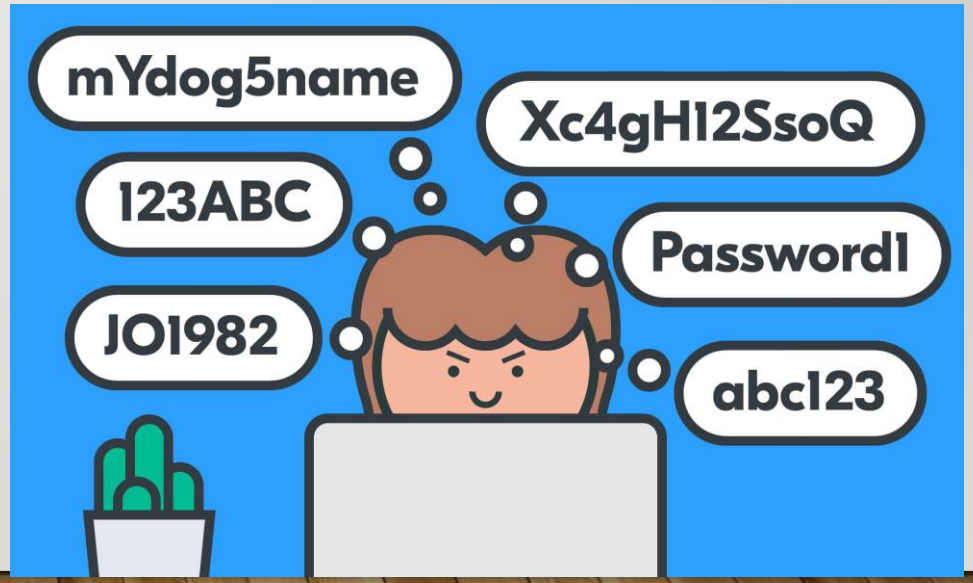
- What is password manager.
- Solution.
- Demonstration.
- Conclusions.

2 PASSWORD MANAGERS

- Stores the user passwords.
- Generates new passwords.
- Automatically fills the passwords to the respective applications.

3 ADVANTAGES

- No need to memorize all the passwords.
- Password generated automatically following specific rules.
- New laws in consumer electronics.



4 DISADVANTAGES

- Passwords are available in a database.
- Does the password really follow the predefined rules?
- Vulnerable to multiple attacks, e.g side-channel attack, cross-site request forgery, man-in-the-middle attack, etc.

5 OBJECTIVES

- Develop an application in Gallina that generates random passwords.
- Investigate how to prove properties about the passwords generated.

6 PROBLEMS

- Generation of pseudo-random numbers depends on an initial seed.
- Acquiring that seed is problematic in a language without side effects.
- Solution:
  - Extract the Gallina code to OCaml.
  - OCaml is used because it simplifies the acquisition of the initial seed.

7 SOLUTION

- Taking as inspiration the QuickChick.
- Guarantees in QuickChick:

```
647   Axiom randomRNatCorrect:
648     forall n n1 n2, n1 <= n2 ->
649       (n1 <= n <= n2 <->
650       exists seed, (fst (randomRNat (n1, n2) seed)) = n).
```

8 SOLUTION

- The program produces a random password with given properties.
- User provides as input:
  - Length of the password;
  - Number of lowercases;
  - Number of uppercases;
  - Number of digits;
  - Number of symbols.

9 SOLUTION

- Generates each part of the password and merges them together.
- Exports code to OCaml file.
- Manipulation of the OCaml code.

SOLUTION

- Coq functions or proofs of specification can be extracted to OCaml, Haskell, and Scheme.
- Code written in Coq and executed in OCaml, Haskell or Scheme.

11 DEMONSTRATION

12 ADDITIONAL WORK

- Prove multiple properties about the Gallina code.
- Improve the password generation algorithm.
- Make fewer modifications in the OCaml code.

13 CONCLUSIONS

- Password managers have many advantages but also some problems.
- It's not easy solving those problems.
- There are multiple challenges when proving properties of password generation algorithms.

14 QUESTIONS?