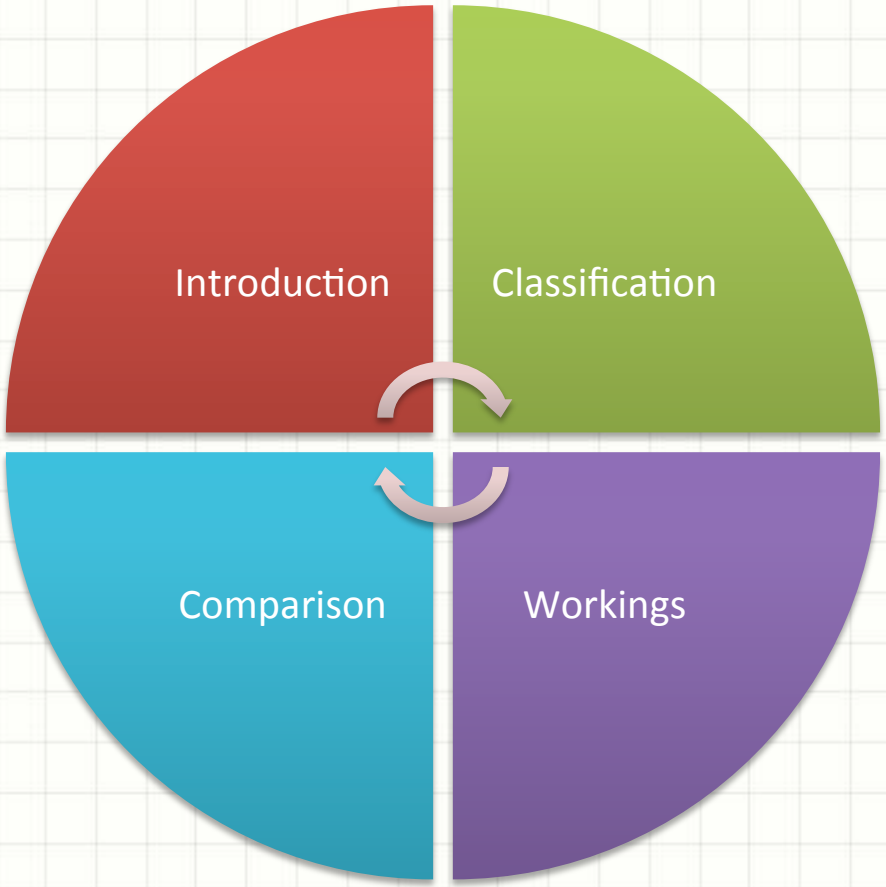
Password Management Techniques

Jay P Patel

Today's Overview



Need for Password Managers

- Increasing web service
  - Gmail, Yahoo, Facebook, Apple, and many more
- Humans generating weaker/common password

Introduction

- Password manager store password securely, provides it back upon the request from user.
- Users of the web application needs to create an account with some personal details where a user id and a password are mandatory inputs provided by user.
- The web application may allow user to upload/ share personal data.
- Security and confidentiality of the data are the top goals for any web service provider.

Introduction

- Users set very weak/common password which helps them to remember easily.
- Ideally all the accounts must have different as well as strong password to prevent attacks from adversary.
- Many password manager also provide strong password generation functionality.
- In this survey, I have discussed 4 different password managers: PassCue, Pass, Versipass, and GeoGP.

Classification

- The main goal of all the previously mentioned tools is to manage password and provide them as and when required.
- All these tools can be classified in two types;
  - Clue based tools: PassCue, Versipass, and GeoGP
  - Encrypt passwords: Pass

Workings

1. PassCue
2. Pass
3. Versipass
4. GeoGP

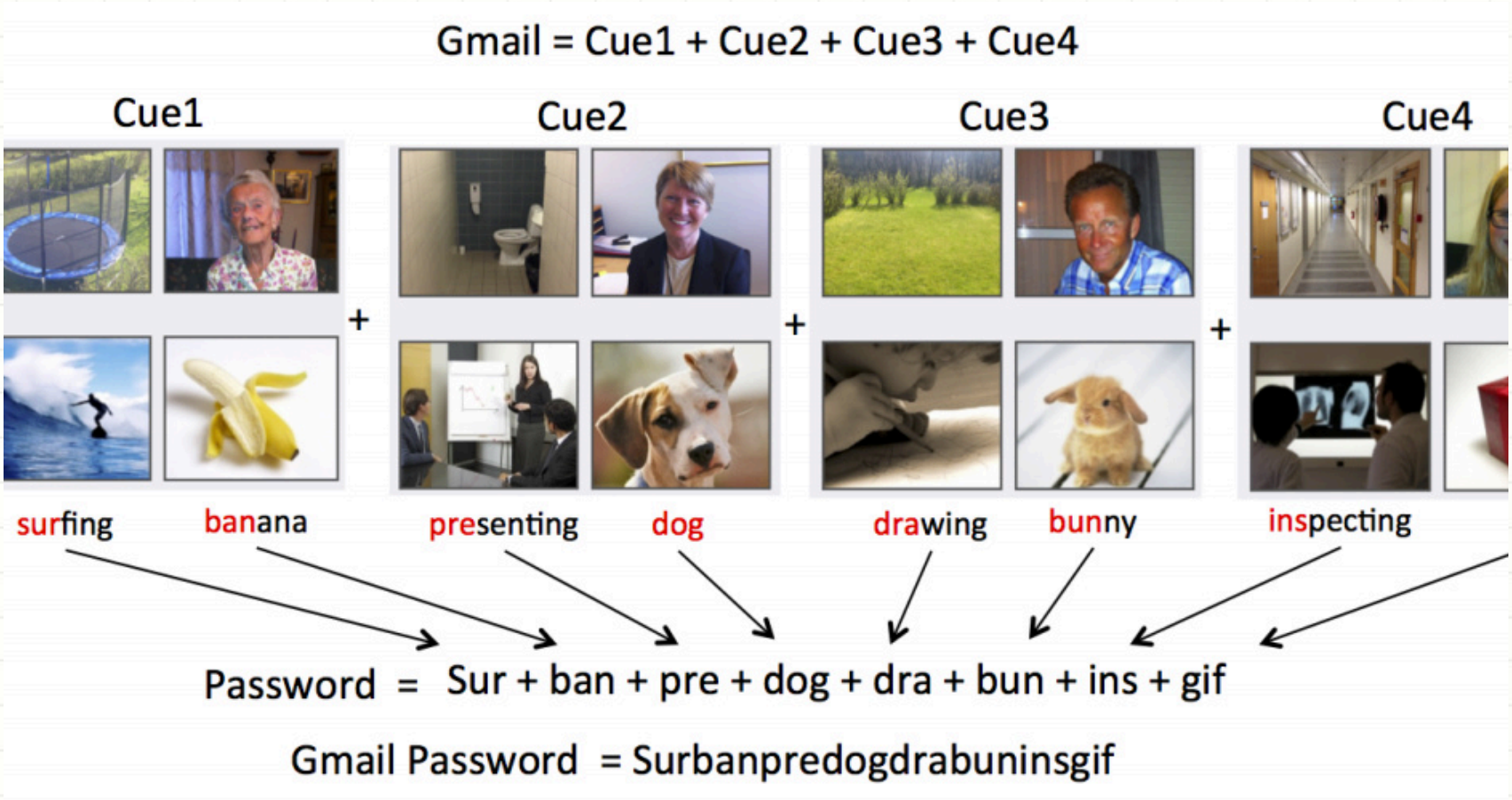
PassCue

- **Shared Cue** use an assumption that the reusability of password on daily basis helps to memorize that password.
- PassCue uses public and private clues (objects) which are graphical entity of real world, provided by user.
- During the password generation phase, PassCue provides both public/private objects.
- User maps relates these objects with each other in such a way that is easy to remember.

PassCue

- PassCue destroys the private clues mapped to respective public clues.
- When the password is requested from PassCue, it shows public clues and request user to enter the detail of respective private clues, which will be used to generate password.

PassCue



Sandvoll, Mats. "Design and Analysis of a Password Management Systems". 2014. Web. 18 September 2015.

Workings

1. PassCue
2. Pass
3. Versipass
4. GeoGP

Pass

- Pass is a command line interface for managing passwords.
- All the passwords are stored through Pass in a ‘gpg’ (GNU Privacy Guard) encrypted file. This makes it easy to transfer from computers.
- Pass provides the functionality to generate and manage store passwords.
- Files are organized into various hierarchy, and file names are the name of the service whose password is stored inside that file.

Pass

- Pass is available to many Linux flavor:
  - Macintosh
  - Debain
  - Ubuntu
  - Fedora
  - RHEL
  - Gentoo
  - Arch
  - FreeBSD

Workings

1. PassCue
2. Pass
3. Versipass
4. GeoGP

Versipass

- Versipass uses Image PassTile scheme, where an image is divided into small identical tiles (2-dimensional grid).
- User is assigned *n* randomly selected tiles during the password generation phase.
- When user request the password, (s)he should click the same tiles in any order to generate the login password.
- Versipass remembers the graphical contents used for password generation instead of password itself.

Versipass

- The default value of *n* is 5 and grid size of dimension 6 x 8.
- These values can be increased for the sake of more security.

Workings

1. PassCue
2. Pass
3. Versipass
4. GeoGP

GeoGP

- GeoGraphical passwords uses the assumption that humans have good memory for graphical contents than the textual contents.
- Geographical location means “knowledge acquired through processing geographically referenced data” [1].
- User marks any number of known place, which can be utilized to generate password.
- Application has divided the earth into small rectangles, also taking altitude in account when generating passwords.

GeoGP

- User cannot select same rectangle more than once, means no repeating input allowed in password generation.
- GeoGP also takes in account the order of rectangle selection which adds more security.
- The values generated from the selected rectangles are **keyed-HMAC**.

Comparison

	Versipass	Pass	PassCue	GeoGP
Security (bits)	>21	-	>61	38 - 371
Supported platform	-	Linux (flavor)	iOS	-

Bibliography

[1] Al-Salloum, Ziyad. “GeoGraphical Passwords”. 2014. Web. 29 September 2015.

QUESTIONS?