Security and Usability of Graphical Passwords

Kyle J. Hakala

UMN Morris

2017 April 15

University of Minnesota
Driven to Discover℠

Introduction

Think for a moment...

How many different systems and services do you need to log into every day?

Introduction

Think for a moment...

How many different systems and services do you need to log into every ~~day?~~
week?

Introduction

Think for a moment...

How many different systems and services do you need to log into every ~~day?~~

~~week?~~

month?

Introduction

Think for a moment...

How many different systems and services do you need to log into every ~~day?~~

~~week?~~

~~month?~~

year?

Introduction

...A lot.

Introduction

neopets®

...A lot.

Introduction

...A lot.

Introduction

FAFSA

FederalStudentAid

An office of the U.S. Department of Education

neopets®

...A lot.

Google

Introduction

FAFSA

FederalStudentAid

An office of the U.S. Department of Education

neopets®

MyU

...A lot.

Google

Introduction

FAFSA

FederalStudentAid

An office of the U.S. Department of Education

neopets®

MyU

...A lot.

usbank®

Google

Introduction

FAFSA

FederalStudentAid

An office of the U.S. Department of Education

neopets®

MyU

...A lot.

usbank®

Google

FIRSTLAYER

HEALTH

Introduction

FAFSA
FederalStudentAid
An office of the U.S. Department of Education

neopets®

MyU

...A lot.

usbank®

wine.com®

Google

FIRSTLAYER
HEALTH

Introduction

FAFSA

FederalStudentAid

An office of the U.S. Department of Education

neopets®

MyU

...A lot.

usbank®

wine.com®

IRS

Google

FIRSTLAYER
HEALTH

Introduction

FAFSA

FederalStudentAid

An office of the U.S. Department of Education

neopets®

MyU

...A lot.

usbank®

wine.com®

IRS

Google

FIRSTLAYER HEALTH

Introduction

FAFSA

FederalStudentAid

An office of the U.S. Department of Education

neopets®

MyU

...A lot.

AOL®

usbank®

wine.com®

IRS

Google

FIRSTLAYER

HEALTH

Introduction

FAFSA
FederalStudentAid
An office of the U.S. Department of Education

neopets®

MyU

...A lot.

AOL®™

usbank®

wine.com®

IRS

Google

FIRSTLAYER
HEALTH

United
Airlines

Introduction

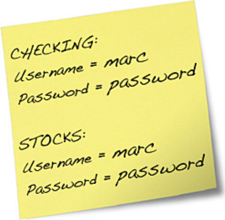
Do you have fewer unique passwords than services?

CHECKING:
Username = marc
Password = password
STOCKS:
Username = marc
Password = password

Introduction

Do you have fewer unique passwords than services?

This may look familiar:



CHECKING:
Username = marc
Password = password

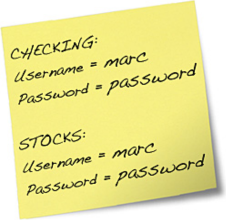
STOCKS:
Username = marc
Password = password

Introduction

Do you have fewer unique passwords than services?

This may look familiar:

- `fluffy2!`



CHECKING:
Username = marc
Password = password

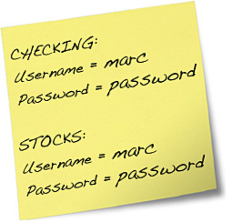
STOCKS:
Username = marc
Password = password

Introduction

Do you have fewer unique passwords than services?

This may look familiar:

- `fluffy2!`
- `fluffy2!!`



CHECKING:
Username = marc
Password = password

STOCKS:
Username = marc
Password = password

Introduction

Do you have fewer unique passwords than services?

This may look familiar:

- `fluffy2!`
- `fluffy2!!`
- `fluffy2!!!`

CHECKING:
Username = marc
Password = password

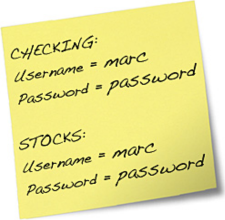
STOCKS:
Username = marc
Password = password

Introduction

Do you have fewer unique passwords than services?

This may look familiar:

- `fluffy2!`
- `fluffy2!!`
- `fluffy2!!!`
- `fluffy2!!!!`



CHECKING:
Username = marc
Password = password

STOCKS:
Username = marc
Password = password

Introduction

You aren't alone!

Introduction

You aren't alone!

We want a means of authenticating that is:

Introduction

You aren't alone!

We want a means of authenticating that is:

- secure

Introduction

You aren't alone!

We want a means of authenticating that is:

- secure
- memorable

Introduction

You aren't alone!

We want a means of authenticating that is:

- secure
- memorable
- practical

Introduction

How about graphical passwords?

Introduction

What are graphical passwords?

Introduction

What are graphical passwords?

Graphical passwords are an alternative method of authentication to traditional text-based passwords.

Introduction

What are graphical passwords?

Graphical passwords are an alternative method of authentication to traditional text-based passwords.

They...

Introduction

What are graphical passwords?

Graphical passwords are an alternative method of authentication to traditional text-based passwords.

They...

- ...provide a more memorable approach to authentication

Introduction

What are graphical passwords?

Graphical passwords are an alternative method of authentication to traditional text-based passwords.

They...

- ...provide a more memorable approach to authentication
- ...can be used as a component of two-factor auth systems

Introduction

What are graphical passwords?

Graphical passwords are an alternative method of authentication to traditional text-based passwords.

They...

- ...provide a more memorable approach to authentication
- ...can be used as a component of two-factor auth systems
- ...can be implemented in many varying styles

Introduction

Popular Implementations

- Windows 8 and 10; users draw shapes over an image

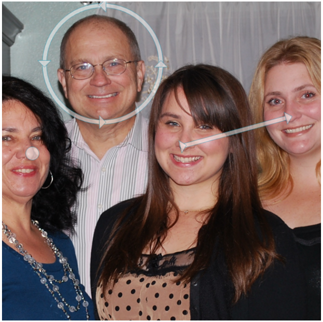


Figure 1: Windows Picture Password

Introduction

Popular Implementations

- Windows 8 and 10; users draw shapes over an image
- Android phones; users draw a pattern by connecting a series of points.

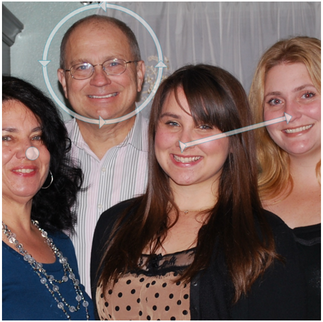


Figure 2: Windows Picture Password

Introduction

Popular Implementations

- Windows 8 and 10; users draw shapes over an image
- Android phones; users draw a pattern by connecting a series of points.

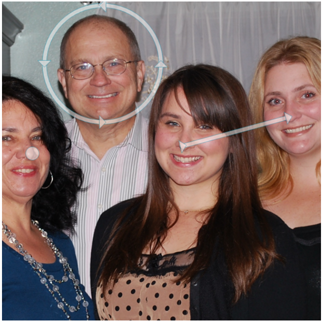


Figure 2: Windows Picture Password

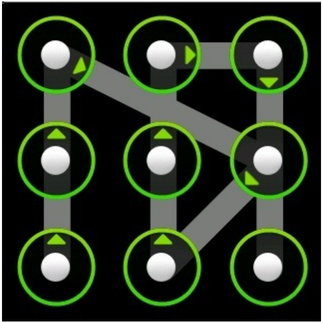


Figure 3: Android Pattern-Lock

Outline

1. Background
   - Components
2. Analysis
   - Security
   - Usability
3. Conclusion

Components

A graphical password consists of two main components:

Components

A graphical password consists of two main components:

- interaction from a user

Components

A graphical password consists of two main components:

- interaction from a user
    - a point, series of points, or set of points

Components

A graphical password consists of two main components:

- interaction from a user
  - a point, series of points, or set of points
  - a shape, series of shapes, or set of shapes

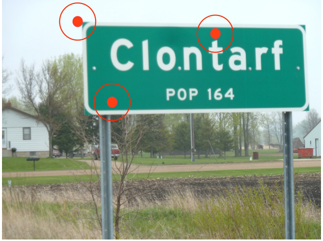


Figure 4: Set of points, selected in any order

Components

A graphical password consists of two main components:

- interaction from a user
  - a point, series of points, or set of points
  - a shape, series of shapes, or set of shapes

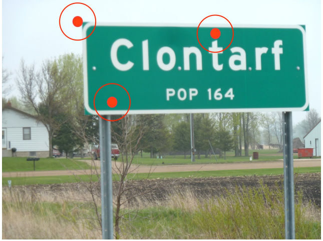


Figure 4: Set of points, selected in any order

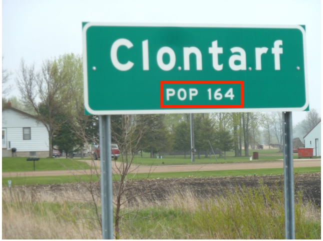


Figure 5: Single shape drawn over image

Components

- an image upon which a user interacts

Components

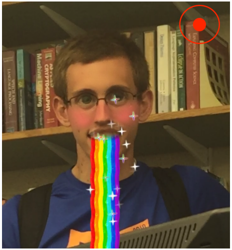
- an image upon which a user interacts
    - can be either user-provided, or system-provided

Components

- an image upon which a user interacts
    - can be either user-provided, or system-provided
    - a single image, series of images, or set of images

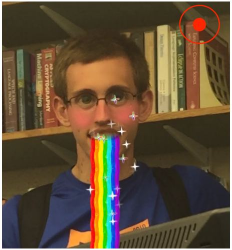
Components

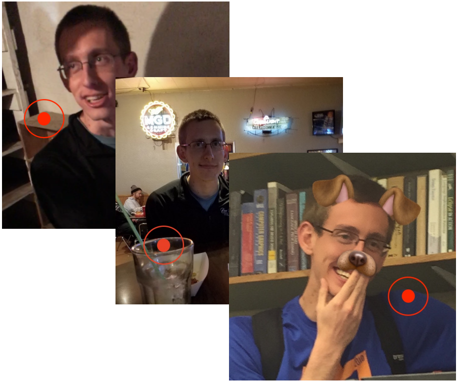
- an image upon which a user interacts
  - can be either user-provided, or system-provided
  - a single image, series of images, or set of images



Components

- an image upon which a user interacts
  - can be either user-provided, or system-provided
  - a single image, series of images, or set of images





Security

Shoulder Surfing

the practice of spying on the user of an ATM, computer, or other electronic device in order to obtain their personal access information

Security

Shoulder Surfing

the practice of spying on the user of an ATM, computer, or other electronic device in order to obtain their personal access information

- GPs are more visual than text

Security

Shoulder Surfing

the practice of spying on the user of an ATM, computer, or other electronic device in order to obtain their personal access information

- GPs are more visual than text
- They are not obscured like text

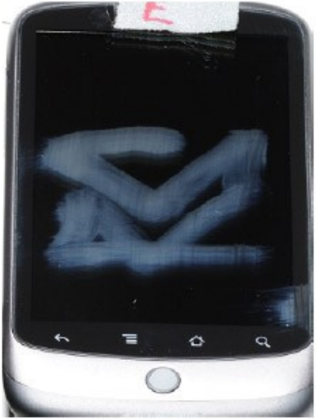
Security

Shoulder Surfing

the practice of spying on the user of an ATM, computer, or other electronic device in order to obtain their personal access information

- GPs are more visual than text
- They are not obscured like text
- Must be large enough for interaction

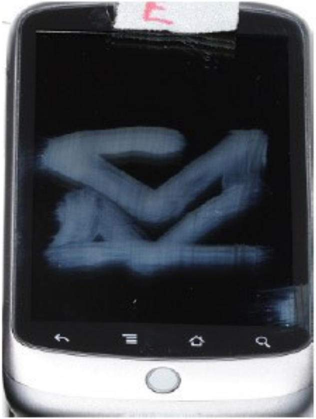
Security



Smudging

residual marks left behind in the shape of a graphical password indicating what was entered

Security

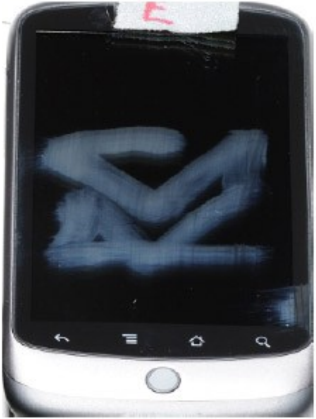


Smudging

residual marks left behind in the shape of a graphical password indicating what was entered

- Prominence depends upon length of usage session

Security

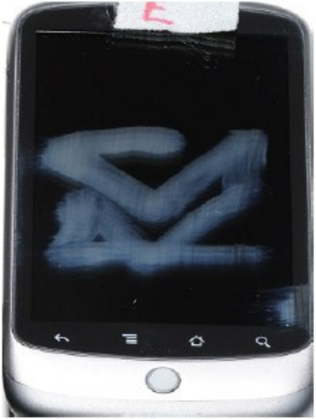


Smudging

residual marks left behind in the shape of a graphical password indicating what was entered

- Prominence depends upon length of usage session
- Can indicate direction and location

Security



Smudging

residual marks left behind in the shape of a graphical password indicating what was entered

- Prominence depends upon length of usage session
- Can indicate direction and location
- Varies between devices

Security

Hotspots

a hotspot is a feature of an image that a user is more likely to base a GP component on

Security

Hotspots

a hotspot is a feature of an image that a user is more likely to base a GP component on

- Cued Click Points (CCP)
    - User is presented 5 images in series
    - One point is chosen per image with no guidance

Security

Hotspots

a hotspot is a feature of an image that a user is more likely to base a GP component on

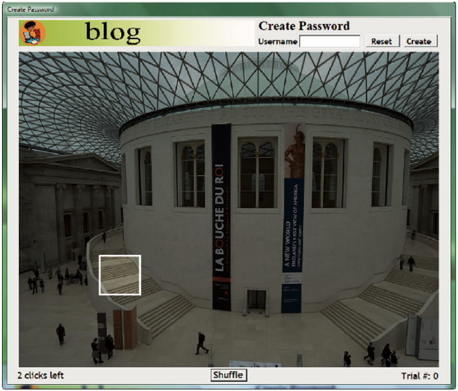
- Cued Click Points (CCP)
  - User is presented 5 images in series
  - One point is chosen per image with no guidance
- Persuasive CCP (PCCP)
  - User is provided 5 images in succession
  - One point is chosen per image from within viewport
  - Viewport is randomly placed, but can be shuffled

Security

Hotspots

a hotspot is a feature of an image that a user is more likely to base a GP component on

- Cued Click Points (CCP)
  - User is presented 5 images in series
  - One point is chosen per image with no guidance
- Persuasive CCP (PCCP)
  - User is provided 5 images in succession
  - One point is chosen per image from within viewport
  - Viewport is randomly placed, but can be shuffled



Security

Let’s use brute force!

Security

Let's use brute force!

S. Widenbeck et al. note in research on PassPoints:

Security

Let's use brute force!

S. Widenbeck et al. note in research on PassPoints:

- it is easy to obtain larger password spaces with GPs

Security

Let's use brute force!

S. Widenbeck et al. note in research on PassPoints:

- it is easy to obtain larger password spaces with GPs
- even considering "cool spots," GP system key-spaces can compete

Security

Let's use brute force!

S. Widenbeck et al. note in research on PassPoints:

- it is easy to obtain larger password spaces with GPs
- even considering "cool spots," GP system key-spaces can compete

	Image size	**Alphabet size***	**Length**	**Key-space**
Alphanum.	N/A	64	8	$2.8\text{x}10^{14}$
Alphanum.	N/A	72	8	$7.2\text{x}10^{14}$

Security

Let’s use brute force!

S. Widenbeck et al. note in research on PassPoints:

- it is easy to obtain larger password spaces with GPs
- even considering “cool spots,” GP system key-spaces can compete

	Image size	**Alphabet size***	**Length**	**Key-space**
Alphanum.	N/A	64	8	$2.8\text{x}10^{14}$
Alphanum.	N/A	72	8	$7.2\text{x}10^{14}$
Graphical	1024x752	3928	5	$9.3\text{x}10^{17}$
Graphical†	1024x752	1964	5	$2.9\text{x}10^{16}$

* *Alphabet size* for the GP is determined by taking the area of the image (in px) and dividing by the area of (in px) tolerance square; for a text based password, it is the set of all characters permitted.

† GP where half of screen is considered usable space

Usability

Memorability

Usability

Memorability

- Easier to recall

Usability

Memorability

- Easier to recall
- Great for children

Usability

Memorability

- Easier to recall
- Great for children
- Difficult to recall when many GPs exist

Usability

Tolerance for Error

Usability

Tolerance for Error

- Can become unusable if too strict

Usability

Tolerance for Error

- Can become unusable if too strict
- Decreases security when too forgiving

Usability

Tolerance for Error

- Can become unusable if too strict
- Decreases security when too forgiving

Tolerance	Image size	Alphabet size*	Key-space
14x14	1024x752	3928	9.3x10^{17}
20x20	1024x752	1925	2.6x10^{16}
26x26	1024x752	1139	1.9x10^{15}

**Alphabet size* is *Image Size* ÷ *Tolerance size*

** Assumes 5 click points are chosen

Usability Overview

But... it's not text...

S. Widenbeck et al. note in their research that PassPoints users:

Usability Overview

But... it's not text...

S. Widenbeck et al. note in their research that PassPoints users:

- easily created a password

Usability Overview

But... it's not text...

S. Widenbeck et al. note in their research that PassPoints users:

- easily created a password
- reasonably recall and input their GPs even after weeks without use

Conclusion

Graphical passwords present a welcome alternative to text based authentication.

Pros of GPs

- Larger password-size space
- More memorable

Cons of GPs

- More susceptible to softer attacks
- No standard form

Acknowledgments

Thank you to KK, Elena, and Justin Mullin (alumni reviewer) for all of the great feedback!

Questions?