Usable Privacy and Security, Fall 2011
Nov. 10, 2011

Graphical Passwords (2)

YoungSeok Yoon
(youngseok@cs.cmu.edu)
Institute for Software Research
School of Computer Science
Carnegie Mellon University

Categories

- picture/photo based vs. grid based
- recognition based vs. recall based

Usability concerns

- Usability
  - Are the passwords easy to memorize?
  - Is the authentication process simple?
  - Is it easy to input the password?
  - How long does it take to input the password?

Security concerns

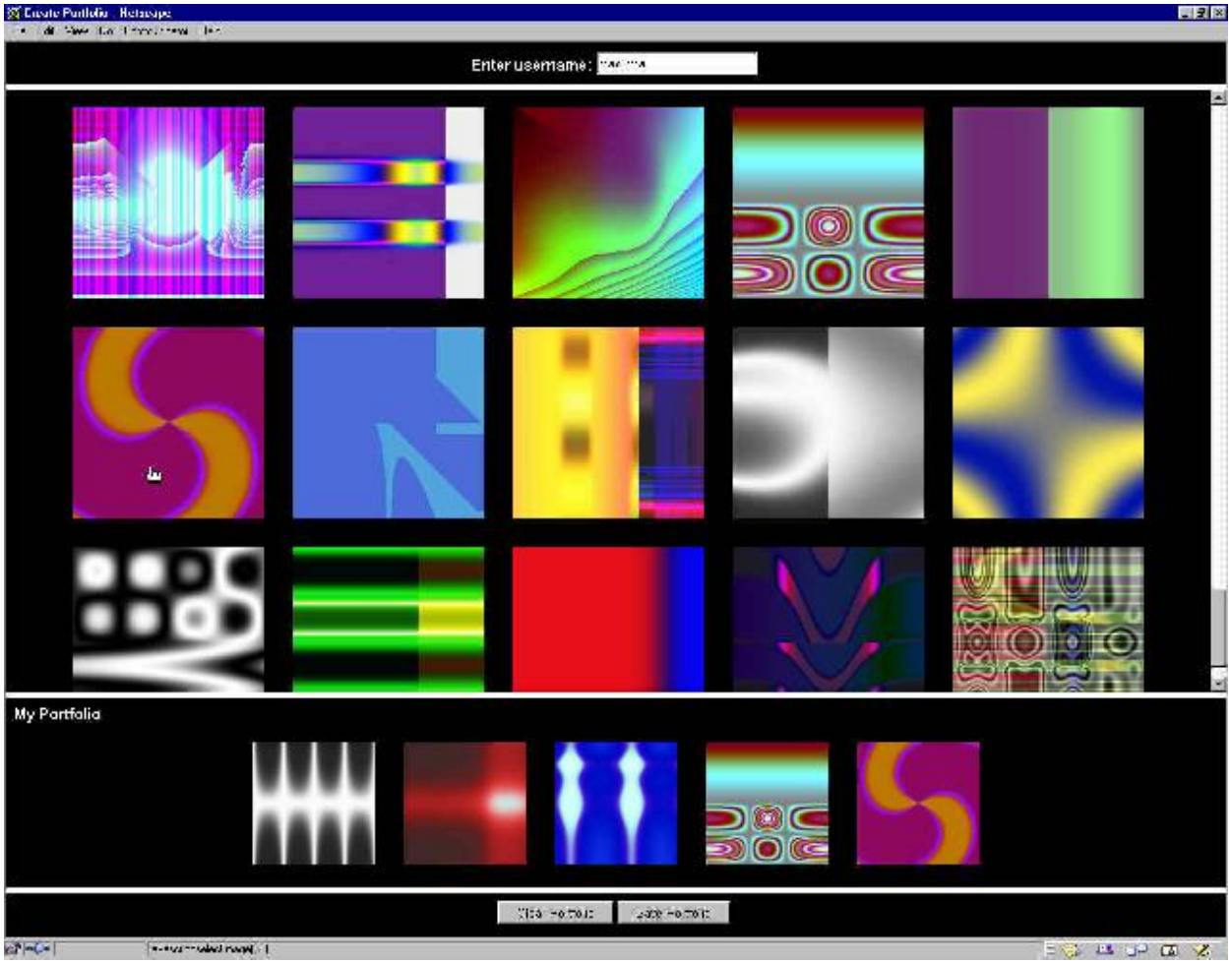
- Security
  - Is the password scheme resistant to various attacks?
    - Brute force
    - Educated guess
      - Collective educated guess
      - Individualized educated guess
    - Shoulder surfing
    - Spyware
    - Social engineering

Educated Guess Resistant Graphical Password Schemes

Déjà Vu [Dhamija+00]

- Picture based / recognition based
  - Use random images generated by Andrej Bauer's *Random Art*
- Three phases:
  - portfolio creation
  - training
  - authentication

Déjà Vu – Sample Screenshot



Déjà Vu – Usability

- Memorability
  - Their user study suggests the portfolios are much easier to remember than the textual passwords
  - However, the study is limited (only 20 participants)
  - Quantitative result

	PIN	Password	Art	Photo
Failed Logins	5% (1)	5% (1)	0	0
Failed Logins (after one week)	35% (7)	30% (6)	10% (2)	5% (1)

Table 2: % Failed logins (# failed logins/20 participants)

  - Qualitative result

> Although some users remarked that they would never be able to remember the portfolios they created, all were surprised that they could recognize their images and at how quickly the selection took place.

Déjà Vu – Usability

- Random Art vs. Photo?
  - Resistance to educated guess attack vs. memorability
- Authentication process
  - It takes a significant time for portfolio creation + training
  - Takes more time to input the password compared to the textual passwords

	PIN	Password	Art	Photo
Create	15	25	45	60
Login	15	18	32	27
Login (after one week)	27	24	36	31

Table 1: Average seconds to create/login

Déjà Vu – Security

- Password space

  $\binom{n}{k}$, where n is the # of images in the challenge set and k is the # of portfolio images shown.

  - e.g. if n = 20 and k = 5, the space size = 15504 (slightly bigger than that of 4-digit PIN)

- The image generating seed value should be stored in the authentication server unencrypted

- Resistant to educated guess attacks

- May be vulnerable to
  - brute force
  - shoulder surfing

Use your illusion

- Below are three distorted images
  Can you guess what the original photos represent?

Use your illusion

Lorrie Cranor

Hunt Library

River & Bridge
(my wallpaper)

Use your illusion [Hayashi+08, 11]

- https://arima.okoze.net/illusion/
- Photo based / recognition based
  - A user has to upload 3 of his/her own images and memorize the *distorted images* of those as the portfolio

Use your illusion – Usability

- Memorability
  - Easier to remember because the user chooses her own images

	The 1st day	2 days later	1 wk. later	4 wks. later
Self-selected, non-distorted	100%(18)	100%(18)	100%(18)	100%(18)
Self-selected, distorted	100%(18)	100%(18)	100%(18)	100%(18)
Imposed, distorted	100%(18)	89%(16)	94%(17)	89%(16)

- Login Time

	1st day	2 days later	1 wk. later	4 wks. later
Self-selected, non-distorted	11.5 (9.9)	12.3 (12.3)	12.7 (11.9)	12.5 (12.8)
Self-selected, distorted	12.4 (11.2)	16.4 (15.9)	14.3 (13.4)	17.9 (16.5)
Imposed, distorted	16.7 (14.1)	25.8 (19.0)	25.1 (17.6)	24.7 (16.7)

Use your illusion – Security

- Password space
  - The same formula as that of Déjà Vu scheme
  - if $n = 27$ and $k = 3$, the space size = 2925
- Resilient to educated guess attacks
- May be vulnerable to
  - brute force attacks
  - shoulder surfing

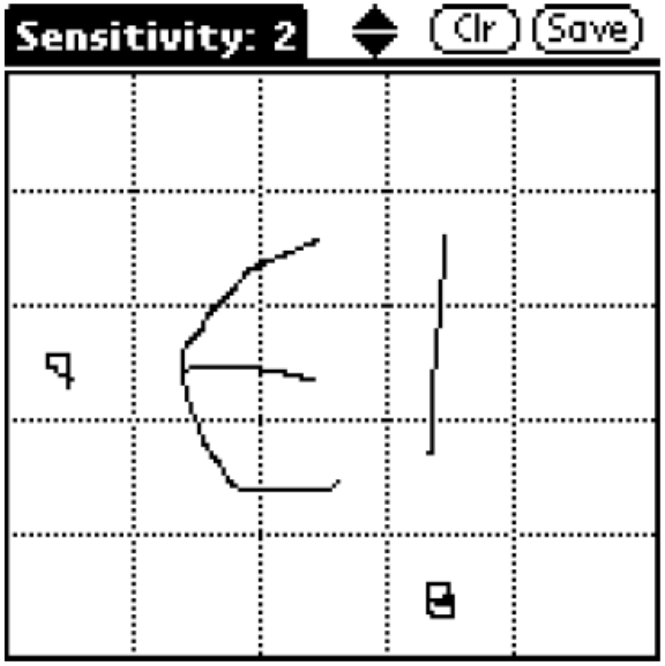
Brute Force Search Resistance Graphical Password Schemes

Password space size revisited

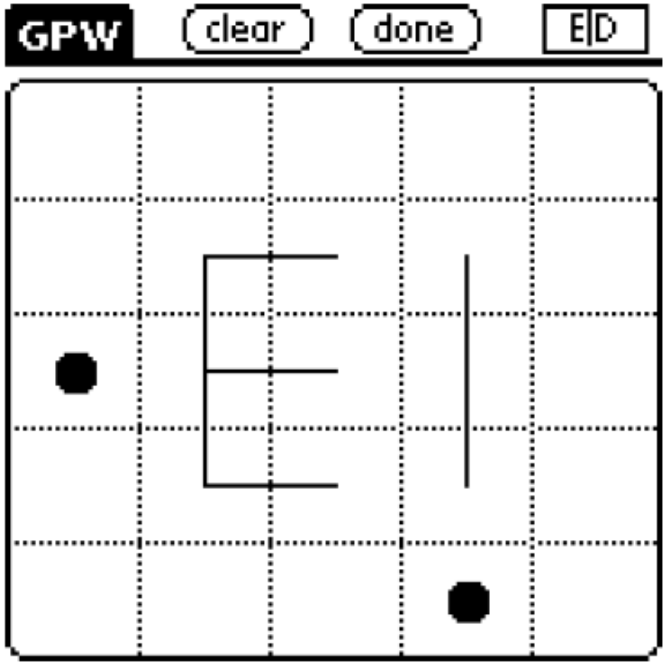
- Previous two schemes have relatively small password space under their default settings
  - Déjà Vu: 15504 (where $n = 20$, $k = 5$)
  - Use your illusion: 2925 (where $n = 27$, $k = 3$)
- We can tune the variables n and k to enlarge the password space
- Then how about the usability??
  - It would be more tedious to look at so many pictures if the # of all images shown in a challenge set (n) gets bigger
  - Trade-off between password space and usability

Draw-A-Secret (DAS) [Jermyn+99]

- Grid based / recall based scheme



(a) User inputs desired secret



(b) Internal representation

DAS – Usability

- Memorability
  - Not all the available passwords are memorable
    but there are some categories of passwords that are relatively memorable
    - Simple shapes, letters, …
    - Patterns that can be generated by short algorithms
    - Symmetric patterns
- Easy to input?
  - Suitable for the touch devices
    (e.g. PDAs, smartphones)
  - Somewhat difficult with mouse
- Not enough user studies about the usability

DAS – Security

- Large enough password space with 5x5 grid

$L_{\max}$	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
$\log_2$(# passwords)	5	10	14	19	24	29	33	38	43	48
$L_{\max}$	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*
$\log_2$(# passwords)	53	58	63	67	72	77	82	87	91	96

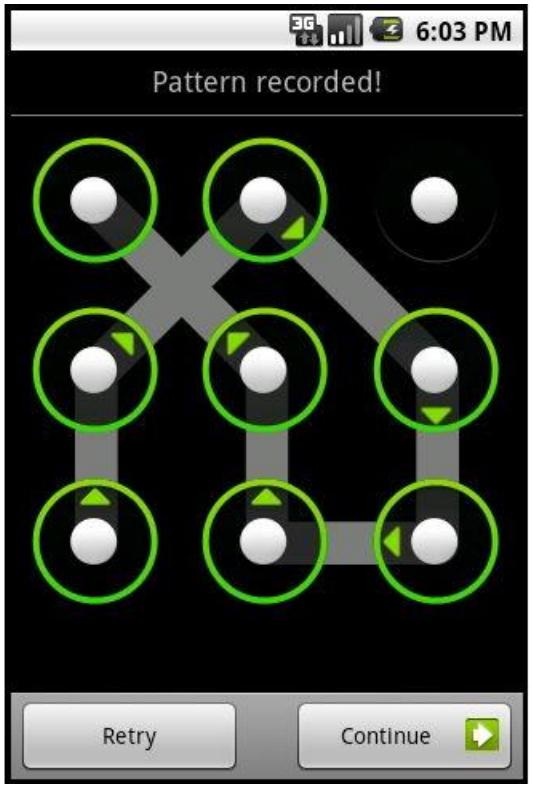
Table 1: Number of passwords of total length less than or equal to $L_{\max}$ on a 5×5 grid.

  - When Lmax > 11, the space size surpasses that of textual password with 8 characters ($95^8 \doteqdot 2^{53}$)

- This is true in theory, but how about in reality?
  - People tent to choose memorable patterns (e.g. symmetric patterns)
  - Vulnerable to collective educated guess attacks (just like dictionary attacks of textual passwords)

A DAS Variant in real life

- Android phone unlock patterns



Android unlock patterns

- Usability
  - Any ideas? Want to hear from the actual users.
- Security
  - Password space
  - How about the smudges on the touch screen?

N	# of PINs	# of patterns (unrestricted)	# of patterns (restricted)
2	100	56	56
3	1,000	360	304
4	10,000	2,280	1,400
5	100,000	14,544	5,328
6	1,000,000	92,448	16,032
7	10,000,000	588,672	35,328
8	100,000,000	3,745,152	49,536

Numbers obtained from http://playingwithmodels.wordpress.com/2010/04/14/android_unlock_patterns/

Is a small password space *always* bad?

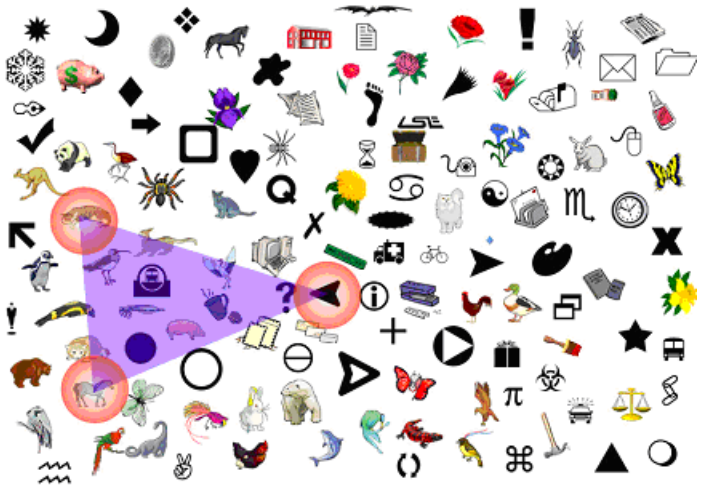
- Any ideas?

- All of the previously mentioned graphical password schemes are *vulnerable* to…?

Shoulder Surfing Resistant Graphical Password Schemes

Convex Hull Scheme [Sobrado+02]

- Picture based / recognition based scheme
  - A user selects *k* pass-objects (portfolio)
  - Then the user has to click somewhere inside the convex hull of the pas s objects
  - To prevent from random guessing, the user is required to do repeat thi s challenge a few times (e.g. 10 times)



Convex Hull Scheme – Usability

- No formal user study for this scheme
- Memorability
  - Would be similar to that of Déjà Vu
- Authentication process
  - To make this scheme effective, the value *n* should be big enough → difficult to find the pass-objects
  - Unlike the Déjà Vu / Use your illusion schemes, the user is required to find all the *k* pass-objects together to see the invisible convex hull, which might affect the usability

Convex Hull Scheme – Security

- Password space

> "The number of possible passwords is the "binomial coefficient" (choose any *K* objects among N). **When *N* = 1000 and *K* = 10**, the number of possible passwords is hence approximately $2.6 * 10^{23}$. This is a little more than the number of alpha-numeric passwords of length 15 ($36^{15} \fallingdotseq 2.2 * 10^{23}$). Having *N* = 1000 objects is not unreasonable (compare with the "Where is Waldo" puzzles, where there are typically tens of thousands of little persons in a picture)."

  - Maybe true, but no evidence

- Resistant to shoulder surfing attack

Summary – Characteristics of Graphical Passwords

Usability of graphical passwords

- More memorable than textual passwords
- Takes significantly longer time to create the graphical passwords
- Takes longer time to input the passwords
- More restrictions
  - big enough screen size is often required
  - some schemes require extra devices (e.g. touch screen)

Memorability

- Why is it so important to make more *memorable* password schemes?
  - One of the most important problems of textual passwords
- Are the graphical passwords *really* significantly more memorable?
  - We do not know yet
  - We need to conduct larger scale field studies

Memorability

- What if a user has many graphical passwords? Would it be still easy enough to correctly remember *all* of them?
  - Chiasson et al. suggest that it may not be the case

Table 10: Effect of interference on success rate[1] (field)

		No Interference	Interference	χ^2
Confirm	Pool	139/284 (49%)	63/99 (64%)	χ^2 (1, N=383)=6.36, p<.05
	Cars	108/193 (56%)	62/100 (62%)	n.s.
Login	Pool	1224/1541 (79%)	226/319 (71%)	χ^2 (1, N=1860)=11.33, p<.001
	Cars	1053/1216 (87%)	248/347 (71%)	χ^2 (1, N=1563)=44.26, p<.001

Security of graphical passwords

- Security and usability trade-off
- Resistant to…
  - Dictionary attacks
  - Social engineering (e.g. phishing)

- Vulnerable to…
  - Brute force attacks
  - Educated guess attacks
  - Shoulder surfing

- How about the spywares?

Authentication server's concerns

- Usually needs more space than the textual passwords
- The passwords cannot be easily hashed

How should we embrace the graphical passwords?

- Quick poll
  - How many of you would like to try out some of th e graphical passwords?
  - How many of you would like to use the graphical p asswords as your main password scheme?
- How should we embrace them?

Conclusion

Conclusion

- Graphical passwords and textual passwords have different characteristics
- Graphical passwords good for authentication, but not as much good for key generation in general
- There exist various graphical password schemes, each with its own strengths and weaknesses
- More user studies with focus on "usability" are needed
  - memorability is not the only usability concern

References

- [Dhamija+00] Dhamija, R. and Perrig, A. 2000. Deja vu: A user study using images for authentication. In *Proceedings of the 9th USENIX Security Symposium (SSYM'2 000). 4-4.*
- [Hayashi+08] Hayashi, E., Dhamija, R., Christin, N. and Perrig, A. 2008. Use Your Il lusion: secure authentication usable anywhere. In *Proceedings of the 4th Symposi um On Usable Privacy and Security (SOUPS'2008). 35-45.*
- [Hayashi+11] Hayashi, E., Hong, J. and Christin, N. 2011. Security through a differ ent kind of obscurity: evaluating distortion in graphical authentication schemes. I n *Proceedings of the 2011 annual conference on Human factors in computing syste ms (CHI'2011). 2055-2064.*
- [Jermyn+99] Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K. and Rubin, A. D. 199 9. The design and analysis of graphical passwords. In *Proceedings of the 8th USEN IX Security Symposium (SSYM'1999). 1-1.*
- [Sobrado+02] Sobrado, L. and Birget, J. C. 2002. Graphical passwords. *The Rutger s Scholar, an electronic Bulletin for undergraduate research, 4, 21.*
- [Chiasson+07] Chiasson, S., Biddle, R. and Oorschot, P. C. v. 2007. A second look a t the usability of click-based graphical passwords. In *Proceedings of the 3rd Sympo sium On Usable Privacy and Security (SOUPS'2007). 1-12.*

Questions?

Related topic

- Social CAPCHA of Facebook