RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

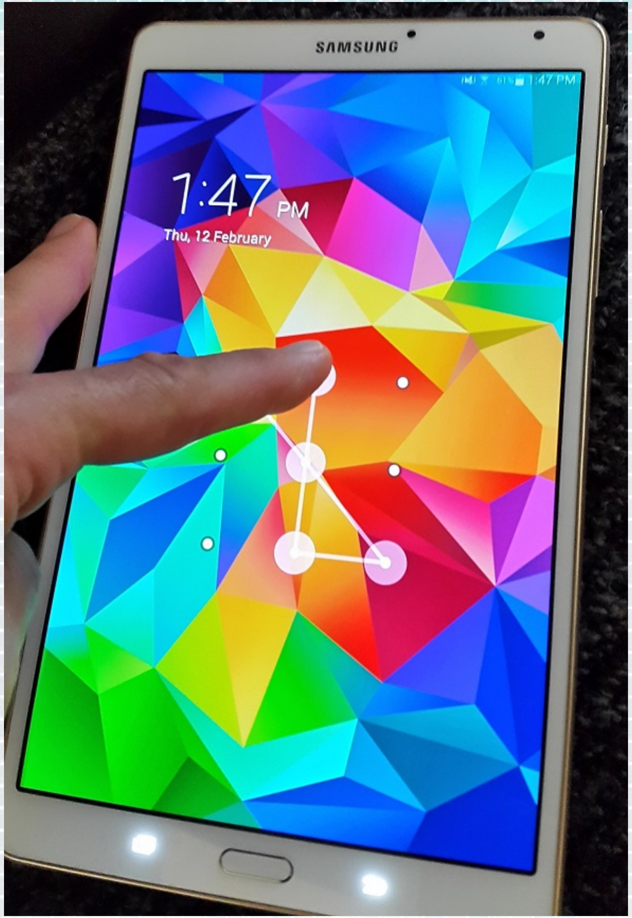
SESSION ID: IDY-F02

Secure Graphical Passwords

Peter Robinson

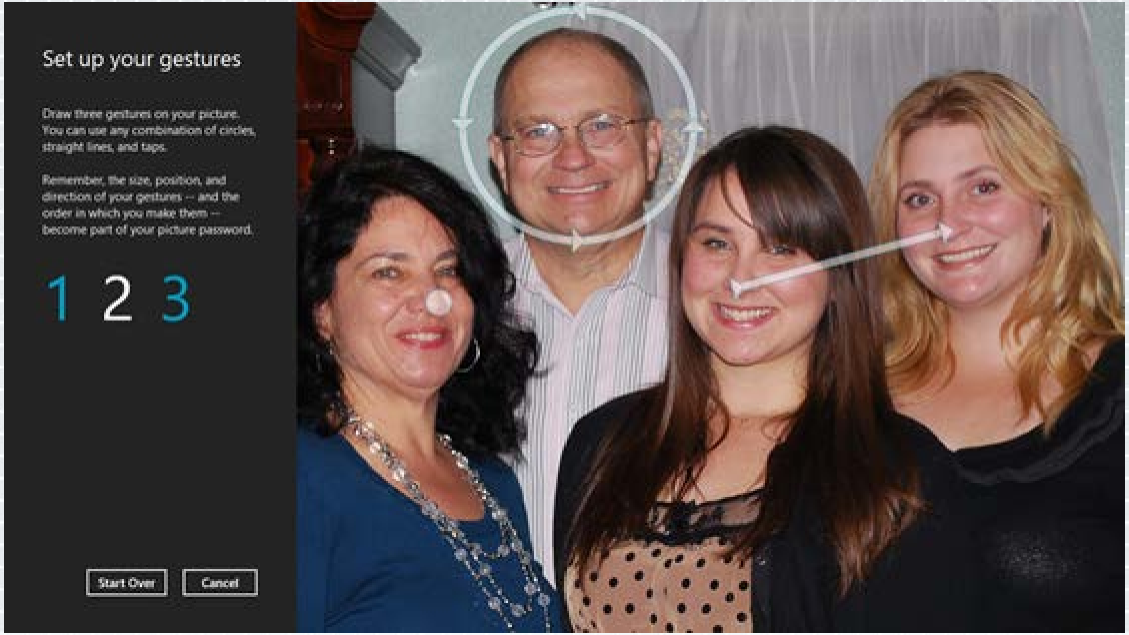
Senior Engineering Manager
RSA, The Security Division of EMC

Is this Secure?



Google^{TM} Android^{TM} Pattern Unlock

What about this?



Set up your gestures

Draw three gestures on your picture. You can use any combination of circles, straight lines, and taps.

Remember, the size, position, and direction of your gestures -- and the order in which you make them -- become part of your picture password.

Microsoft® Windows 8 ® Picture Password

Introduction

This presentation:

- Analyses the security strength of Android Pattern Unlock and Windows 8 Picture Password.
- Introduces a new graphical password scheme which offers:
  - Better security strength, whilst still being memorable, and fast to enter.
  - Allows for automatic password simplification, which makes passwords easier to remember.

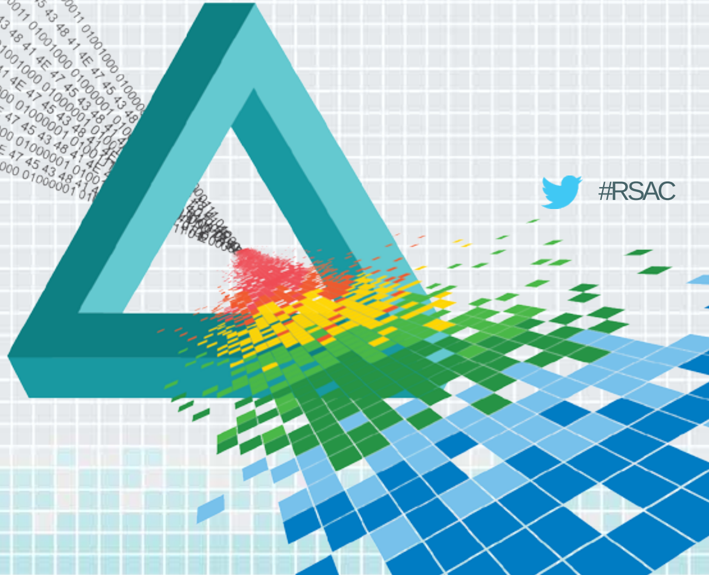
Agenda

- Password Entropy and Security Strength
- Android Pattern Unlock
- Windows 8 Picture Password
- Peter’s Graphical Password Scheme
- Other Considerations

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Password Entropy and Security Strength



#RSAC

Password Entropy and Security Strength

- Entropy:
  - The amount of uncertainty or unpredictable randomness.

  Example:
  - Sample the pixel colour value from a light sensor pointed at a busy street.
  - The light sensor could return 256 possible values.
  - Entropy = 8 bits = $\log_2(256)$
  - Assumes:
    - Attackers can’t see the street scene & don’t know when the sample is taken.
    - The possible light values are evenly distributed.

Password Entropy and Security Strength

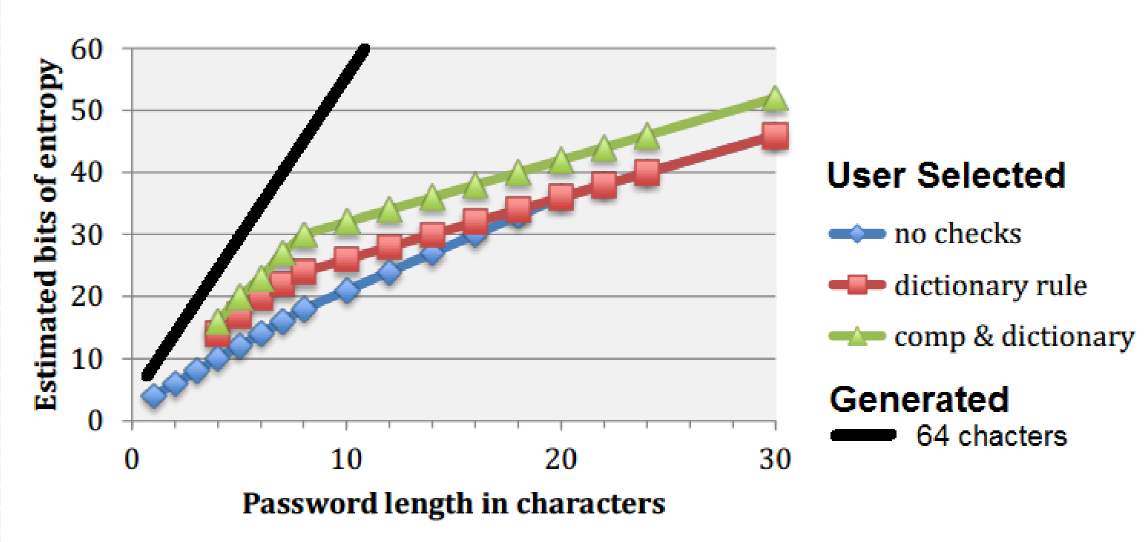
- Password Entropy:
  - The amount of entropy which can be derived from a password.

Example:

- Randomly selected 8 character password with 64 possible values per character.
- The Password Entropy is 48 bits = $\log_2(64) \times 8$
- Can anyone remember: cFz8^Mcq ?

Password Entropy and Security Strength

- NIST SP-800-63[1] has a methodology for estimating the entropy of user selected passwords.
- Wier et al.[2] have introduced the concept of Guessing Entropy, which is based on how hard a password is to crack.



Note 1: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

Note 2: http://dl.acm.org/citation.cfm?id=1866327

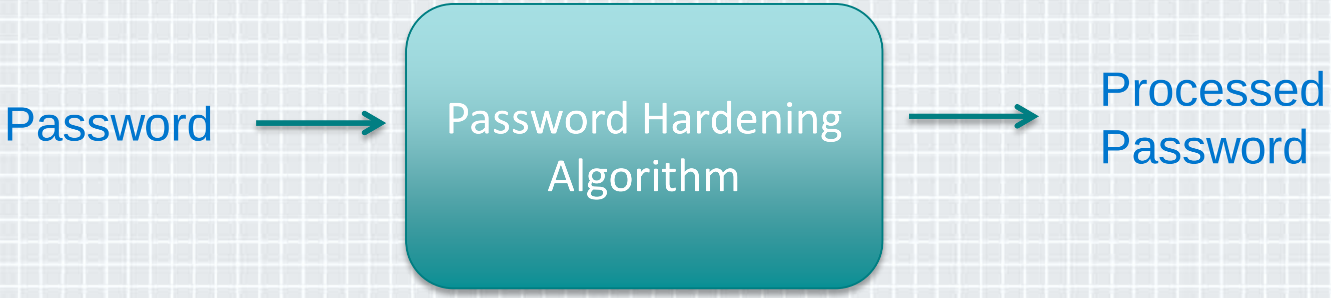
Password Entropy and Security Strength

- Security Strength:
  - A measure of the difficulty of discovering a key or breaking an algorithm.

Password Entropy and Security Strength

	Security Strength (bits)	Symmetric	RSA (bits)	ECC (bits)	Message Digest
2010	**80**	3DES (2-key)	1024	160	SHA-1
2030	**112**	3DES (3-key)	2048	224	SHA-224
Secret	**128**	AES 128	3072	256	SHA-256
Top Secret	**192**	AES 192	7060	384	SHA-384
	256	AES 256	15360	521	SHA-512

Password Entropy and Security Strength



Password

Password Hardening Algorithm

Processed Password

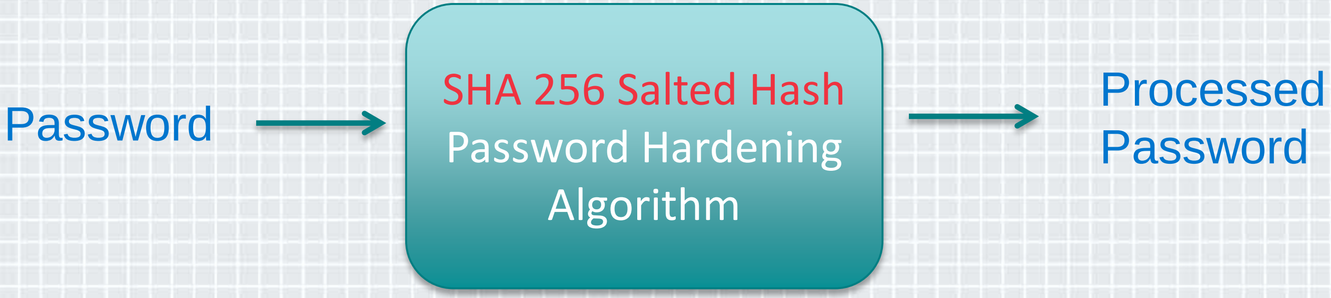
Password Entropy

Processed Password Security Strength

Password Entropy and Security Strength

- Password hardening algorithms:
  - SHA 256 salted hash
  - PBKDF2
    - Variable time factor
  - scrypt
    - Variable time / memory factor

Password Entropy and Security Strength



Password

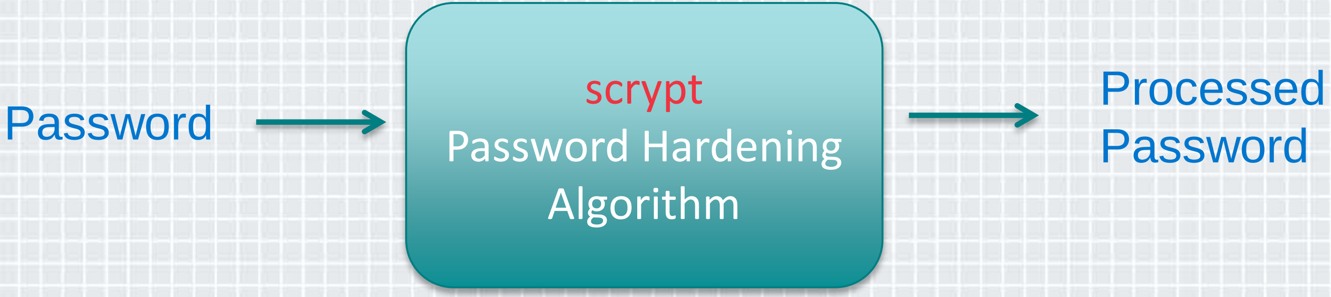
SHA 256 Salted Hash Password Hardening Algorithm

Processed Password

$$\mathit{Processed\ Password\ Security\ Strength} = \mathit{Password\ Entropy}^3$$

Note 3: With the limitation that Password Entropy < security strength of SHA256

Password Entropy and Security Strength



Password

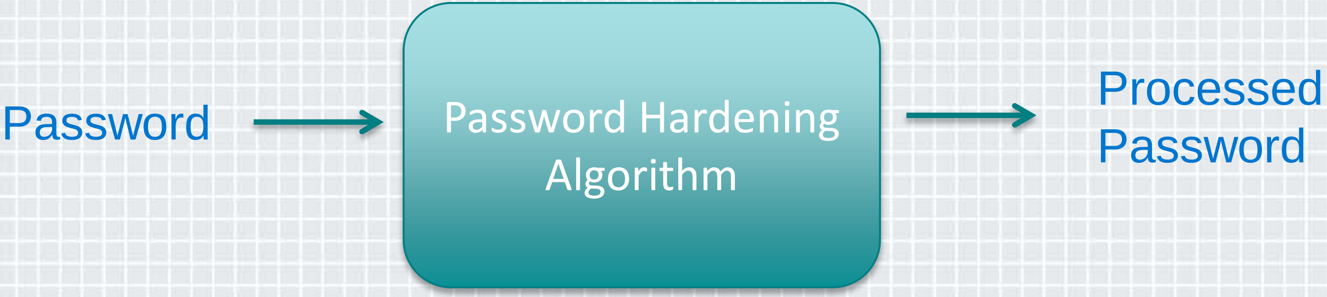
scrypt

Password Hardening Algorithm

Processed Password

$$\mathit{Processed\ Password\ Security\ Strength} = \mathit{Password\ Entropy} + \log_2\left(\frac{\mathit{scrypt\ time\ to\ process\ one\ candidate}}{\mathit{SHA256\ time\ to\ process\ one\ candidate}}\right)$$

Password Entropy and Security Strength



Password

Password Hardening Algorithm

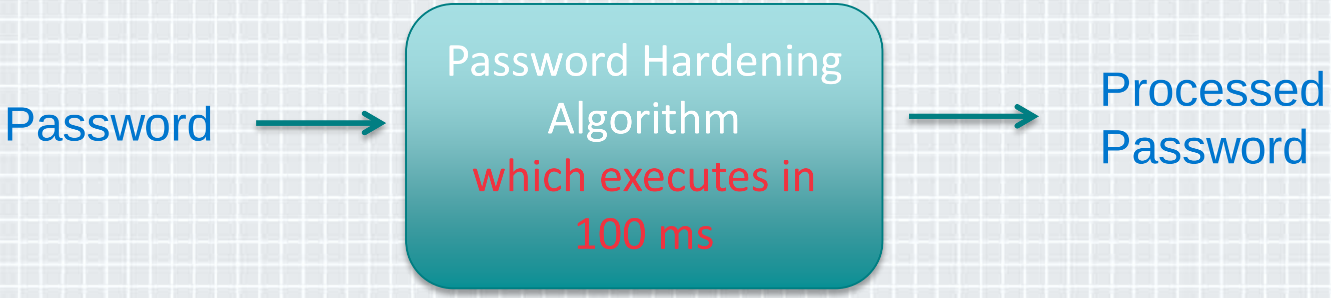
Processed Password

$$Processed\ Password\ Security\ Strength$$
$$= Password\ Entropy\ + \log_2\left(\begin{matrix} effective\ number\ of\ SHA256 \\ operations\ executed \end{matrix}\right)$$

Password Entropy and Security Strength

- Password Hardening Algorithm parameters:
  - Scale so algorithm execution time is acceptable on target hardware. 100 ms on a Samsung Galaxy S5 or iPhone 6.
  - Battery usage may be a factor in determining acceptable hardening.
- Effective number of SHA 256 operations:
  - Number of times SHA 256 can execute in 100 ms on target hardware. This is approximately 1,000,000.
    $20 \cong \log_2(1{,}000{,}000)$

Password Entropy and Security Strength



Password

Password Hardening Algorithm which executes in 100 ms

Processed Password

$$Processed\ Password\ Security\ Strength = Password\ Entropy\ + 20\ bits$$

$$Required\ Password\ Entropy$$
$$= Desired\ Processed\ Password\ Security\ Strength\ -\ 20\ bits$$

Password Entropy and Security Strength

Summary

- Entropy: The amount of uncertainty or unpredictable randomness.
- Password Entropy: The amount of entropy which can be derived from a password.
- Security Strength:
  - A measure of the difficulty of discovering a key or breaking an algorithm.
  - The security strength of a system whose strength is based on password entropy is typically limited by the entropy of the passwords.

Password Entropy and Security Strength

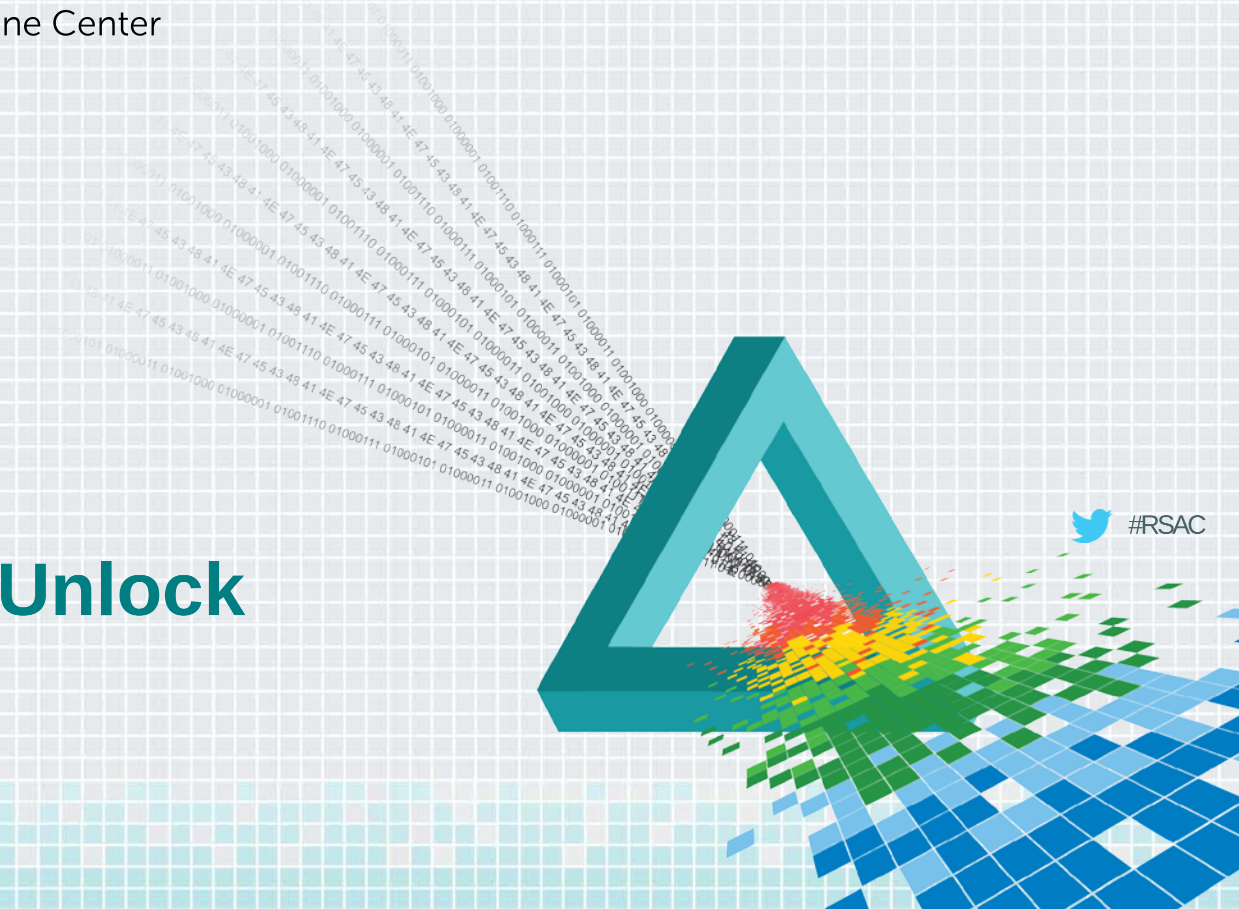
Summary

- 20 bits:
  - Approximate scaling factor between password entropy and security strength, assuming a well written algorithm which takes 100 ms to execute.
- 60 to 90 bits:
  - Amount of password entropy needed for systems which base their security strength on passwords.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

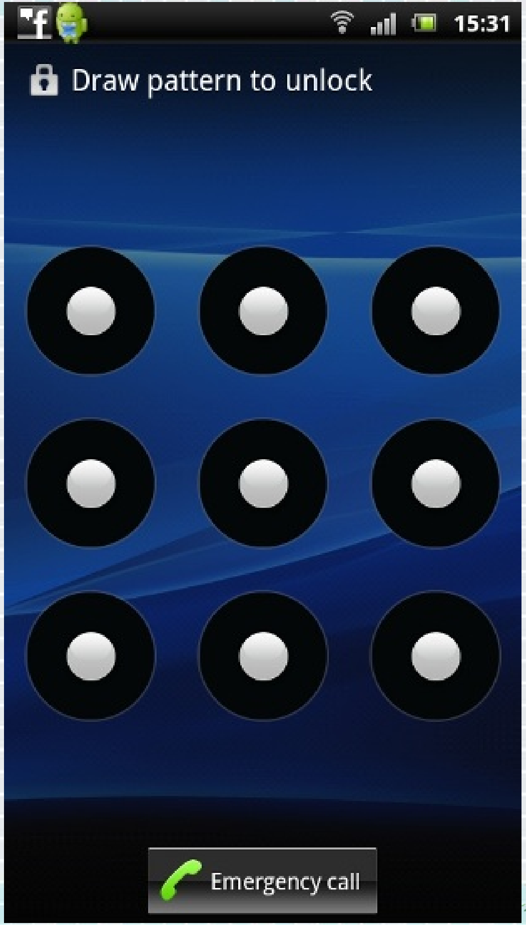
Android Pattern Unlock



#RSAC

Android Pattern Unlock

- At least four points must be chosen.
- No point can be used twice.
- Only straight lines are allowed.
- Cannot jump over points not visited before.



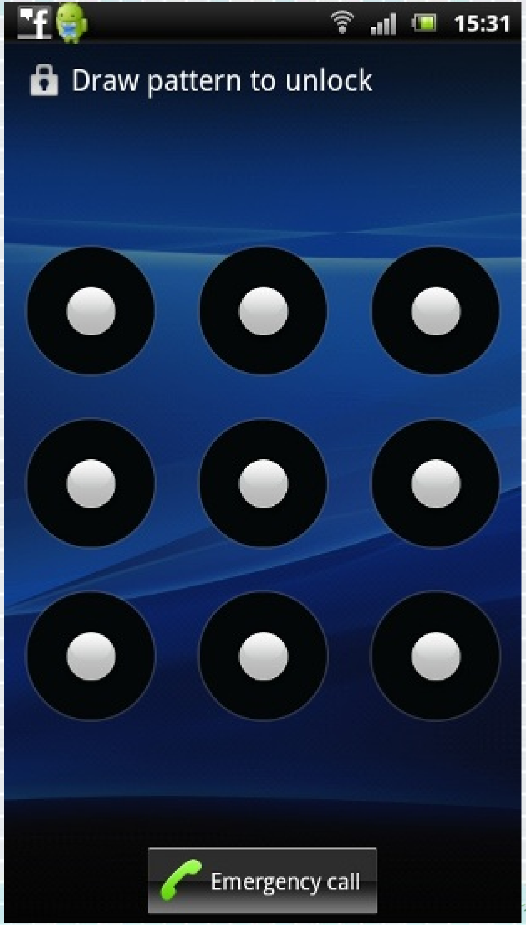
15:31

Draw pattern to unlock

Android Pattern Unlock: Video Demo

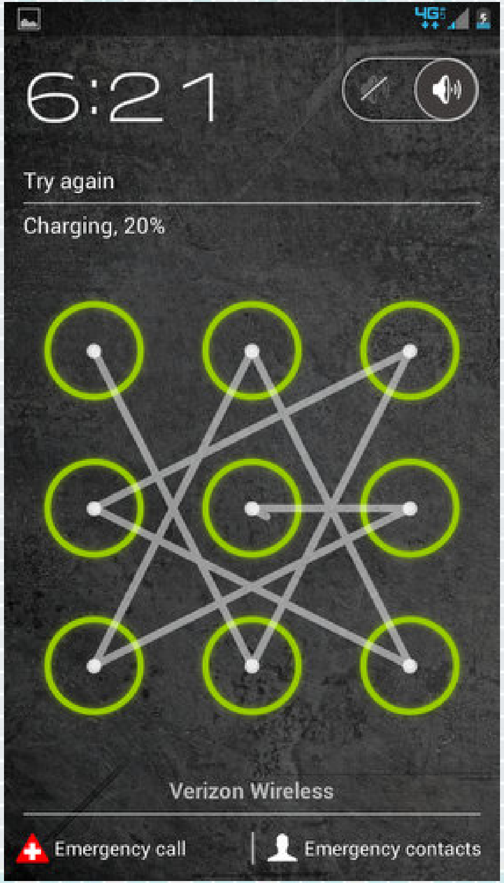
Android Pattern Unlock

- Theoretically:
  - 389,112 possible combinations.
  - Password entropy: 19 bits.
- After five failed attempts, the user is locked out for 30 seconds.



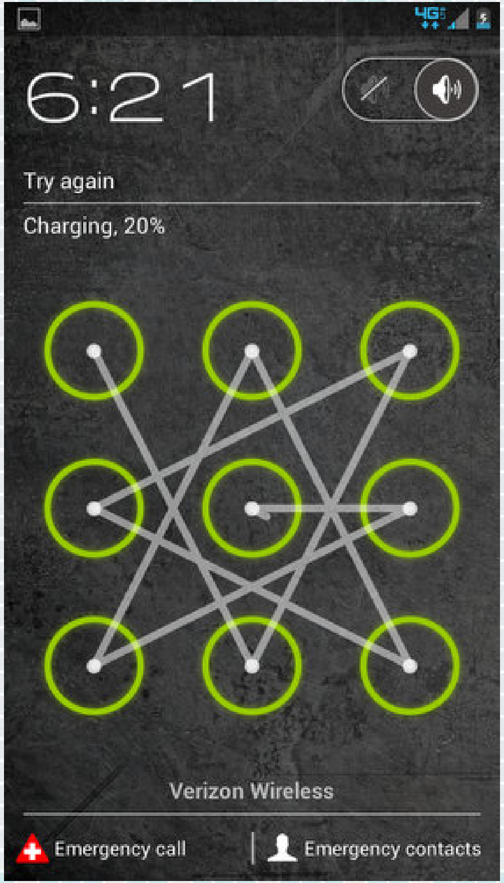
Android Pattern Unlock

- Do people really do this?



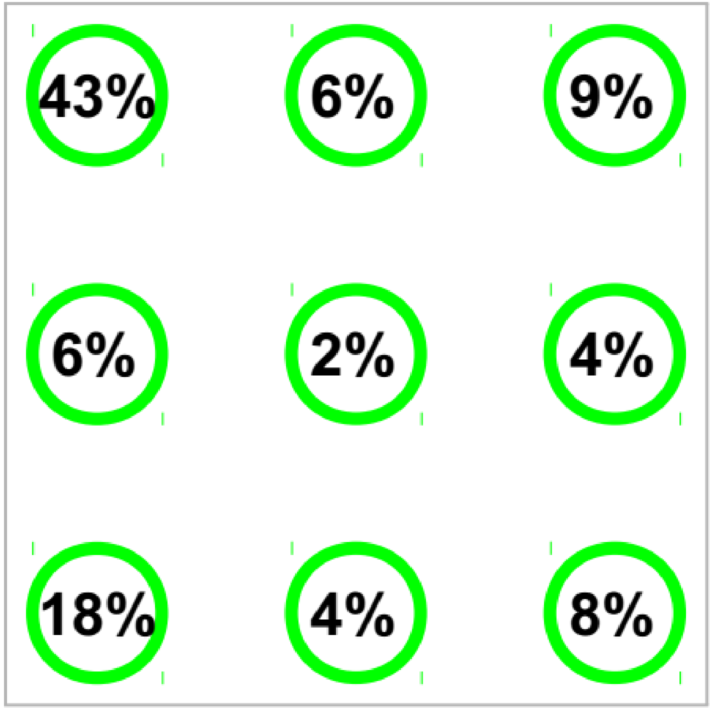
Android Pattern Unlock

- Do people really do this?
- People avoid *hard to enter* patterns.
- Most people use a 4 or 5 point pattern.



Android Pattern Unlock

- Uellenbeck et al.[4] did a user study (584 participants creating 2900 patterns) which showed:
  - Starting point bias[5].
  - Bias towards lines along outside.
  - 300 patterns capture around 50% of the whole test population.
  - Password Entropy: 8 bits for 50%.



43%	6%	9%
6%	2%	4%
18%	4%	8%

Note 4: http://emsec.rub.de/media/emma/veroeffentlichungen/2013/09/26/patternLogin-CCS13.pdf

Note 5: Probably culturally specific.

Android Pattern Unlock

- Android pattern unlock passwords are SHA1 message digested and compared with a value in a system file:

  android/data/system/gesture.key

- If your phone has been *rooted*[6], the system file is accessible.

  The pattern can then be quickly recovered by comparing the SHA1 hash of all possible patterns.

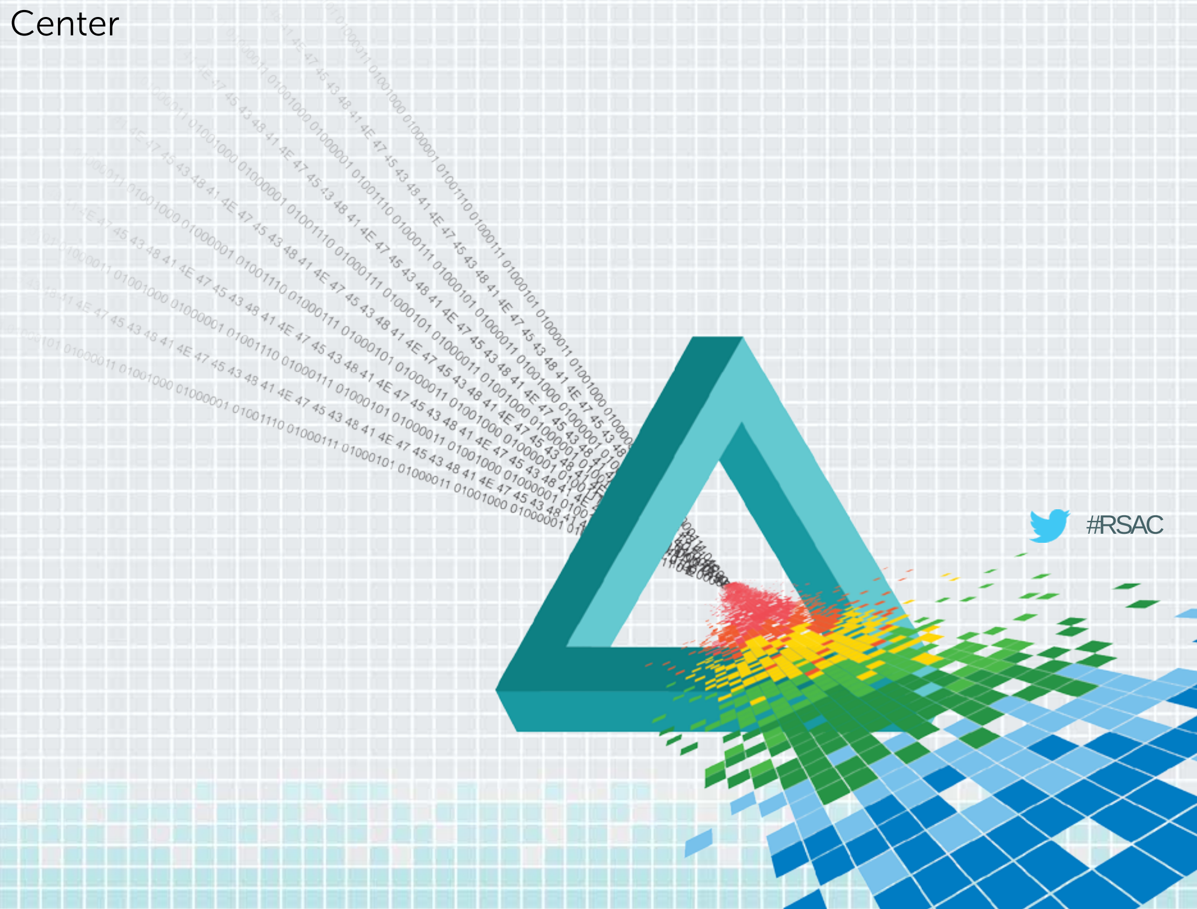
- Security Strength: between 8 bits and 19 bits.

Note 6: Rooted definition: http://en.wikipedia.org/wiki/Rooting_%28Android_OS%29

Android Pattern Unlock
Summary

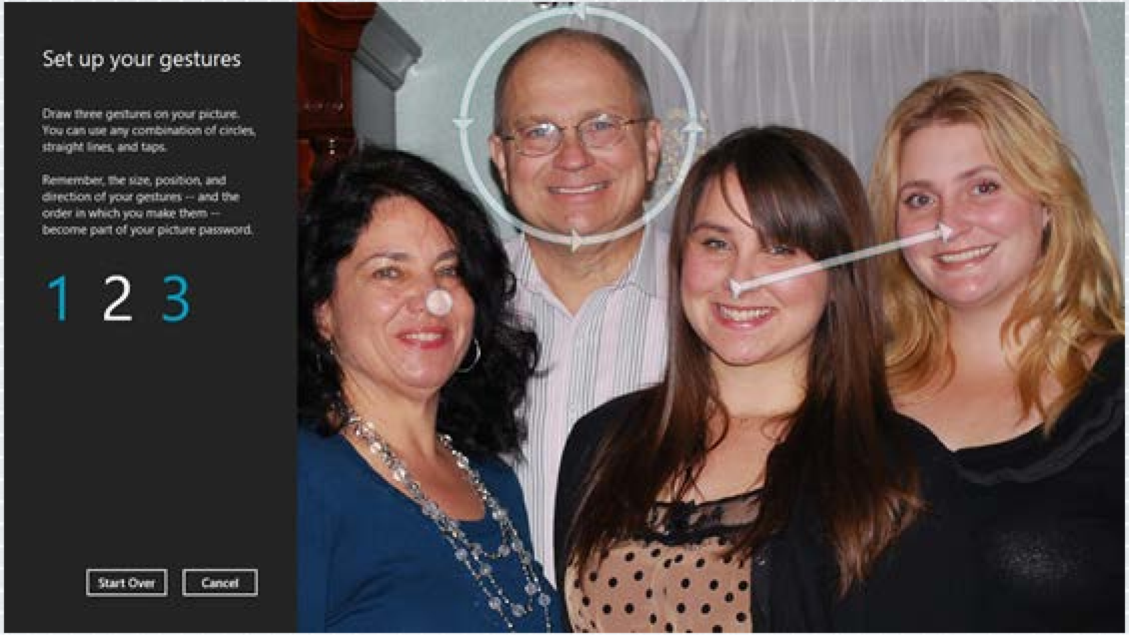
- Usability:
  - User selected.
  - Time to enter: 1 second (usually correct first attempt).
  - Easy to remember.
- Security:
  - Security Strength: 8 bits, but possibly as much as 19 bits.
  - 300 patterns cover 50% of all passwords.
  - User selected security level (user select number of points).

Windows 8
Picture Password



Windows 8 Picture Password

- User chooses photo.
- Draw three gestures in sequence.
- Circle, line, or dot.
- Direction of circle or line is important.

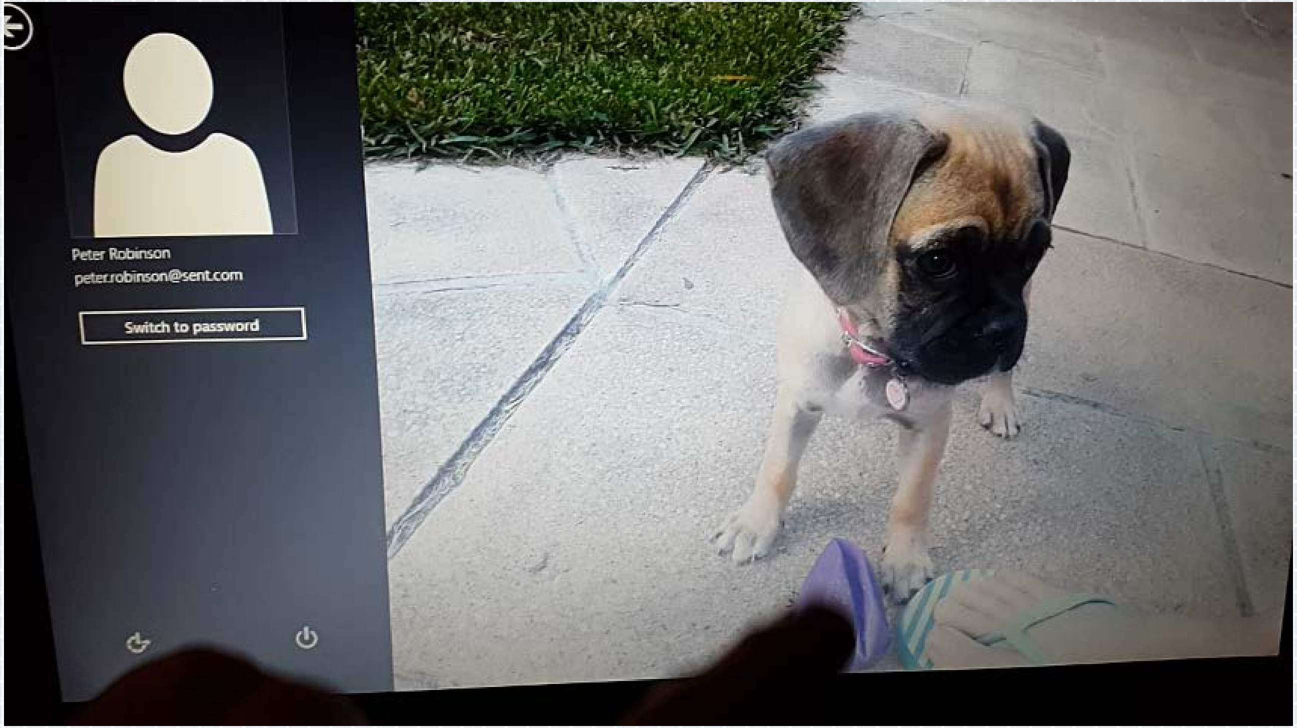


Set up your gestures

Draw three gestures on your picture. You can use any combination of circles, straight lines, and taps.

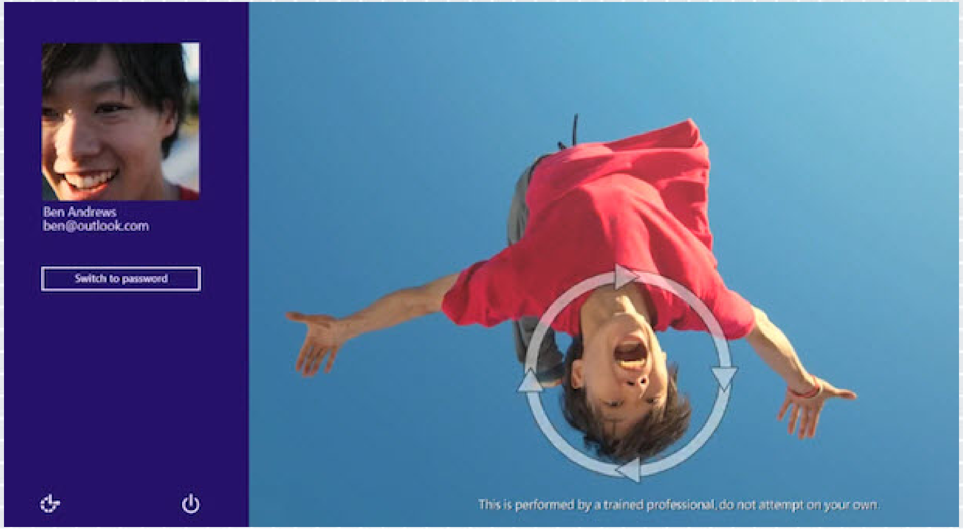
Remember, the size, position, and direction of your gestures -- and the order in which you make them -- become part of your picture password.

Windows 8 Picture Password: Video Demo



Windows 8 Picture Password

- Example passwords invariably contain a limited number of Points Of Interest.

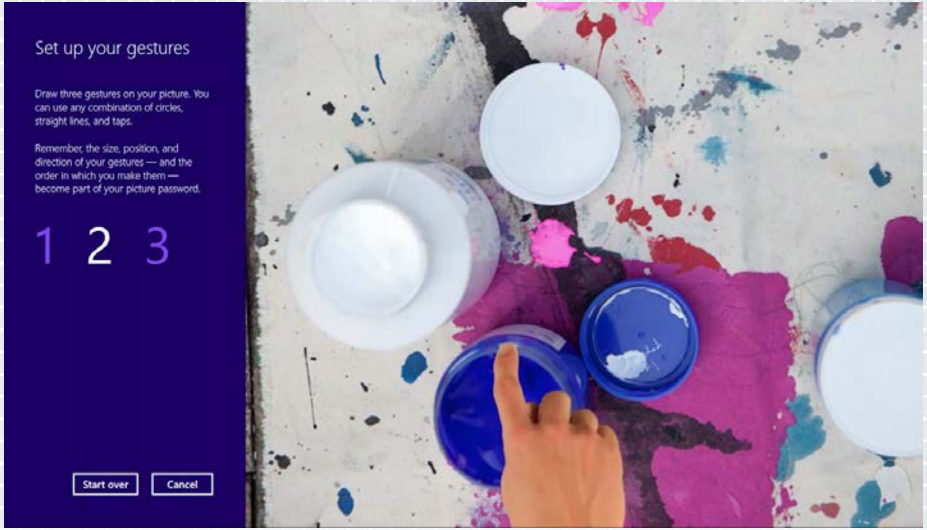


Ben Andrews
ben@outlook.com

This is performed by a trained professional, do not attempt on your own.

Windows 8 Picture Password

- From a security perspective, lines and circles are better than dots.
- However, dots are faster to enter and easier to reliably enter than circles and lines.



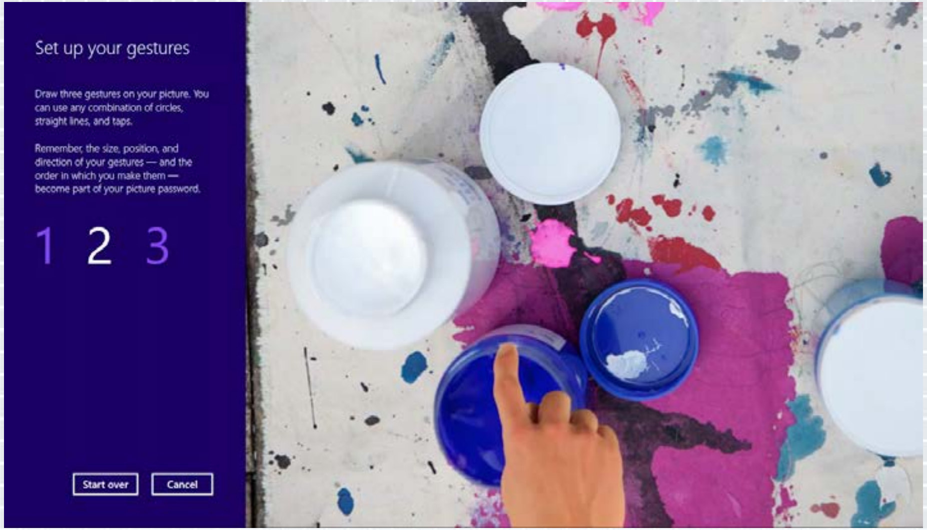
Set up your gestures

Draw three gestures on your picture. You can use any combination of circles, straight lines, and taps.

Remember, the size, position, and direction of your gestures — and the order in which you make them — become part of your picture password.

Windows 8 Picture Password

- Picture passwords can only be used for local login.
- After five failed attempts, you must enter your character based password.



Set up your gestures

Draw three gestures on your picture. You can use any combination of circles, straight lines, and taps.

Remember, the size, position, and direction of your gestures — and the order in which you make them — become part of your picture password.

Windows 8 Picture Password

- Microsoft[7] have analysed possible combinations based on the number of Points of Interest in a photo.
- They have assumed all gesture types (dot, line, circle) are equally likely, which is not the case.

Note 7: http://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-with-a-picture-password.aspx

Windows 8 Picture Password

Points of Interest	Microsoft's Analysis	My Analysis		
	Number of Combinations, assuming lines, circles and dots	Bits of Entropy	Number of Combinations, assuming dots only	Bits of Entropy
5	421,875	19	125	7
10	8,000,000	23	1,000	10
15	52,734,375	26	3,375	12
20	216,000,000	28	8,000	13

Windows 8 Picture Password

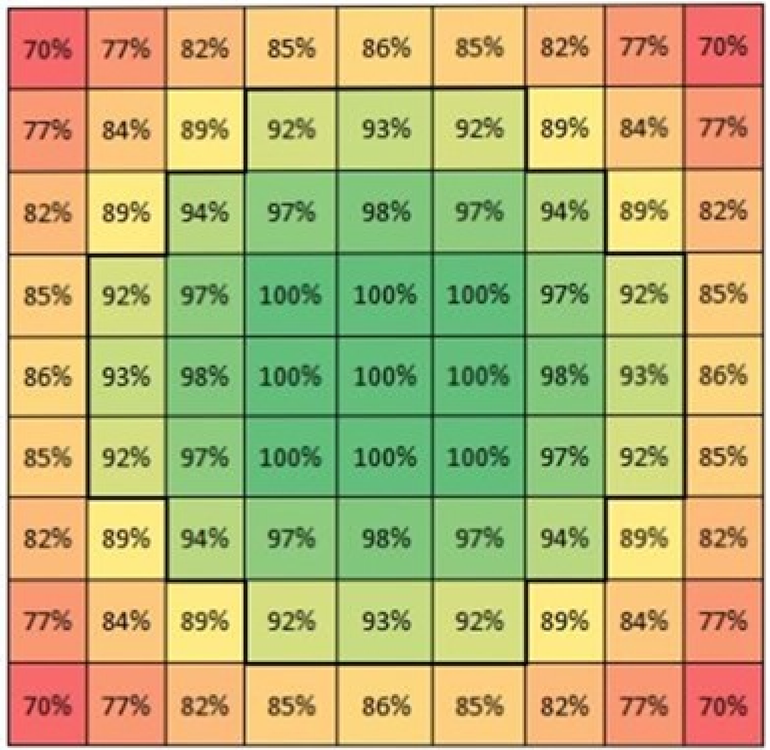
- Zhao et al.[8] devised automated analysis tools to find Points of Interest in picture passwords.

Methodology	Correct Guesses
Automated PoI recognition, 1st guess	0.8%
Manual PoI recognition, 1st guess:	0.9%
Automated PoI recognition, 5 guesses	1.9%
Manual PoI recognition, 5 guesses	2.6%

Note 8: http://sefcom.asu.edu/publications/security-picture-gesture-security2013.pdf

Windows 8 Picture Password

- The longest dimension of the image is divided into 100 segments. The shorter dimension is then divided on that scale to create the grid upon which you draw gestures[9].
- Within the grid, points nearby are deemed to be a match.

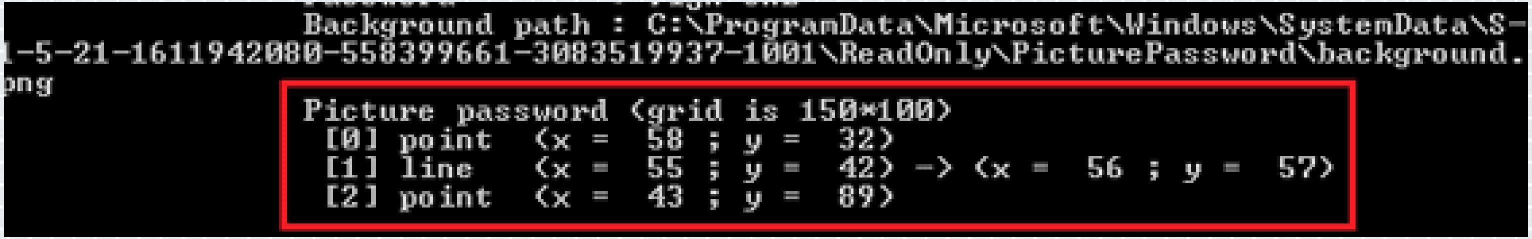


70%	77%	82%	85%	86%	85%	82%	77%	70%
77%	84%	89%	92%	93%	92%	89%	84%	77%
82%	89%	94%	97%	98%	97%	94%	89%	82%
85%	92%	97%	100%	100%	100%	97%	92%	85%
86%	93%	98%	100%	100%	100%	98%	93%	86%
85%	92%	97%	100%	100%	100%	97%	92%	85%
82%	89%	94%	97%	98%	97%	94%	89%	82%
77%	84%	89%	92%	93%	92%	89%	84%	77%
70%	77%	82%	85%	86%	85%	82%	77%	70%

Note 9: Image from: http://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-with-a-picture-password.aspx

Windows 8 Picture Password

- Windows stores the Picture Password information encrypted.
- It decrypts and compares the stored password with the entered password.
- For users with admin privileges, there are tools to recover the Picture Password information![10]



```
                    Background path : C:\ProgramData\Microsoft\Windows\SystemData\S-
1-5-21-1611942080-558399661-3083519937-1001\ReadOnly\PicturePassword\background.
png
                    Picture password (grid is 150*100)
                     [0] point  (x =  58 ; y =  32)
                     [1] line   (x =  55 ; y =  42) -> (x =  56 ; y =  57)
                     [2] point  (x =  43 ; y =  89)
```

[10] Note 10: Image from: http://www.top-password.com/knowledge/recover-windows-8-pin-code-picture-password.html

Windows 8 Picture Password

Summary

- Usability:
  - User selected.
  - Time to enter: 3 seconds for each attempt (I find it difficult to reliably enter).
  - Generally, easy to remember.
- Security:
  - Password Entropy: More than 12 bits and less than 26 bits.
  - Probability of guessing a password is 2.6%.
  - Password was encrypted, not processed by a one way function.
  - User selected security level (user selected types and position of gestures).

RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

Peter’s Graphical Password Schemes

Competing Qualities

Quality	User Selected	Computer Generated
Security	Much Lower Difficult to Measure	Much Higher Deterministic
Ease of memory	Generally Easier	Generally Harder
Speed of Entry	Generally Faster	Generally Slower

- I chose Computer Generated.

Competing Styles

Style	Processing
Grid Based	Hash / Process to a fixed value
Free Form	Encrypt plain text, or try to use Fuzzy Hashing

- I chose Grid Based.

Variable Security

Password Type / Usage		Typical Existing Passwords	NIST Entropy	Guessing Entropy
Serious	Access at work	correct horse battery staple[11]	94	44
Important	Internet Banking Work phone	bill00pay	34	30
Casual	Social networking Personal phone	truelove	27	20
Kids	Education software	home21	19	12
Android Pattern Unlock		4 points	-	8 to 19
Windows 8 Picture Password		3 dots	-	12 to 26

Note 11: See: http://xkcd.com/936/

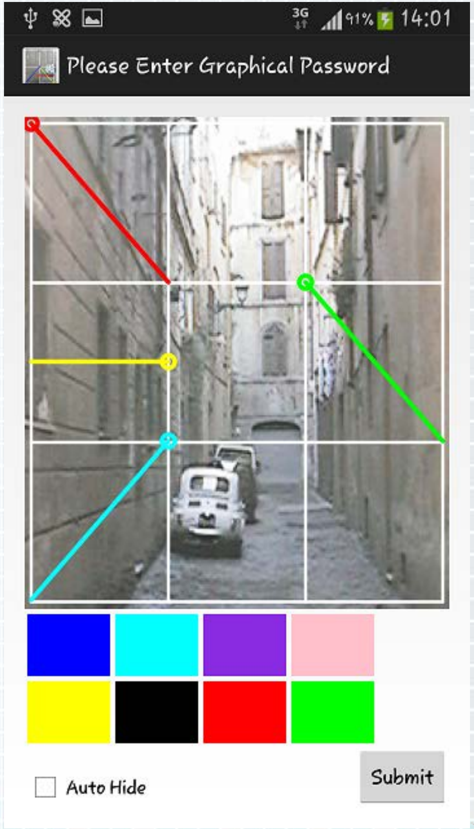
Variable Security

- I chose to design the scheme to allow different configurations for different usages, matching the security, ease of use trade-offs.

Peter's Graphical Password Scheme

Password Entry

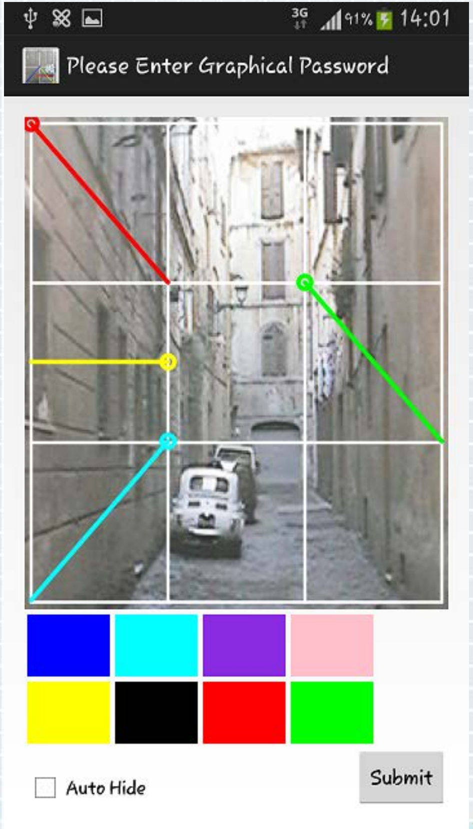
- To enter password:
  - Select the line colour.
  - Slide finger along the screen to enter a line.
  - Enter the lines in order.
  - Click on **Submit** to authenticate.



Peter’s Graphical Password Scheme

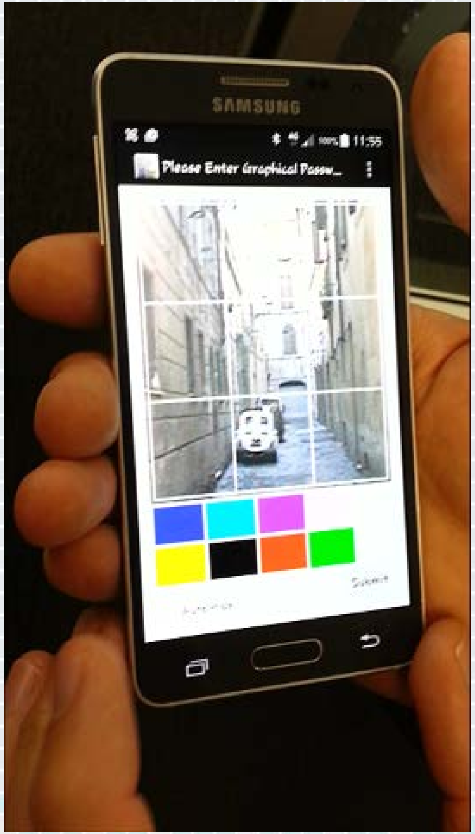
Password Entry

- Lines are snapped to the grid, either on the side or corners of boxes.
- Use the Android device’s Back button to remove the previously entered line if a mistake is made.
- Check **Auto Hide** to hide lines moments after you enter them if you are concerned about shoulder surfers.



Peter’s Graphical Password Scheme

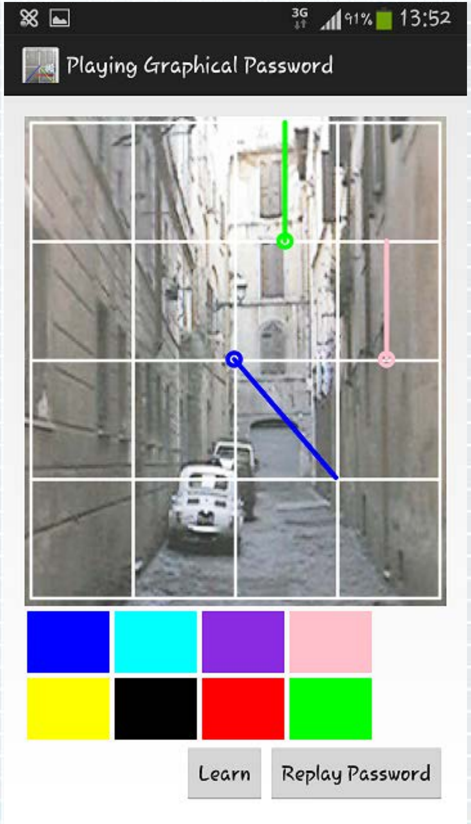
Video Demo: Authentication



Peter's Graphical Password Scheme

Password Creation

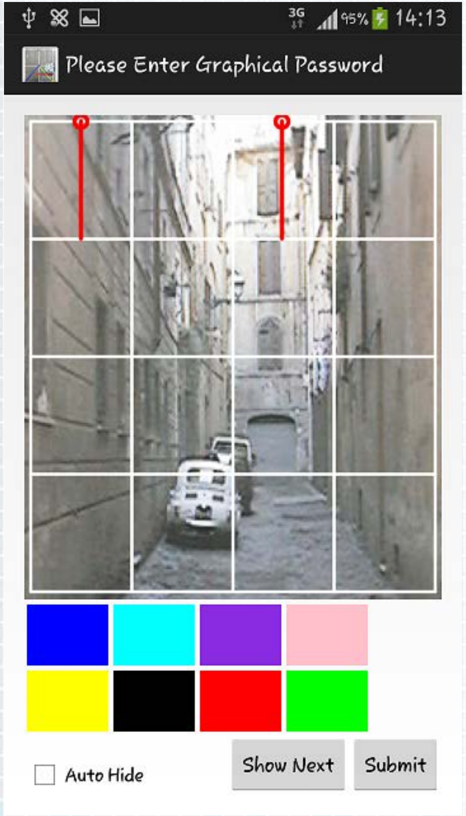
- When a password is created:
  - The password is *played* to the user; the App draws the lines one at a time.
  - The user can ask for the password to be replayed by clicking on **Replay Password**.
  - The user can learn the password by clicking on **Learn**.



Peter’s Graphical Password Scheme

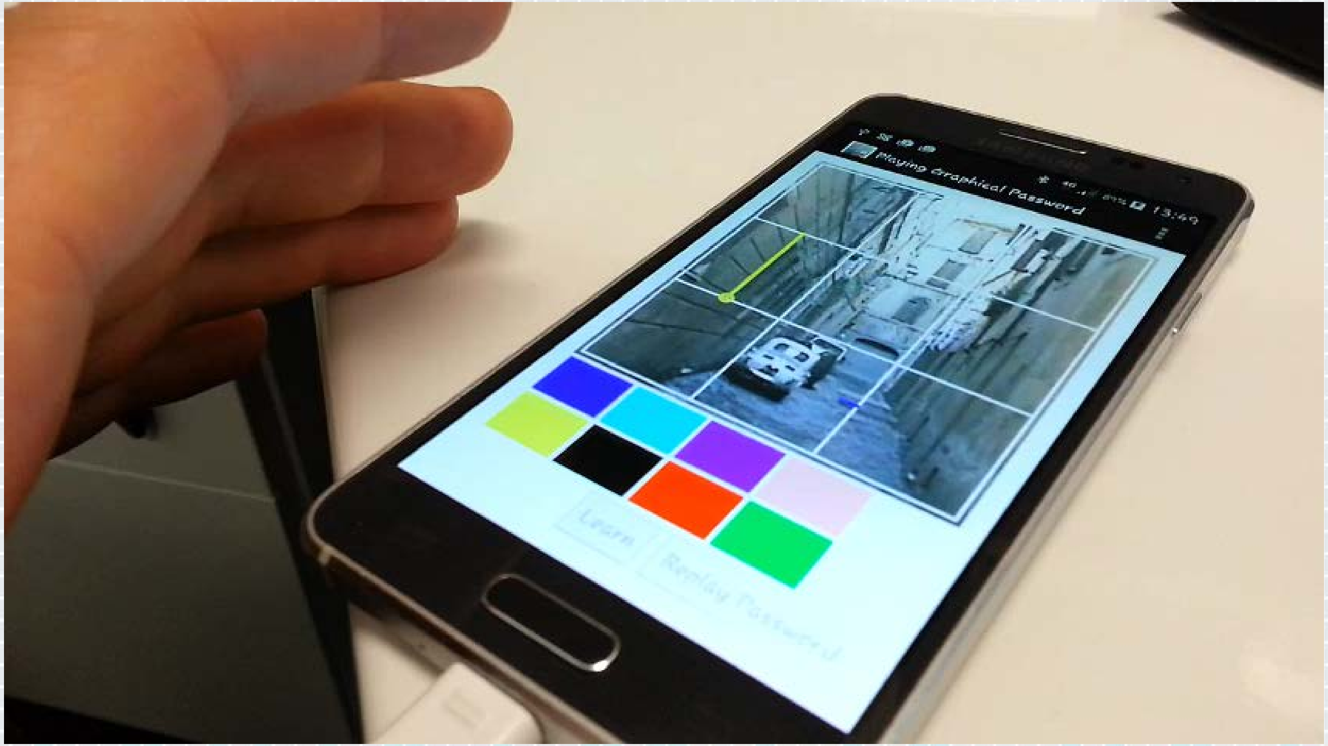
Learn Mode

- In Learn mode:
  - The user draws lines and gets feedback on whether they are correct.
  - They can ask for the next line to be drawn by clicking on **Show Next**.



Peter’s Graphical Password Scheme

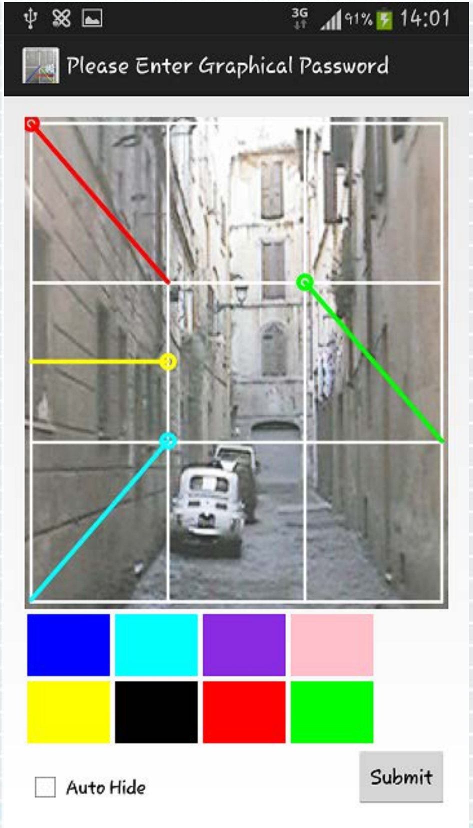
Video Demo: Learning



Peter’s Graphical Password Scheme

Default Configuration

- Default Configuration:
  - 9 cells.
  - 4 lines.
  - 8 line directions.
  - 8 line colours.
- Learning time: 60 seconds.
- Entry time: 5 seconds.
- Password Entropy: 36 bits

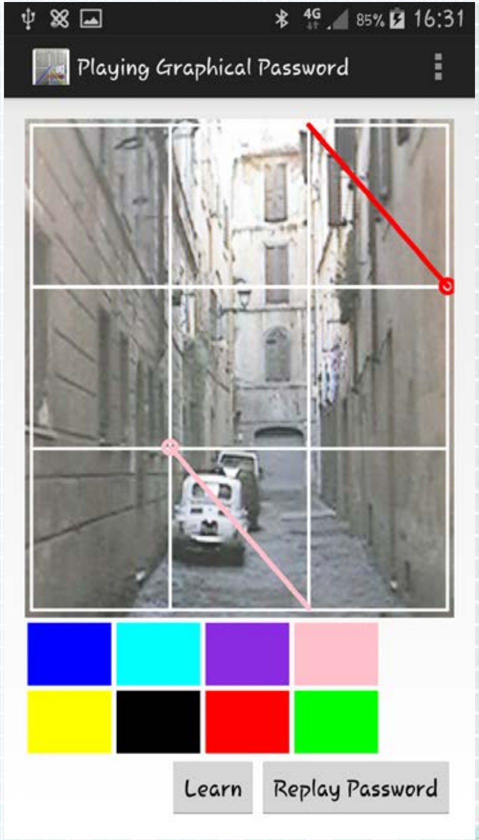


Please Enter Graphical Password

Peter's Graphical Password Scheme

Simple Configuration

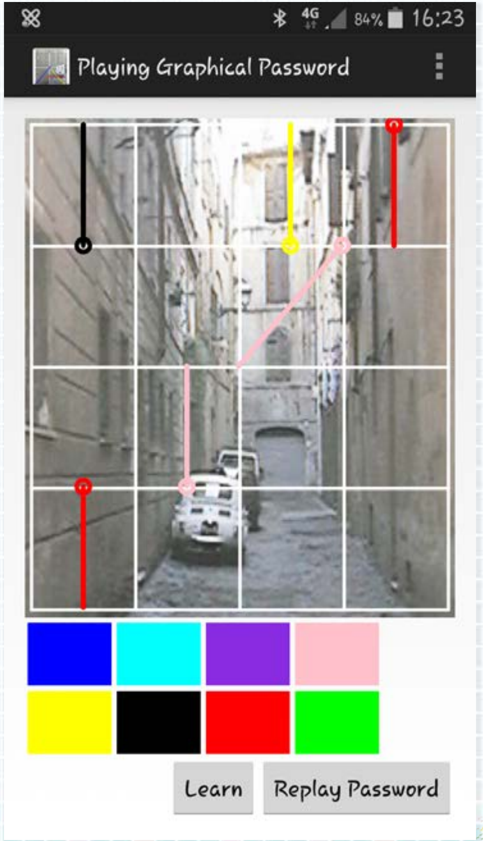
- Simple Configuration:
  - 9 cells.
  - 2 lines.
  - 4 line directions (either diagonal or along grid).
  - 8 line colours.
- Child learning time: 60 seconds.
- Child entry time: 5 seconds.
- Password Entropy: 17 bits



Peter's Graphical Password Scheme

Strong Configuration

- Strong Configuration:
  - 16 cells.
  - 6 lines.
  - 8 line directions.
  - 8 line colours.
- Learning time: 5 minutes.
- Entry time: 10 seconds.
- Password Entropy: 60 bits



Peter’s Graphical Password Scheme

Comparison

Password Category	Example Usage	Typical Existing Password	Peter’s Graphical Password Scheme
		Guessing Entropy	Entropy
Serious	Access at work	44	60
Important	Internet Banking	30	36
Casual	Social networking	20	36
Kids	Education software	12	17

Peter's Graphical Password Scheme

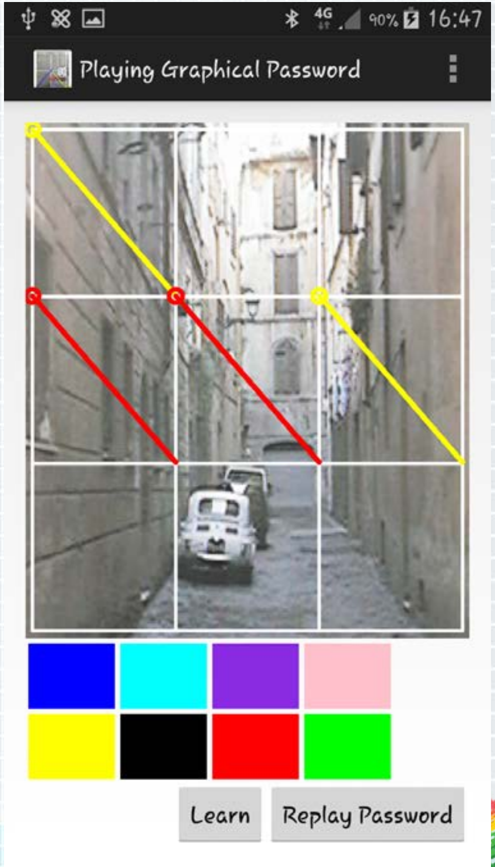
Auto Simplification

- Auto simplification:
  - A method of generating new passwords which are simpler, whilst minimally reducing password entropy.
  - Good for users who forget their password and need a password reset.
- Parallel to PIN number auto simplification:
  - Initial PIN: 4673
  - After first PIN reset: 4554
  - After second PIN reset: 1234
  - After third PIN reset: 1111

Peter’s Graphical Password Scheme

Auto Simplification Methodology

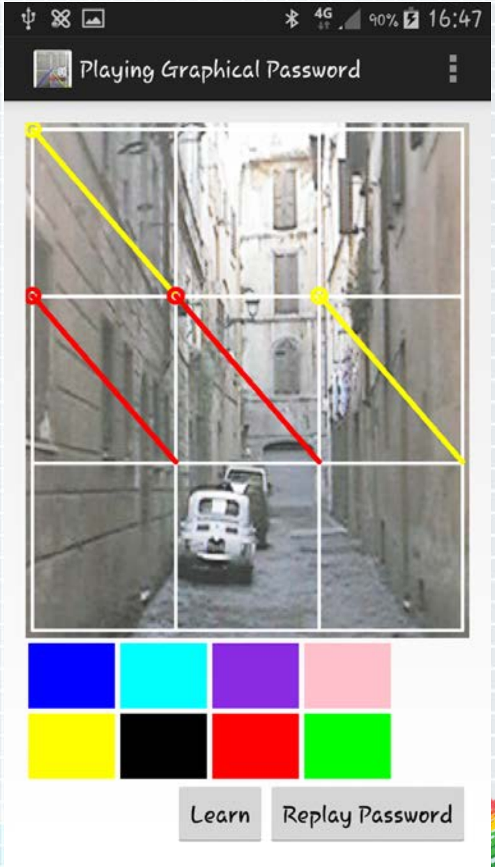
- Randomly select first line.
- Base subsequent lines on the first line. Randomly select between:
  - Same colour or sub-set of colours and / or
  - Same direction or sub-set of direction and / or
  - Same cell or sub-set of cells.



Peter's Graphical Password Scheme

Auto Simplification Methodology

- As the first line is randomly selected:
  - First line has full entropy.
- As there are many options for how subsequent lines can be simplified:
  - Entropy of subsequent lines is greater than if a deterministic simplification approach was used.
- A graduated amount of simplification can be applied.



Peter’s Graphical Password Scheme

Auto Simplification Methodology

Simplification Scheme	Password Entropy
None: 9 cells, 4 lines, 8 colours, 8 line directions	36
9 cells, 4 lines, 8 colours, 2 line directions	32
9 cells, 4 lines, 2 colours, 8 line directions	32
9 cells, 4 lines, 8 colours, same line direction	29
9 cells, 4 lines, 8 directions, same colour direction	29
9 cells, 4 lines, same colour and same direction	20

- What is the minimum entropy you are comfortable with?

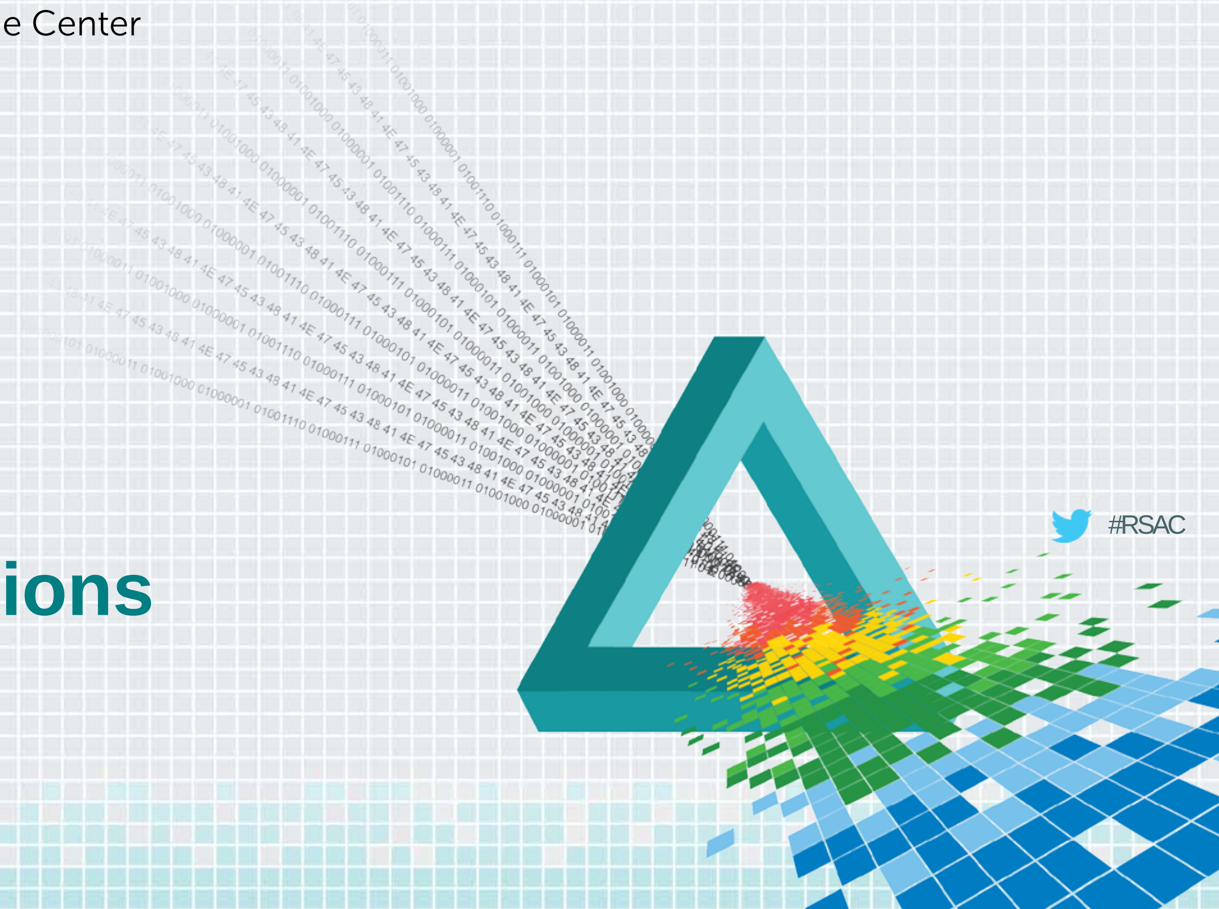
Peter’s Graphical Password Scheme

Summary

- Usability:
  - Computer generated.
  - Time to enter: 5 to 10 seconds, depending on configuration.
  - As hard to remember as equivalent character based password.
- Security:
  - Entropy: 17 to 60 bits, depending on configuration.
  - User / application selected security level.
  - Auto simplification.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

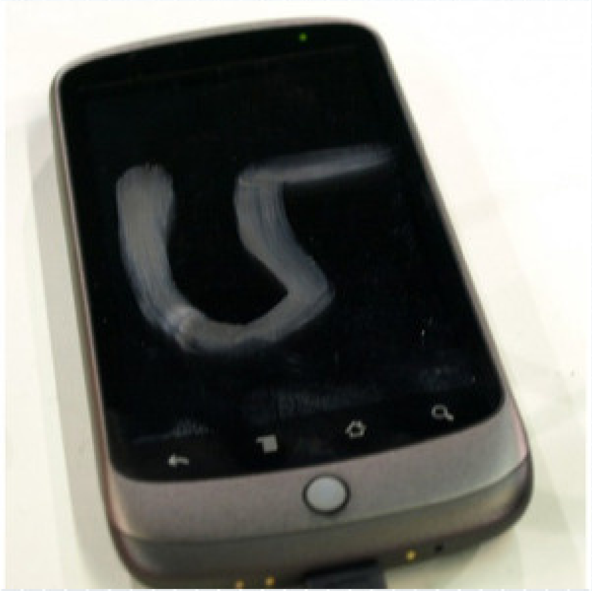


#RSAC

Other Considerations

Other Considerations

- Smudge Attack[10]:
  - Wikipedia, "..a method to discerning the password pattern of a touchscreen device…"
  - A big factor in degree of smudge is how hard the user touches the screen.
- My graphical password scheme provides some protection against this type of attack:
  - Line colours.
  - Line ordering.
  - The intricate nature of the password promotes lighter touch.



Note 10: http://static.usenix.org/events/woot10/tech/full_papers/Aviv.pdf

Note 11: Photo from: https://guardianproject.info/2012/01/04/strong-mobile-passwords-with-yubikey-usb-token/

Other Considerations

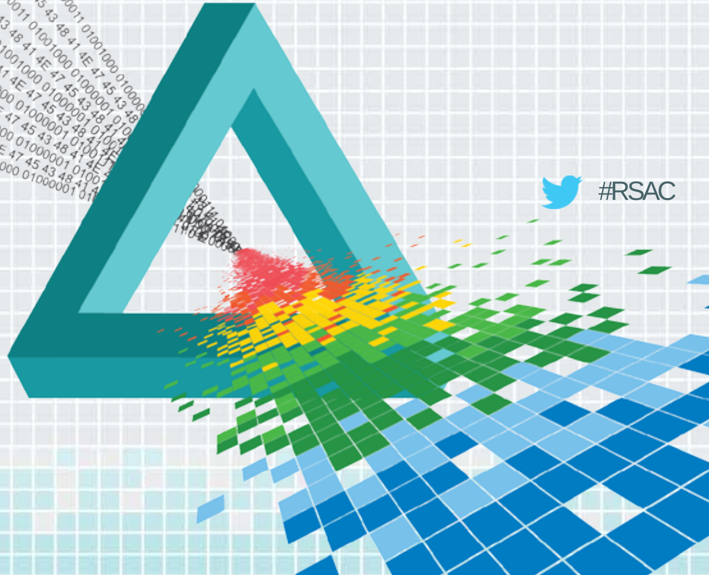
- Offline attack and online attack.
- Colour blind[12] support.
- Gamification: Gamify graphical password learning.
- Biometrics: They can never be revoked.
- Complex passwords, TodayIsAGreatDayToHaveAL1zPassword:
  - Allow more than three attempts before lockout.
  - Allow password hiding to be optional.

Note 12: http://www.colourblindawareness.org/colour-blindness/types-of-colour-blindness/

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Wrapping Up



#RSAC

Security Strength Gap

- 112+ bits security strength: What we need.
- 20 bits hardening: 100 ms of password hardening.
- 60 bits entropy: What my algorithm can supply.
- 32 bits: The difference between what we need and what we can achieve.

How to Apply this Information?

- In the systems you have today:
  - What are the password requirements?
  - How are passwords processed?
  - What security strength does your system need?
- When you assess a graphical password scheme, compared to existing passwords for the same usage:
  - Is it more secure?
  - Is it easier to remember?
  - Is it faster to enter?

Summary

- Google’s Android Pattern Unlock and Microsoft’s Windows 8 Picture Password, given typical usage, are very weak.
- My graphical password scheme offers varying levels of security depending on configuration and usage. For each usage, when compared with traditional passwords, it offers:
  - Password entropy: Better.
  - Ease of memorization and speed of entry: Similar.
- My password scheme can’t deliver as much entropy as we need.

Any Questions?

- Peter Robinson: peter.robinson@rsa.com