University of BRISTOL

A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks

P Andriotis, T Tryfonas, G Oikonomou, C Yildiz
(presented at ACM WiSec 2013, Budapest)

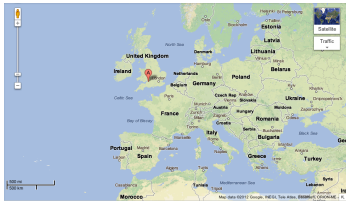
@theotryfonas

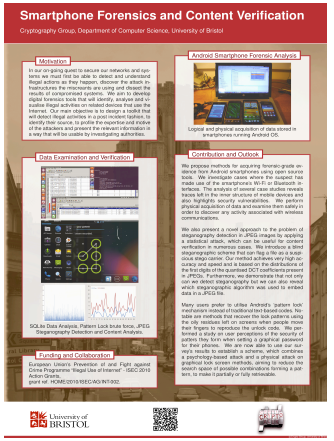
Ionian Uni. Seminar
Wed., 15 May 2013

Where are we from?

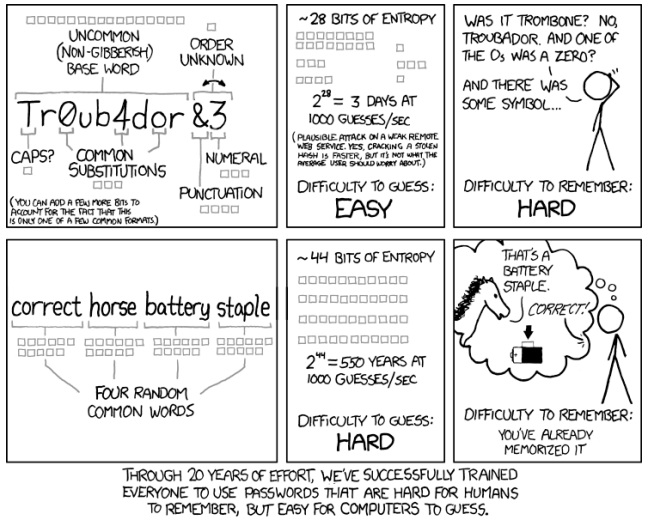
University of BRISTOL

CSE BRISTOL CRYPTO ACUK





http://xkcd.com/936/



Talk Outline

- Graphical password authentication
  - Android pattern lock mechanism
- Physical attacks
  - Thermal camera to detect swiped pattern heat emission
  - Optical camera, microscope to detect swiped pattern oily residues (smudges)
- Pattern-setting survey: security vs. usability perceptions of android users
  - Web-based survey results
  - Physical side-channel attack validation
- Further work

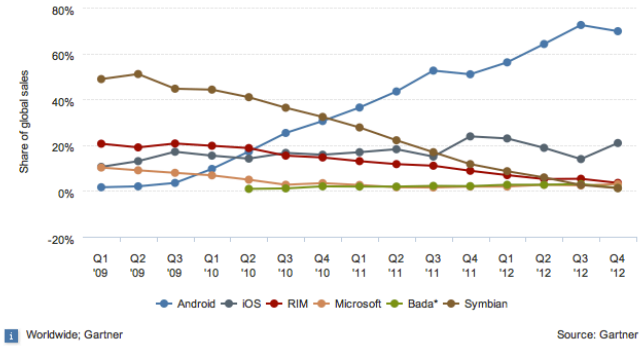
Authentication with graphical passwords

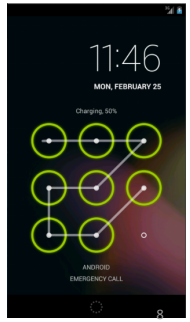
- Existing attacks concentrate on
  - 'hot spot' identification (areas of used image concentration)
  - Dictionary style attacks taking into account 'password' length, number of components, symmetry

Authentication with graphical passwords (cont'd)

- Studies detected some cognitive biase in choosing graphical passwords
  - as in e.g. the Passfaces system, with attraction and race preference
  - 10% of male passwords were guessable in **two attempts!**

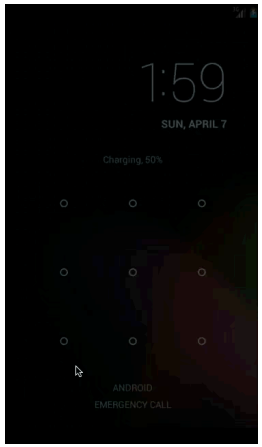
Motivation: Android's popularity and pattern lock mechanism use





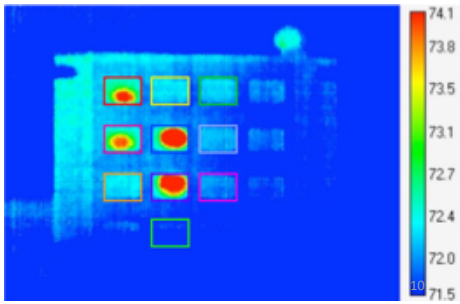
The Android Pattern Lock

- Min 4 and Max 9 nodes to create a pattern.
- Nodes can be visited only once.
- Total number of possible patterns is 389,112.

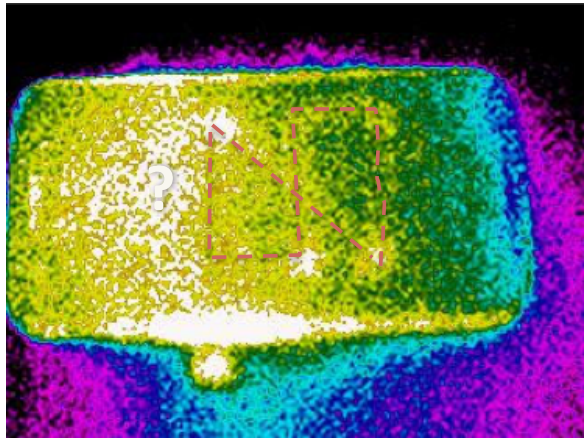


'Side channel' attacks on pattern locks

- Attacks based on information gained from the physical implementation of a security scheme are called side channel attacks
  - E.g. existing thermal attacks on ATMs



Thermal emission detection



Oily residue detection

- With a hi res camera
- With a microscope

Detecting directionality

Figuring out the swiped pattern

Despite oleophobic coating!

Survey Objectives

- Understand how perceptions of security or usability affect the effectiveness of the mechanism
- Detect biases in the setting of the patterns as graphical passwords
- Facilitate the recovery of locking patterns for forensics and intelligence purposes

Survey instrument

- Done on-line
  - Webpage was live at http://patternsurvey.biz/
- Key questions (pilot) included
  1. Demographics (gender, age)
  2. Experience with smartphones
  3. Use of patterns or not
  4. Asked to set a secure pattern
  5. Asked to set a usable pattern
  6. Preference of pattern between those and why

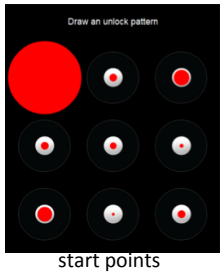
Data Analysis

- Calculated average pattern lengths
- Calculated average number of direction changes
- Computed entropy per node (frequency metric)
  - i.e. probability of being selected as start or end point or monogram selected in the pattern
- Computed conditional entropy of *n*-grams (Shannon's formula)
  - i.e. most frequently used bi-grams, tri-grams, four-gams (sub-patterns of swiped paths)

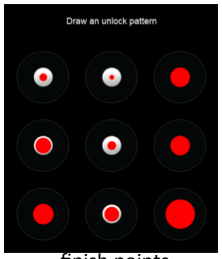
Survey results

- 144 unique participants
- Gender: **Male** 66%, **Female** 34%
- Age: **18-29** 81%, **30-49** 15%
- 92% own a smartphone of which 40% use Android
- Less than half (47%) use any type of lock, primarily to
  - Protect personal data
  - Prevent fiddling
- …

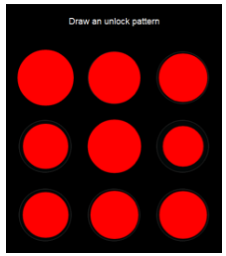
Survey results (cont'd)



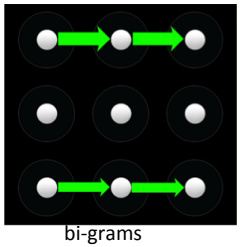
start points

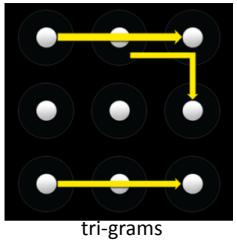


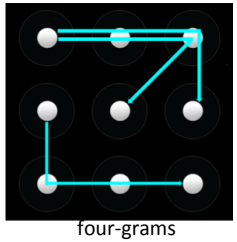
finish points



monograms


bi-grams


tri-grams


four-grams

Survey results (cont'd)

Table 1: Average pattern lengths and standard deviations.

Group	Average Length		Standard Deviation	
	Secure	Easy	Secure	Easy
Females	6.16	5.94	1.87	1.75
Males	6.89	6.32	1.91	1.94
Total	6.64	6.19	1.92	1.88

Table 2: Average number of direction changes (all users).

Average Changes		Standard Deviation	
Secure	Easy	Secure	Easy
3.57	2.74	1.65	1.59

Preliminary validation: performing side channel attacks (physical/behavioral)

- 22 participants:
  - Male: 68%, Female: 32%
- Origin:
  - Europe: 59%, Asia: 32%, America: 9%.
- Apply a secure pattern lock on device.
- Take photo with DSLR camera.

Preliminary validation (cont'd)

Optical Attack	Number	Percentage
0 - 49% of pattern	5/22	22.73%
50 - 99% of pattern	5/22	22.73%
100% of pattern	12/22	54.54%
Total Recovery	18/22	81.82%
Phychological	**Number**	**Percentage**
Start point	18/22	81.82%
End point	11/22	50.00%
Bigrams	12/22	54.54%
Trigrams	7/22	31.81%
Fourgrams	4/22	18.18%
Direction (C)	14/22	63.63%
Total Retrieval	20/22	90.9%

Further work

- Extended data set
- Add more detailed demographics (mother tongue, dexterity, location)
- Further analytics (e.g. symmetry detection, other cognitive biases)
- Validate the gender bias claim (over ⅓rd of the pilot sample were women)
- Link with decision-making theory (e.g. prospect theory) to develop profiles of pattern preferences per decision-making type (suspect type)

Thank You

Any Questions?

Theo.Tryfonas@bristol.ac.uk

Panagiotis Andriotis, Theo Tryfonas, George Oikonomou, Can Yildiz.
"A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks. "

Security and Privacy in Wireless and Mobile Networks - WiSec 13, ACM, pp. 1-6, 2013.

This work has been supported by the European Union's Prevention of and Fight against Crime Programme "Illegal Use of Internet" - ISEC 2010 Action Grants, grant ref. HOME/ 2010/ISEC/AG/INT-002

Sources

- Aviv, et al. Smudge attacks on smartphone touch screens. In Proceedings of the 4th USENIX conference on Offensive technologies, pages 1–7. USENIX Association, August 2010.
- Mowery et al. Heat of the moment: characterizing the efficacy of thermal camera-based attacks. In Proceedings of the 5th USENIX conference on Offensive technologies, pages 6–6. USENIX Association, August 2011.
- Oorschot et al. On predictive models and user-drawn graphical passwords. ACM Trans. Inf. Syst. Secur., 10(4):5:1–5:33, January 2008
- Thorpe et al. Human-seeded attacks and exploiting hot-spots in graphical passwords. In USENIX Assosiation Proceedings of the 16th USENIX Security Symposium, pages 103–118. USENIX Association, August 2007.