Smartphone Users’ Family, Friends, and Other Enemies

Konstantin (Kosta) Beznosov
risks to smartphones

- Malware
- Theft — on decline due to “kill switch” and activation barriers
- Loss — Find my iPhone service and alike.

- Strangers
- Social insiders
  - Coworkers
  - Spouses
- Parents/Kids
- Classmates/Friends
- Etc.

scope of this talk
four studies
smartphone study

- semi-structured interviews (N=22) — Nov. 2011
  - users’ concerns with sensitive data.
- MTurk survey (N=724) — early 2012
  - strangers vs. insiders

Android study

- Android monitoring app (N=41)
- 20 days between 12/20/2014 and 3/13/2015
- (un)locking and app usage behaviour

Touch ID study

small-scale (N=90)
• in-person survey
• late 2014
• iPhone model and passcode length verification

online larger-scale (N=374)
• MTurk survey (US/95%)
• early 2015
• unlocking method and iPhone model verification

• privacy-preserving MTurk survey (N=1,381) — 2015

• MTurk followup (N=653) — early 2016

findings
smartphones contain various data

- Photos and videos (phv)
- SMS/MMS messages (sms)
- Call history (cah)
- Emails (eml)
- Contacts details (cod)
- Music (mus)
- Browser search history (bsh)
- Browsing history (bwh)
- Events in calendar (evt)
- Notes and memos (n&m)
- Data in social networking applications (osn)
- Progress in games (gam)
- Documents (doc)
- Voice recordings (voc)
- Psswds saved in apps or psswd managers (pwd)

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
users’ concerns about insiders and strangers are comparable.
20% of US adults had engaged in snooping in a 1-year period
likelihood correlates with age and ...
... and with depth of adoption

![Graph showing predicted likelihood (0 to 1) vs. depth of adoption (scale 10-70)]
adoption of locking

Android

Harbach, UCB, SOUPS '14

57%

43%

50%

50%

PIN/Password/DAS

Slide-to-Unock / None

Mahfouz, UBC

PMC '16

46%

54%

Android Study

iPhone

Harbach, UCB

CHI '16

5%

95%

Touch ID study
users lock their phones against

proportion of participants

non-Touch ID (n = 201)  Touch ID (n = 173)

2% 2%

Others
Roommates 16% 27%
Classmates 16% 27%
Family 29% 30%
Friends 26% 42%
Co-workers 37% 54%
Strangers 97% 99%

Touch ID study

Laboratory for Education and Research in Secure Systems Engineering (lerse.ece.ubc.ca)
users lock their phones against

<table>
<thead>
<tr>
<th></th>
<th>non-Touch ID (n = 201)</th>
<th>Touch ID (n = 173)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Others</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>Insiders</td>
<td>58%</td>
<td>59%</td>
</tr>
<tr>
<td>Strangers</td>
<td>97%</td>
<td>99%</td>
</tr>
</tbody>
</table>

Touch ID study

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
those who lock, use more often …

Figure 2: Average number of unlocking attempts per day: (a) for Locked and Not-Locked groups, where the “overall” shows the results for all 41 participants; (b) for participants grouped by the used unlocking method. In both figures, the red squares and the horizontal lines in the boxes represent the mean and the median values, respectively.

In addition, Pattern participants were unlocking their devices 27% more often than the participants from Not-Locked group. We did not find statistically significant difference in the remaining pair-wise comparisons. The spread of the average number of unlocks per day is shown at Figure 2b.

4.1.2. Auto/User Locking

The value of auto-lock timeout in Android OS defines how soon a smartphone will lock itself after the device enters the sleep mode, i.e., turns off the screen as a result of a user not being active. This timeout can be chosen by the user in discrete values. The default is 5 seconds. Note, that if a user explicitly presses the power button, then the device locks immediately. For each participant, our app read the auto-lock timeout value from Android system’s settings. This value only has a meaning for the participants from Locked group, because it only applies to the devices that has authentication-based unlock setup, i.e., a user has set a PIN, a Password or a Pattern for device unlock.

Our analysis revealed that only 6 participants (out of 22 in Locked group) …
... and for longer, each time

Android study (N=41)

Percentage [%]

Session-Length for Locked (seconds)

average 50 seconds

Session-Length for Not-Locked (seconds)

average 46 seconds

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
unlocking methods vary in cost

Figure 3: The distributions of (a) locking types (auto-lock or user-lock) and (b) entry time for different screen-lock methods over locked group (N=22). The red squares and the horizontal lines in the boxes in (b) represent the mean and the median values, respectively.

On the other hand, if a user presses the power button, a smartphone locks immediately. We refer to such cases as user-lock. In contrast to auto-lock, user-lock does not leave any opportunity for an attacker to gain unauthorized access (by accessing the phone before it auto-locks). In order to measure how often participants used user-lock we recorded all power button pressed events, i.e., ACTION_SCREEN_OFF events at Figure 1 that were triggered by the user pressing power button. These records allowed us to classify all locked states into two groups: auto-locked and user-locked. The distribution of average daily unlocks and how they split into these two groups is shown at Figure 3a.

Statistical analysis revealed a statistically significant difference in the distribution of locked states originating from auto-lock and user-lock between subjects that used PINs, Passwords and Patterns (Bonferroni corrected, \((2) = 2328, p < 0.05\)). Furthermore, the results of pairwise comparison suggest that there is a statistically significant difference between each pair (Bonferroni corrected \((2)-test, p<0.05\), Pattern vs. PIN \((1) = 2216\), 13 Android study (N=22)

<table>
<thead>
<tr>
<th>Unlocking Method</th>
<th>Likelihood of an error [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern</td>
<td>4.1</td>
</tr>
<tr>
<td>PIN</td>
<td>2.5</td>
</tr>
<tr>
<td>Password</td>
<td>1.7</td>
</tr>
</tbody>
</table>

Android study (N=22)
30-80% cost for shorter sessions

Relative Cost of Unlocking [%]

CU = UT / (ST + UT)

Android study (N=41)
The top ten applications comprise 57% of all observed sessions.

- Facebook
- Dialer
- Whatsapp
- Contacts
- Messaging
- Chrome Browser
- Facebook Messenger
- Gmail
- Internet Browser
- Instagram

564 apps observed in the study

Android study (N=41)
85% of sessions involved 1-3 apps

25 seconds average time for 1-2 app sessions

Android study (N=41)
Touch ID & iPhone security
how unlock works
(iPhone 5s and later)

user

passcode
e.g., “3985”

fingerprints

Touch ID Sensor

Secure Enclave Co-processor

Class Keys

“3985”

Touch ID Sub-System

Class Keys

Temporary Encryption Key

Main Processor

Storage

metadata

File

File I/O

DMA Path Crypto-Chip

Device Key

AES 256 Crypto-Engine

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
why passcode strength matters

on-device guessing attack

- 80 ms/guess
  - 6 alphanumeric — 5.5 years
  - 6 numeric — 22 hours
  - 4 numeric — 14 minutes
- requires exploitable bug in the boot-chain
  - LimeRa1n for iPhone 3GS, 4
  - Blackra1n, October 2009
  - Limera1n/greenpois0n, October 2010
  - exploit by iH8sn0w, February 2014
what Apple says about Touch ID

• “Touch ID makes using a longer, more complex passcodes far more practical because users won’t have to enter it as frequently”.

• “The stronger the user passcode is, the stronger the encryption key becomes. Touch ID can be used to enhance this equation by enabling the user to establish a much stronger passcode than would otherwise be practical. This increases the effective amount of entropy protecting the encryption keys used for Data Protection without adversely affecting the user experience of unlocking an iOS device multiple times throughout the day”.

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
Touch ID has had no significant impact on iPhone passcodes
$H_2^{null}$ — Availability of Touch ID has no effect on the ratio of users who lock their iPhones.

<table>
<thead>
<tr>
<th>Method</th>
<th>Non-Touch ID users (n=201)</th>
<th>Touch ID users (n=173)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN</td>
<td>88%</td>
<td>96%</td>
</tr>
<tr>
<td>Password</td>
<td>3%</td>
<td>4%</td>
</tr>
<tr>
<td>PIN</td>
<td>88%</td>
<td>96%</td>
</tr>
<tr>
<td>Password</td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td>PIN</td>
<td>88%</td>
<td>96%</td>
</tr>
<tr>
<td>Password</td>
<td>4%</td>
<td>4%</td>
</tr>
</tbody>
</table>

MTurk

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
$H_{1}^{\text{null}}$ — Use of Touch ID has no effect on the entropy of passcodes used for iPhone locking.
passcode info collected

Enter a structure of your iPhone passcode. That is, substitute
• each digit with D
• lowercase with L
• uppercase with U
• special character with S.
For example structure for passcode A1b%B is UDLSU.

PIN

DDDD
D L U S
Delete
RESET ALL

password

DDLUS
D L U S
Delete
RESET ALL

Touch ID study
Laboratory for Education and Research in Secure Systems Engineering
(lersse.ece.ubc.ca)
Passcodes are weak

<table>
<thead>
<tr>
<th></th>
<th>In-person (n=90)</th>
<th>MTurk (n=374)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Zero-order entropy</td>
<td>Time to crack</td>
</tr>
<tr>
<td>Non-Touch ID</td>
<td>15.6</td>
<td>1h10m</td>
</tr>
<tr>
<td>Touch ID</td>
<td>15.9</td>
<td>1h20m</td>
</tr>
</tbody>
</table>

Touch ID study
most use 4-digit PINs

- **in-person** (n=90):
  - PIN: 73%
  - Password: 22%
  - None: 4%

- **MTurk** (n=374):
  - PIN: 92%
  - Password: 3%
  - None: 5%
reasons for using PIN (not pwd)

- Easier to share
- Other
- Don't have anything to protect
- I reuse it on other devices
- Don't care about security
- Used PIN in previous device
- PIN is enough
- Touch ID is enough
- Easy to remember
- Didn't know about password
- PIN is faster

proportion of participants

<table>
<thead>
<tr>
<th>Reason</th>
<th>non-Touch ID (n =177)</th>
<th>Touch ID (n =166)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easier to share</td>
<td>0%</td>
<td>10%</td>
</tr>
<tr>
<td>Other</td>
<td>10%</td>
<td>20%</td>
</tr>
<tr>
<td>Don't have anything to protect</td>
<td>20%</td>
<td>30%</td>
</tr>
<tr>
<td>I reuse it on other devices</td>
<td>30%</td>
<td>40%</td>
</tr>
<tr>
<td>Don't care about security</td>
<td>40%</td>
<td>50%</td>
</tr>
<tr>
<td>Used PIN in previous device</td>
<td>50%</td>
<td>60%</td>
</tr>
<tr>
<td>PIN is enough</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Touch ID is enough</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Easy to remember</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Didn't know about password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIN is faster</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Touch ID study

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
reasons for using PIN (not pwd)

- Easier to share
- Other
- Don't have anything to protect
- I reuse it on other devices
- Don't care about security
- Used PIN in previous device
- PIN is enough
- Touch ID is enough
- Easy to remember
- Didn't know about password
- PIN is faster

Touch ID study
Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
PINs are easier to share

- PINs are easier to share
- Easier to share
- Other
- Don't have anything to protect
- I reuse it on other devices
- Don't care about security
- Used PIN in previous device
- PIN is enough
- Touch ID is enough
- Easy to remember
- Didn't know about password
- PIN is faster

<table>
<thead>
<tr>
<th>Easier to share</th>
<th>Touch ID (n = 166)</th>
<th>non-Touch ID (n = 177)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>50%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>60%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Touch ID study

Laboratory for Education and Research in Secure Systems Engineering
who users share PIN with?

- Co-workers: 1%
- Others: 3%
- Friends: 11%
- Family: 26%
- Partners: 30%
- No one: 40%

Proportion of participants (N = 356)
more on phone sharing

[Matthews, Google, CHI ’16]

• share mostly with significant others and children

• sharing types
  • borrowing (device but not accounts) for convenience.
  • set up/maintenance (access remaining) to help
  • broadcasting to view content together
  • accidental account sharing

• trust and convenience dimensions

confusion about passcode vs. Touch ID

Touch ID itself increases security

“I guess Touch ID will protect my phone. They cannot open my phone without my finger. So it will definitely help.” [P1]
why Touch ID?
reasons for using Touch ID

- Reliability: 29%
- Novelty: 32%
- Fun to use: 34%
- Privacy: 39%
- Cool to use: 46%
- Efficiency: 47%
- Security: 58%
- Time/speed: 70%
- Ease of use: 76%
- Convenience: 90%

proportion of participants (n = 173)

Laboratory for Education and Research in Secure Systems Engineering
(lerse.ece.ubc.ca)
main findings (1/2)

• Users’ concerns about strangers and social insiders are comparable

• 1 in 5 Americans engaged in smartphone snooping in past 12 months

• Overwhelming majority of iPhone (but not Android) users lock their devices

• Smartphone locking is likely linked to its value (hardware, data, apps)

• Most sessions are short and involve 1-3 apps

• Usability cost of unlocking methods is crucial
main findings (2/2)

• Touch ID is for convenience
  • no measurable impact of TouchID on passcodes
  • passcodes are weak: 1-2 hours to guess

• PINs vs. passwords
  • usability (e.g., sharing) considerations
  • lack of awareness: set up, salespeople

• unlocking methods need to support device sharing
design recommendations: unlocking secrets

- stronger than PINs and yet just as memorable
- comparable speed and accuracy

reasons for PIN

- Easier to share
- Don't have anything to protect
- I reuse it on other devices
- Used PIN in previous device
- PIN is enough
- Touch ID is enough
- Easy to remember
- Didn't know about password
- PIN is faster

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
design recommendations
facilitate phone sharing

facilitate contacting owners of lost phones

proportion of participants (N = 356)

Co-workers 11%
Others 3%
Friends 11%
Family 26%
Partners 30%
No one 40%
design recommendations:

better mental model of TouchID+passcode

user

- passcode (e.g., “3985”)
- fingerprint
- Touch ID

Secure Enclave

Class Keys

Crypto-Chip

Device Key

Crypto-Engine

Temporary Encryption Key
design recommendations

better feedback on passcode strength
acknowledgements

LERSSE team

• Ildar Muslukhov
• Ivan Cherapau
• Ahmed Mahfouz
• Yazan Boshmaf
• Nalin Asanka

Collaborators

• University of Lisbon
  • Diogo Marques
  • Tiago Guerreiro
  • Luís Carriço
• Nokia Research
  • Cynthia Kuo
  • Jonathan Lester
selected publications


