Lecture 5

USABILITY OF PLATFORM SECURITY

You will be learning:

- Can usability of app authorization be improved?
- What other problems require balancing usability and security?

Usability of security?

Lack of security usability

- Harms security, eventually
- Lowers attractiveness of the device/service, eventually
- Costs money!

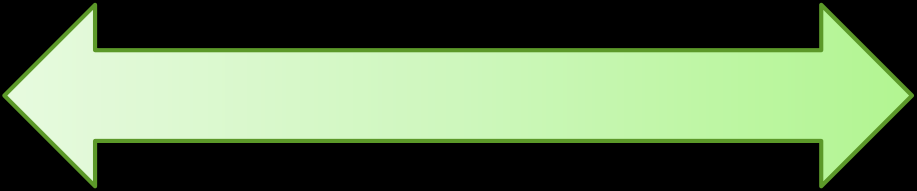
Outline

- Challenges in permission granting
- Why is usable mobile security different
- Examples of usable mobile security problem instances

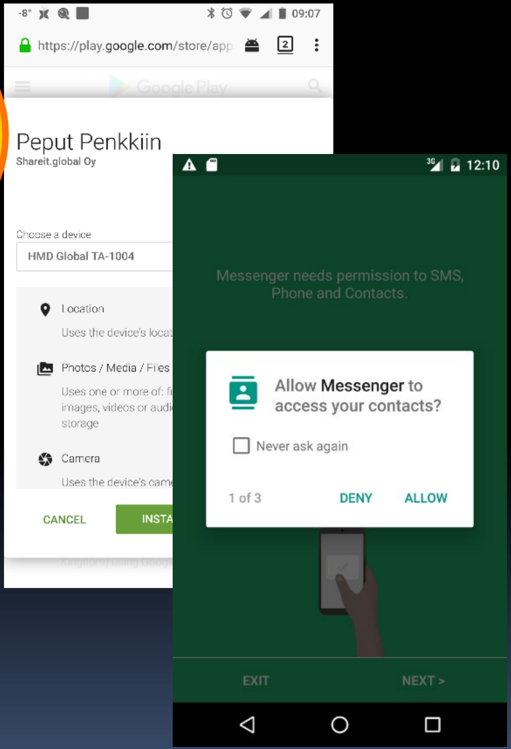
Challenges in permission granting

Granting permissions to apps

Punt to user
(mostly)



Decide centrally
(mostly)



-8° 09:07

https://play.google.com/store/app

Peput Penkkiin
Shareit.global Oy

Choose a device
HMD Global TA-1004

Location
Uses the device's locat

Photos / Media / Files
Uses one or more of: fi
images, videos or audi
storage

Camera
Uses the device's cam

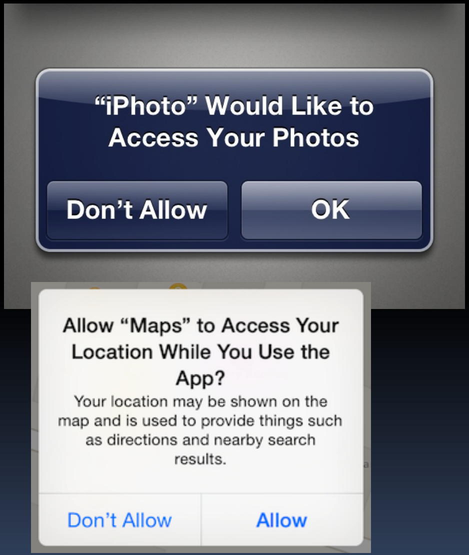
12:10

Messenger needs permission to SMS, Phone and Contacts.

Allow **Messenger** to access your contacts?

□ Never ask again

1 of 3



“iPhoto” Would Like to Access Your Photos

Allow “Maps” to Access Your Location While You Use the App?

Your location may be shown on the map and is used to provide things such as directions and nearby search results.

Android

iOS, Windows Phone,
(late) Symbian

Granting permissions to apps

Punt to user

- Personalized
- …
- Hard-to-use
- Ill-informed decisions
- Habituation
- …

Decide centrally

- Ease-of-use
- …
- Not personalized
- Potential liability
- …

Improving usability

1. Provide more context in prompts

   Annotations with useful information

2. **Time** of granting: Install time vs. Run time
3. Implicit granting via **trusted UIs**
4. **Automatic granting** + auditability

Porter Felt et al, HotSec '12

1. Annotations

- Users don’t have enough signals to make informed decisions

Chia et al, “Is this app safe?: a large scale study on application permissions and risk signals.”, WWW 2012

- Analyze app; show results to user
- Social navigation
  - Experts
  - Crowdsourcing

Annotations from analysis

- Problem: privacy risk depends on context
  - E.g., “Location”: ok for maps, not for flashlight
  - Privacy at risk if user’s expectations not met

Lin et al, “Expectation and Purpose: Understanding Users’ Mental Models of Mobile App Privacy through Crowdsourcing“ , UbiComp 2012

Annotations from analysis

- Idea:
  - *Training*: Tell users what app does & ask if it matches their expectations
  - *Use*: Annotate permission prompt with results

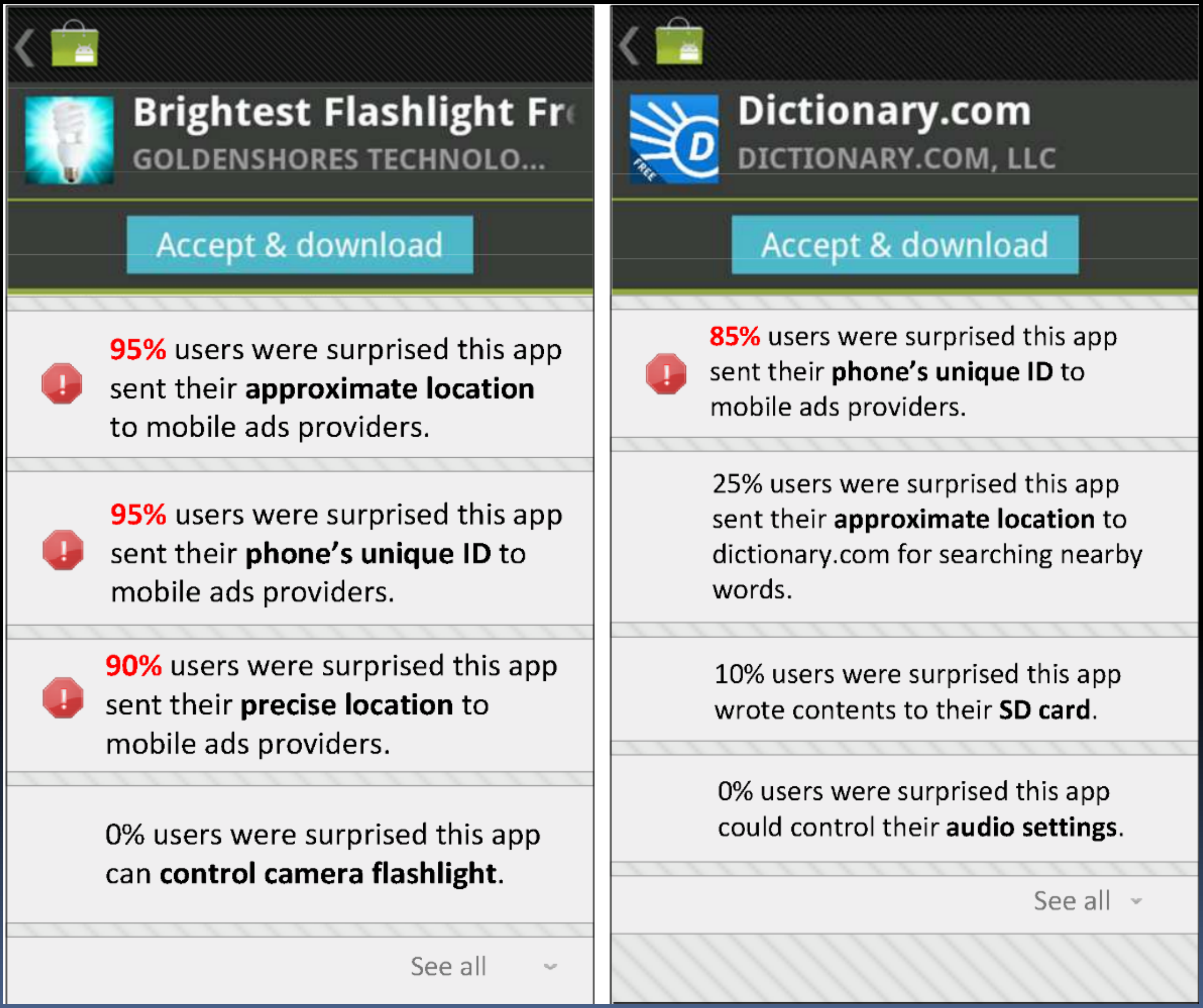
Training: Get annotation info

- Step #1: Get permissions from manifests
- Step #2: Learn how data is used
  - Analyse using TaintDroid (tracks where data goes)
  - Categorize uses: core functionality / secondary (e.g. tagging, sharing) / targeted ads

Training: Get annotation info

- Step #3: Check user reactions
  - Do you expect this app to use …
  - Are you uncomfortable with it using X to support Y
  - Participants recruited on Amazon Mechanical Turk

Use: Show cues to users



Brightest Flashlight Fr
GOLDENSHORES TECHNOLO...

95% users were surprised this app sent their **approximate location** to mobile ads providers.

95% users were surprised this app sent their **phone's unique ID** to mobile ads providers.

90% users were surprised this app sent their **precise location** to mobile ads providers.

0% users were surprised this app can **control camera flashlight**.

Dictionary.com
DICTIONARY.COM, LLC

85% users were surprised this app sent their **phone's unique ID** to mobile ads providers.

25% users were surprised this app sent their **approximate location** to dictionary.com for searching nearby words.

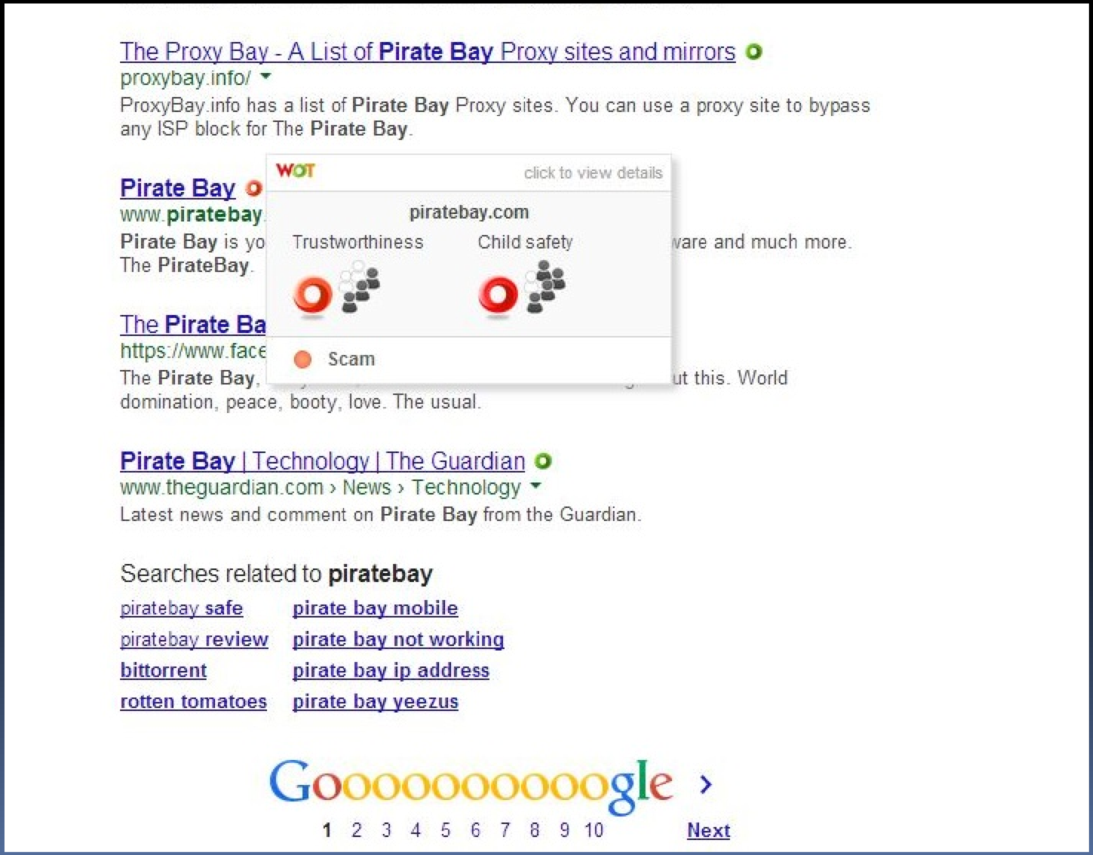
10% users were surprised this app wrote contents to their **SD card**.

0% users were surprised this app could control their **audio settings**.

Example permission UI from Lin et al, 2012

Crowdsourcing ratings

- Another example: Web of Trust



The Proxy Bay - A List of Pirate Bay Proxy sites and mirrors
proxybay.info/
ProxyBay.info has a list of Pirate Bay Proxy sites. You can use a proxy site to bypass any ISP block for The Pirate Bay.

Pirate Bay
www.piratebay.
Pirate Bay is yo … ware and much more.
The PirateBay.

The Pirate Ba
https://www.face
The Pirate Bay, … ut this. World domination, peace, booty, love. The usual.

WOT click to view details
piratebay.com
Trustworthiness
Child safety
Scam

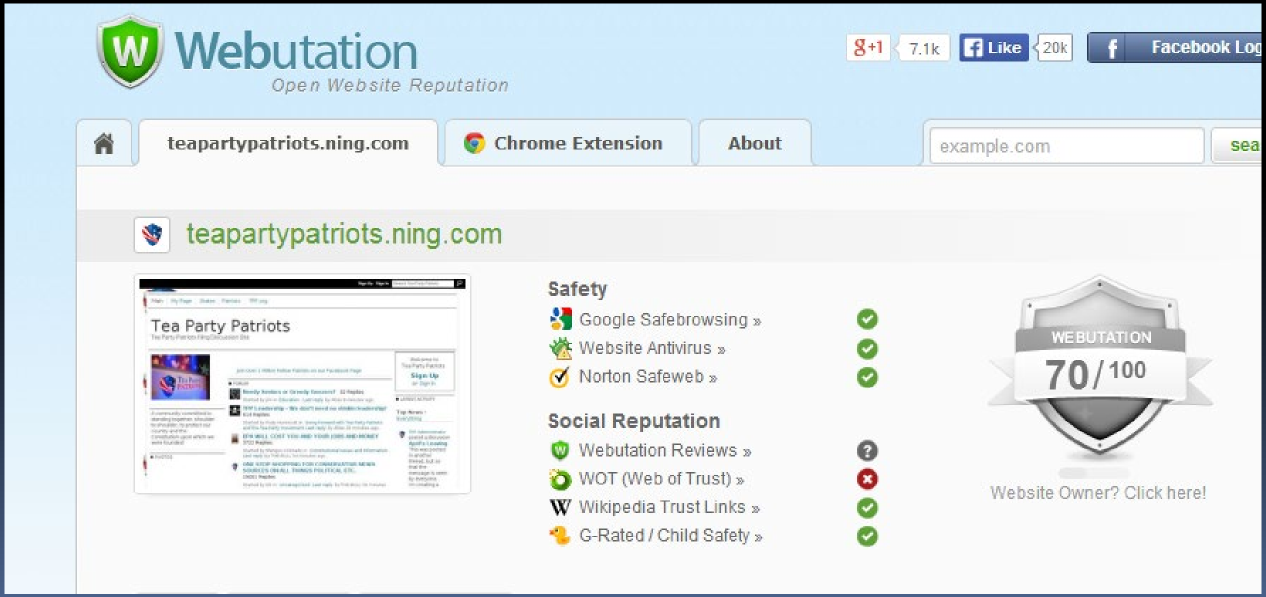
Pirate Bay | Technology | The Guardian
www.theguardian.com › News › Technology
Latest news and comment on Pirate Bay from the Guardian.

Searches related to piratebay

piratebay safe	pirate bay mobile
piratebay review	pirate bay not working
bittorrent	pirate bay ip address
rotten tomatoes	pirate bay yeezus

Concerns in centralized rating

- Who decides if a website/app/… is “bad”?
- How to incentivize participation?



Webutation
Open Website Reputation

g+1 7.1k · Like 20k · Facebook Log

teapartypatriots.ning.com · Chrome Extension · About

example.com · sea

teapartypatriots.ning.com

Tea Party Patriots

Safety

- Google Safebrowsing » ✓
- Website Antivirus » ✓
- Norton Safeweb » ✓

Social Reputation

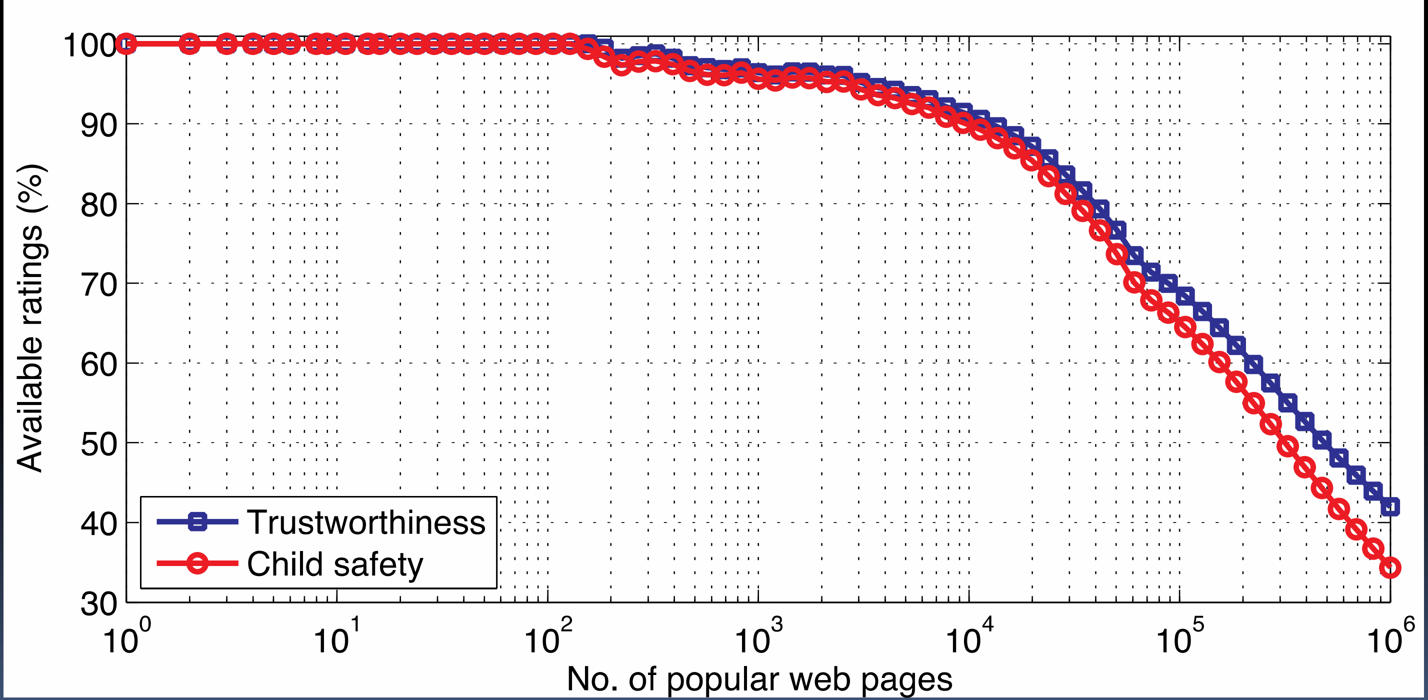
- Webutation Reviews » ?
- WOT (Web of Trust) » ✗
- Wikipedia Trust Links » ✓
- G-Rated / Child Safety » ✓

WEBUTATION 70/100

Website Owner? Click here!

Concerns in ratings by people

- How to improve coverage?



Web of Trust (https://www.mywot.com/) ratings for popular web pages

Addressing concerns

- Groupsourcing?
  - Feedback from social circles, rather than the crowd as whole

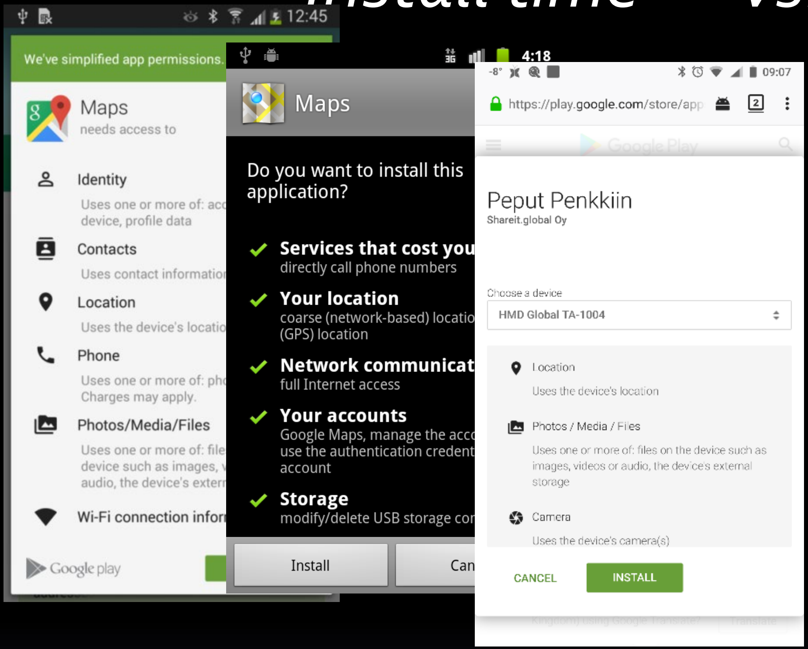
See: "Groupsourcing: nudging users away from unsafe content", NordiCHI 2014

- Machine learning?
  - Predict likely rating using model trained on sample ratings

See: "LookAhead: Augmenting Crowdsourced Website Reputation Systems With Predictive Modeling", TRUST 2015

2. Time of granting

Install time vs. Run time



12:45

We've simplified app permissions.

Maps
needs access to

Identity
Uses one or more of: acc
device, profile data

Contacts
Uses contact informatio

Location
Uses the device's locatio

Phone
Uses one or more of: ph
Charges may apply.

Photos/Media/Files
Uses one or more of: file
device such as images, v
audio, the device's extern

Wi-Fi connection infor

Google play

4:18

Maps

Do you want to install this application?

✓ **Services that cost you**
directly call phone numbers

✓ **Your location**
coarse (network-based) locatio
(GPS) location

✓ **Network communicat**
full Internet access

✓ **Your accounts**
Google Maps, manage the acc
use the authentication credent
account

✓ **Storage**
modify/delete USB storage co

Install | Can

09:07

https://play.google.com/store/app

Google Play

Peput Penkkiin
Shareit.global Oy

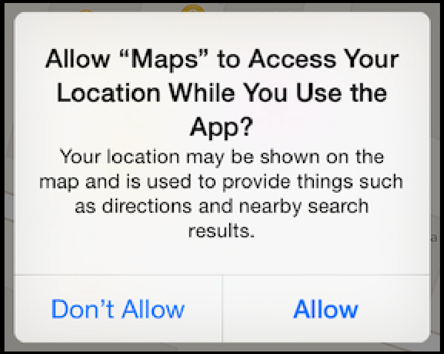
Choose a device
HMD Global TA-1004

Location
Uses the device's location

Photos / Media / Files
Uses one or more of: files on the device such as images, videos or audio, the device's external storage

Camera
Uses the device's camera(s)

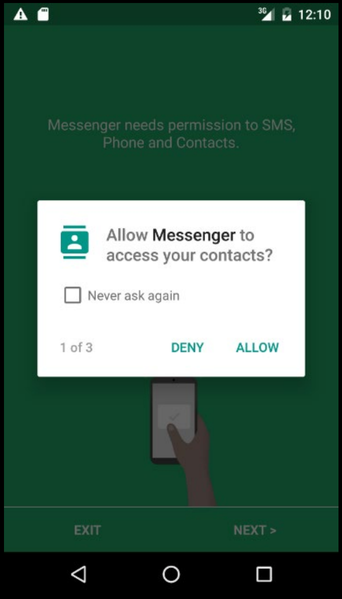
CANCEL | INSTALL



Allow “Maps” to Access Your Location While You Use the App?

Your location may be shown on the map and is used to provide things such as directions and nearby search results.

Don’t Allow | Allow



12:10

Messenger needs permission to SMS, Phone and Contacts.

Allow **Messenger** to access your contacts?

□ Never ask again

1 of 3 DENY ALLOW

EXIT NEXT >

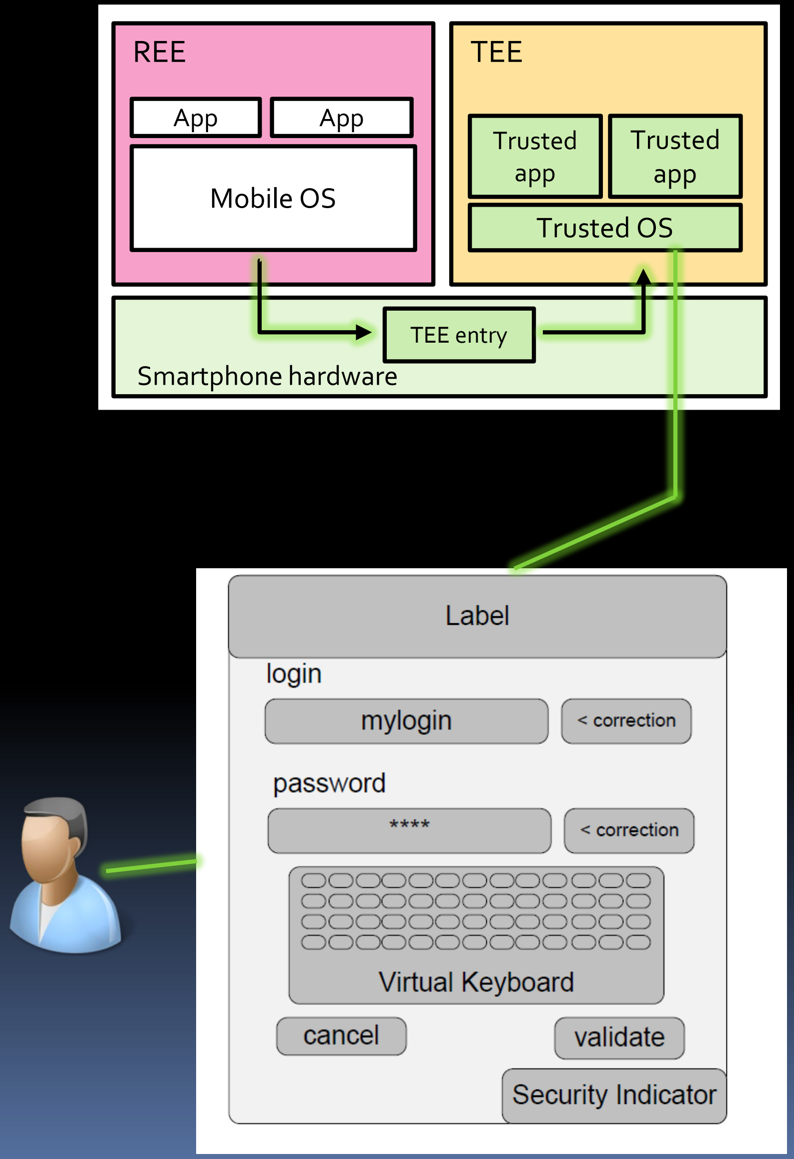
- more time to think
- less disruptive
- no contextual info.

- contextual info.
- more fine-grained
- intrusive

3. Trusted UI

- Trusted path to user
  - (E.g. PIN/login input screen)
  - Trusted widgets
- Not forgeable or obscurable by REE apps
  - Hardware/OS support needed
- Other application areas:
  - User authentication
  - Transaction confirmation
  - Provisioning

Example: Dedicated Trusted UI (Global Platform)

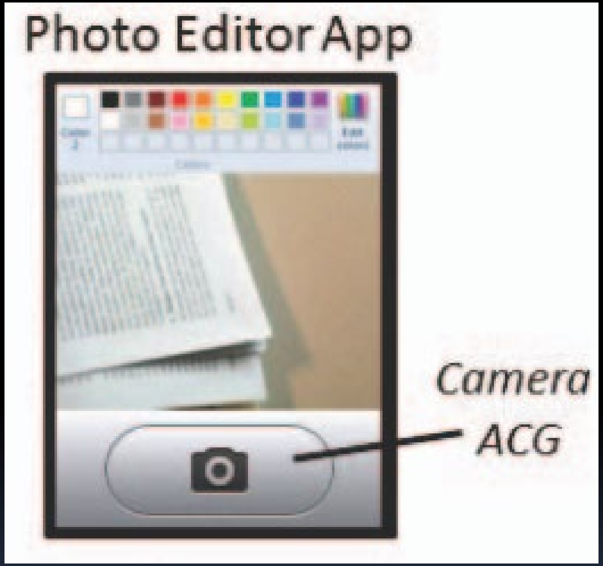


Trusted permission widgets

- Goal: Permission requests should be
  - In context – informed decisions
  - Least-privilege – not ”take photos at any time”
  - Supporting user task – not interrupting it

Trusted permission widgets

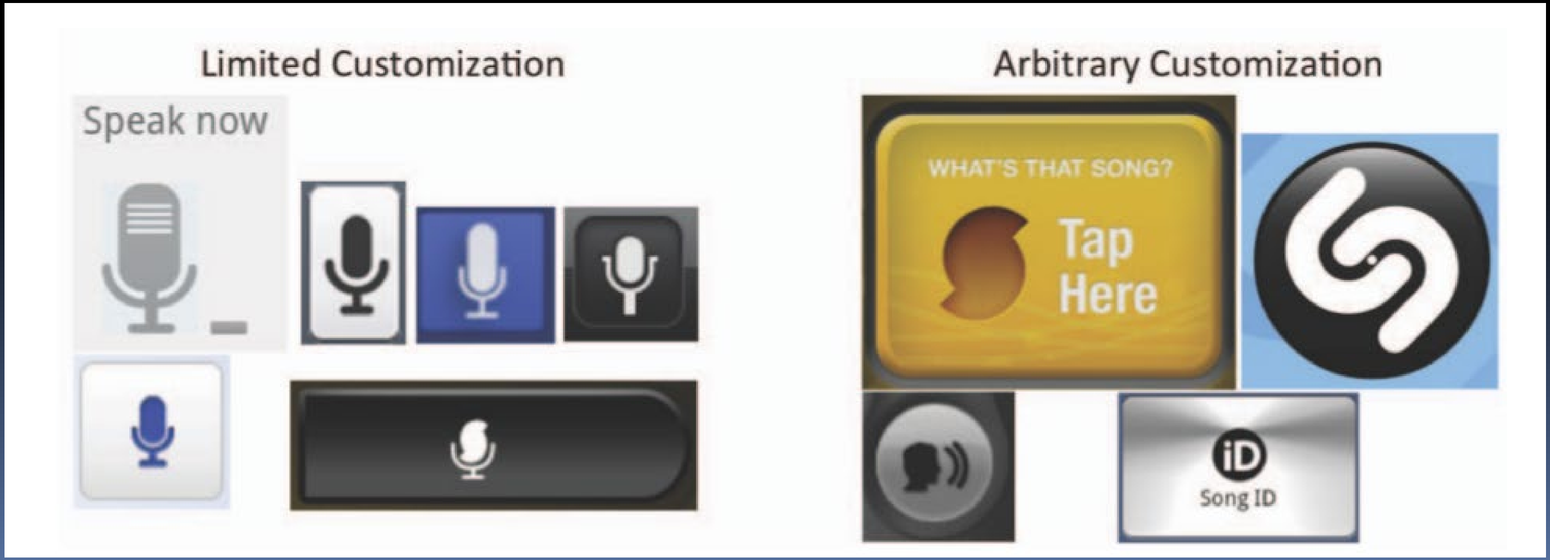
- Idea: trusted widget for action [1] + permission
  - "Camera trigger"
  - "Record button"
  - *access control gadget*



[1] Roesner et al, "User-driven access control: Rethinking permission granting in modern operating systems", IEEE S&P 2012

Permission widgets: How?

- Grant: once, session, scheduled, permanent…
- Convey semantics clearly to user
- Identifiability vs. customizability?



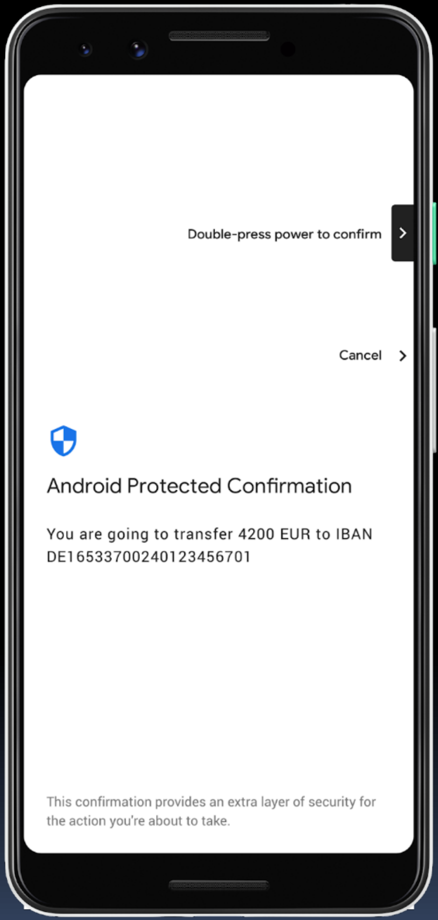
[1]

How to realize permission widgets?

- How to make them unforgeable and unobscurable?
- What can be done without OS support?

Ringer et al, "AUDACIOUS: User-Driven Access Control with Unmodified Operating Systems", ACM CCS 2016

Trusted Path in practice



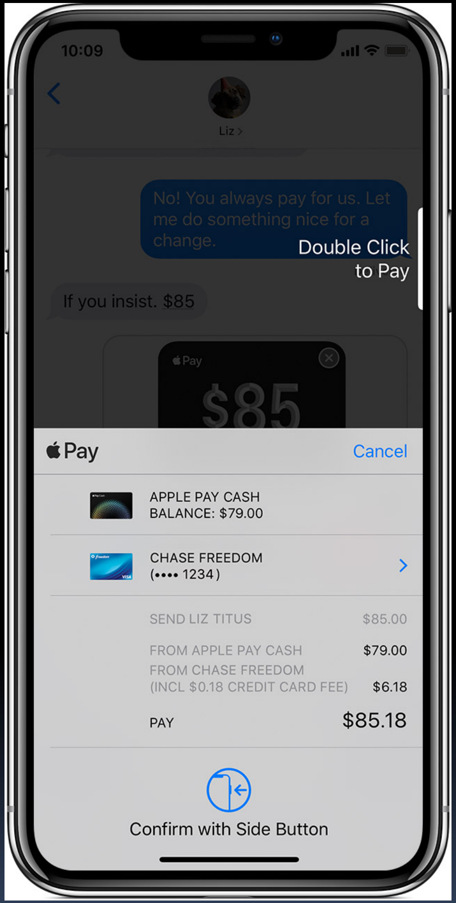
Double-press power to confirm

Cancel

Android Protected Confirmation

You are going to transfer 4200 EUR to IBAN DE16533700240123456701

This confirmation provides an extra layer of security for the action you're about to take.



10:09

Liz

No! You always pay for us. Let me do something nice for a change.

Double Click to Pay

If you insist. $85

Pay $85

Pay Cancel

APPLE PAY CASH
BALANCE: $79.00

CHASE FREEDOM
(•••• 1234)

SEND LIZ TITUS	$85.00
FROM APPLE PAY CASH	$79.00
FROM CHASE FREEDOM (INCL $0.18 CREDIT CARD FEE)	$6.18
PAY	$85.18

Confirm with Side Button

https://android-developers.googleblog.com/2018/10/android-protected-confirmation.html

https://support.apple.com/fi-fi/HT207875
https://www.apple.com/ca/business-docs/FaceID_Security_Guide.pdf

4. Automatic granting

Grant requested permissions

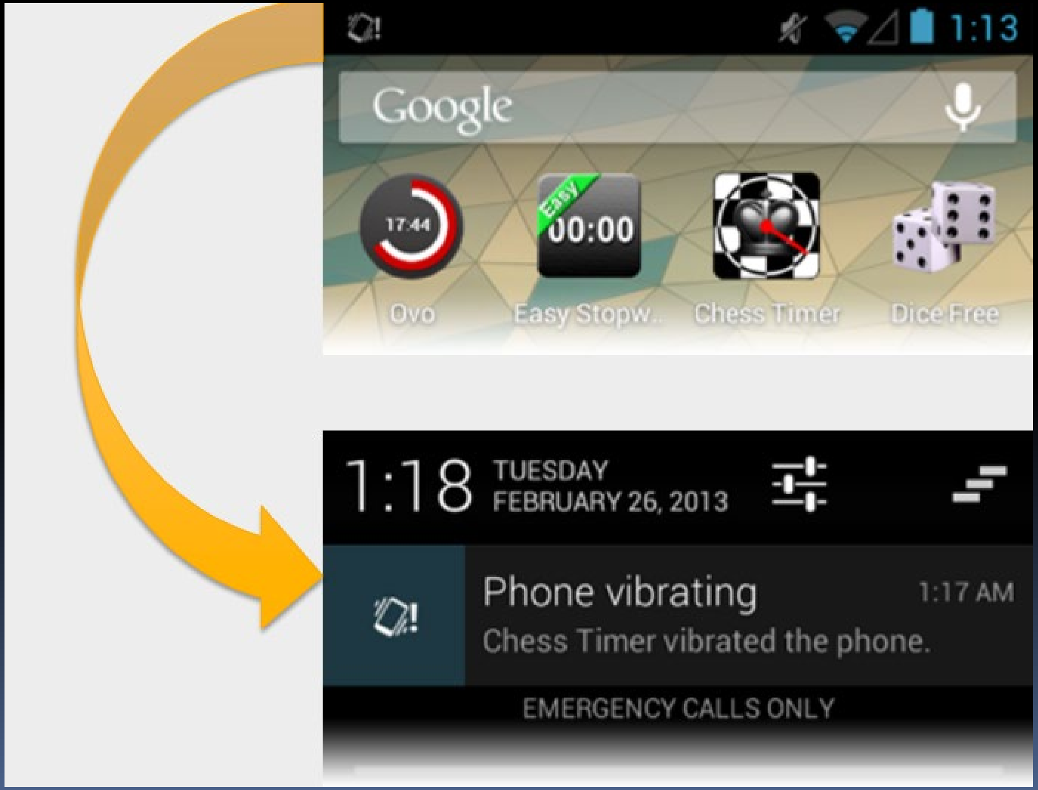
- … for low risk and reversible permissions
- … but allow for **auditability**
  - Letting user figure out if app abuses permission

Thompson et al, "When it's better to ask forgiveness than get permission: attribution mechanisms for smartphone resources", SOUPS 2013

Allowing for auditability

Show who was responsible for a change (e.g., notification)

e.g., notification shows which app is vibrating phone



Phone vibrating 1:17 AM

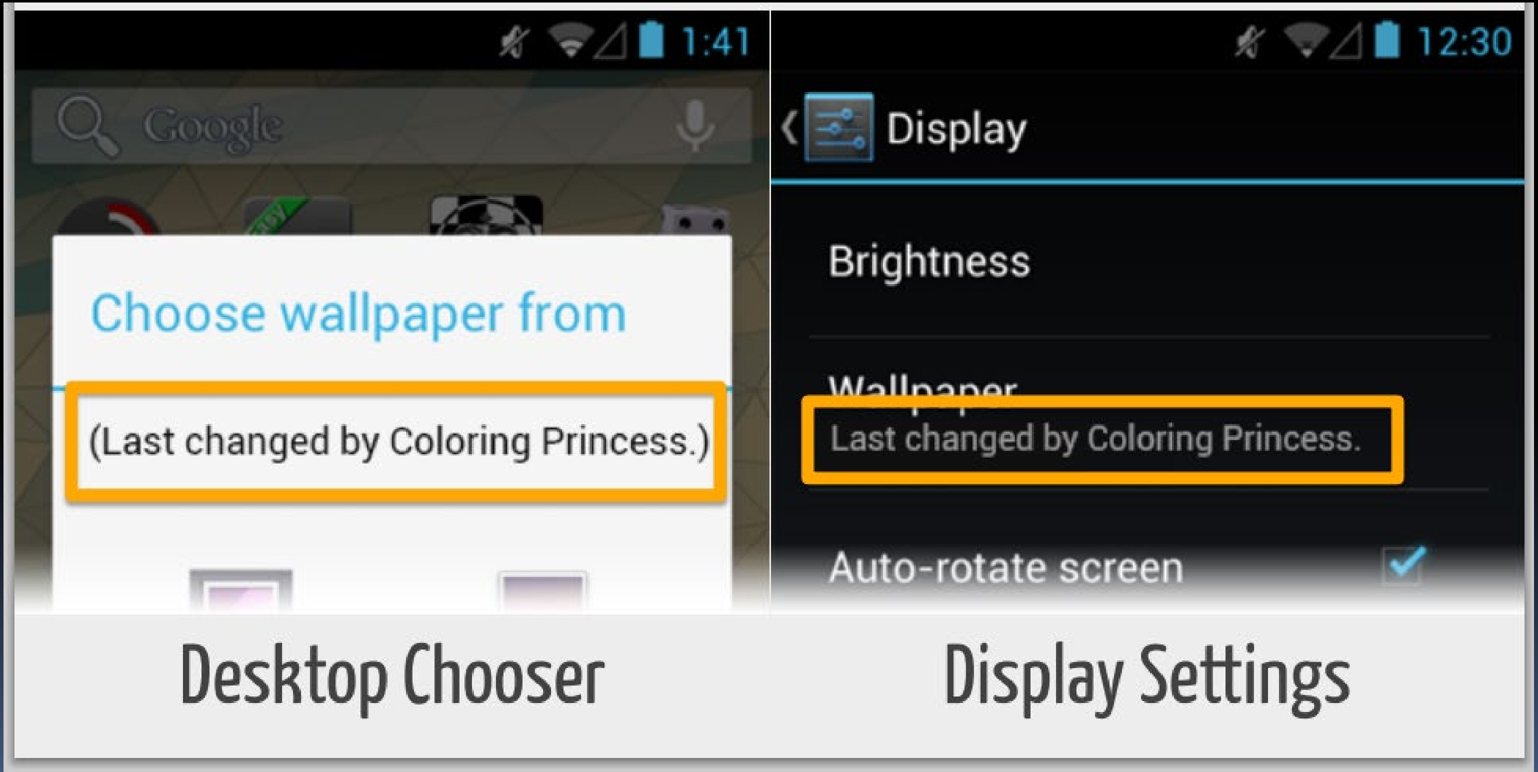
Chess Timer vibrated the phone.

EMERGENCY CALLS ONLY

Allowing for auditability

Show who was responsible for a change (e.g., notification)

e.g., notification shows which app changed wallpaper



(Last changed by Coloring Princess.)

Last changed by Coloring Princess.

Desktop Chooser

Display Settings

Is attribution effective?

- Will users notice attribution indicators?
- Will they identify the apps responsible?

- Controlled laboratory study

Testing effectiveness

- How to test?
  - Pilot study, questionnaires, …
- Experiment design
  - Avoid influence of other factors
    - E.g., only one app with wallpaper permission
  - Control condition vs. experiment condition

Thompson et al, “When it’s better to ask forgiveness than get permission: attribution mechanisms for smartphone resources”, SOUPS 2013

Usability testing methods

- Expert evaluation: no test users
  - E.g. cognitive walkthrough
- Questionnaires
  - Standardized: SUS, SUMI, PSSUQ, UMUX
  - Can be used remotely (e.g. online surveys) or in lab settings

Usability testing methods

- Lab test: experimental test setting
  - Quantitative results
    - Questionnaires (multiple choice, e.g. Likert scale)
    - Behavioral (e.g. reaction times)

    Statistical tests: *comparing* the results of different groups
  - Qualitative results
    - Verbal: interviews, free-form questionnaires
    - Behavioral: detecting users' mistakes or misunderstandings

Testing security usability

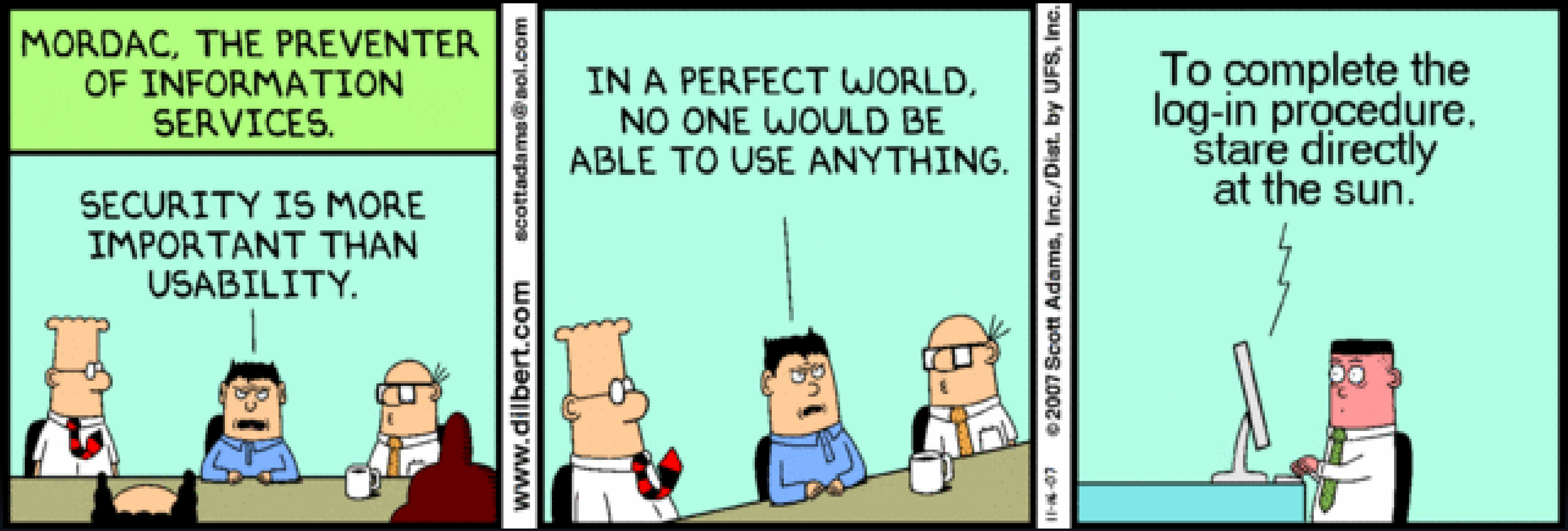
- Moral hazard
  - Taking risks because of lack of consequences
  - E.g., lending test devices to participants
- Priming and self-reporting
  - Saying/doing what is expected
  - Example priming: saying "we are testing whether people choose strong passwords"

Ecological invalidity: test vs real life mismatch

Exercise: self-reporting

You want to find out the rate of mobile malware payloads delivered via adult websites. For this you need to know what proportion of infected users visited adult websites. For privacy reasons, you cannot automatically collect data about websites visited by users. You are only allowed to ask them (i.e., “self-reporting”)

How will you formulate your question in order to get an accurate measure for fraction of users visiting adult websites?


MORDAC, THE PREVENTER OF INFORMATION SERVICES.
SECURITY IS MORE IMPORTANT THAN USABILITY.
scottadams@aol.com
www.dilbert.com
IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.
11-16-07
©2007 Scott Adams, Inc./Dist. by UFS, Inc.
To complete the log-in procedure, stare directly at the sun.

http://www.dilbert.com (11/16/2007)

Exercise: self-reporting

You want to find out the rate of mobile malware payloads delivered via adult websites. For this you need to know what proportion of infected users visited adult websites. For privacy reasons, you cannot automatically collect data about websites visited by users. You are only allowed to ask them (i.e., "self-reporting")

How will you formulate your question in order to get an accurate measure for fraction of users visiting adult websites?

Exercise: self-reporting

- How to extract true statistics from self-reported responses to sensitive questions?
- Hint 1: ask a more general question
- Hint 2: divide your sample into two groups; ask each group a *different* general question

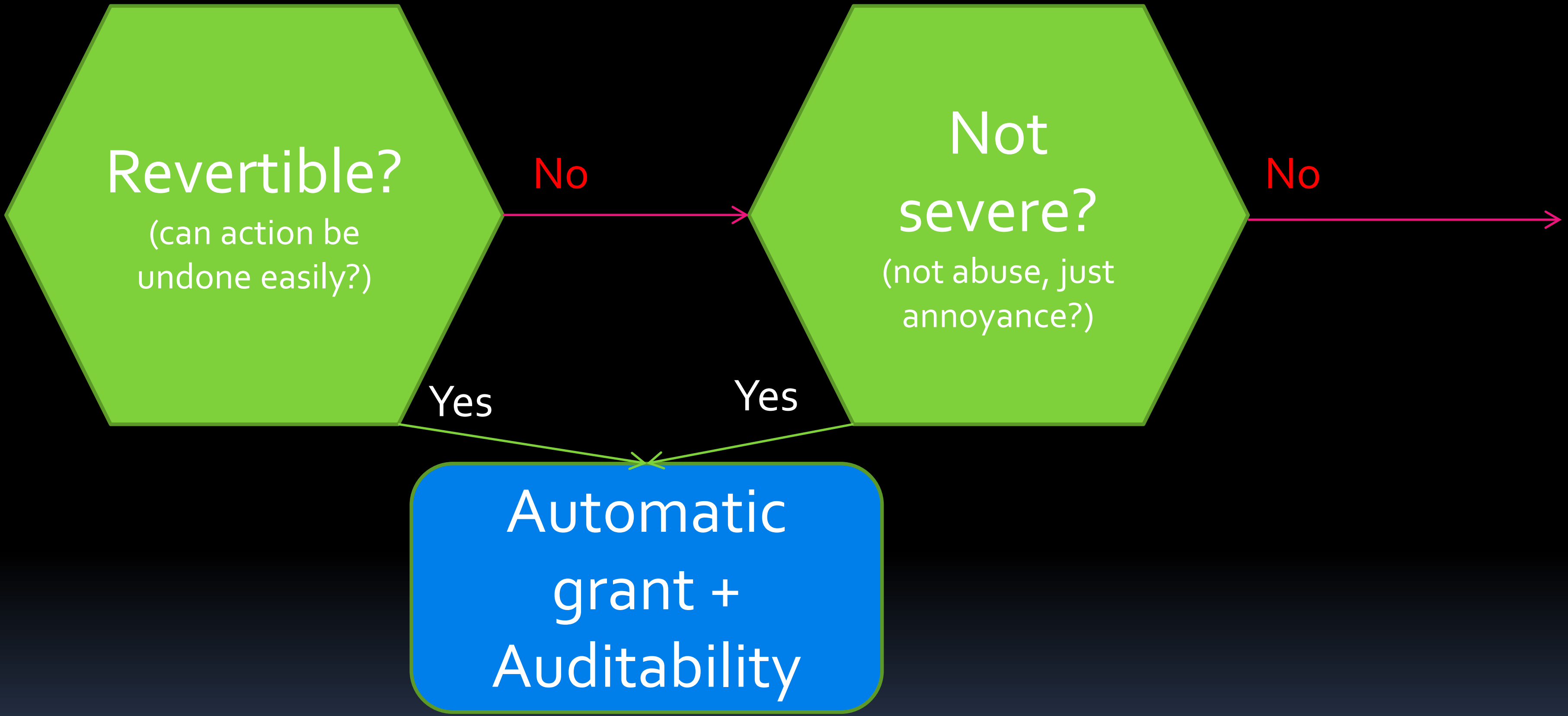
Improving usability

1. Provide more context in prompts

   Annotations with useful information

2. **Time** of granting: Install time vs. Run time
3. Implicit granting via **trusted UIs**
4. **Automatic granting** + auditability

Choosing granting mechanism (1/3)



Revertible?

(can action be undone easily?)

No

Not severe?

(not abuse, just annoyance?)

No

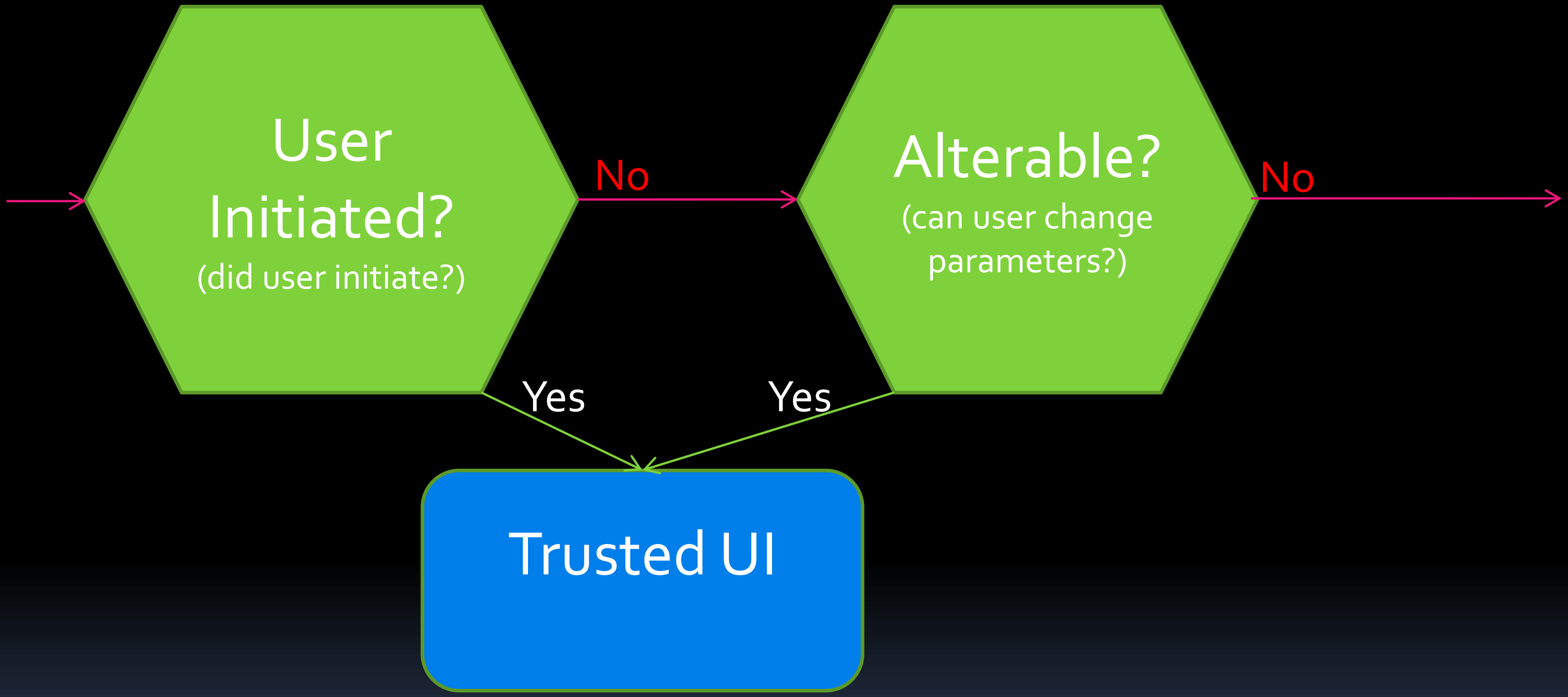
Yes

Yes

Automatic grant + Auditability

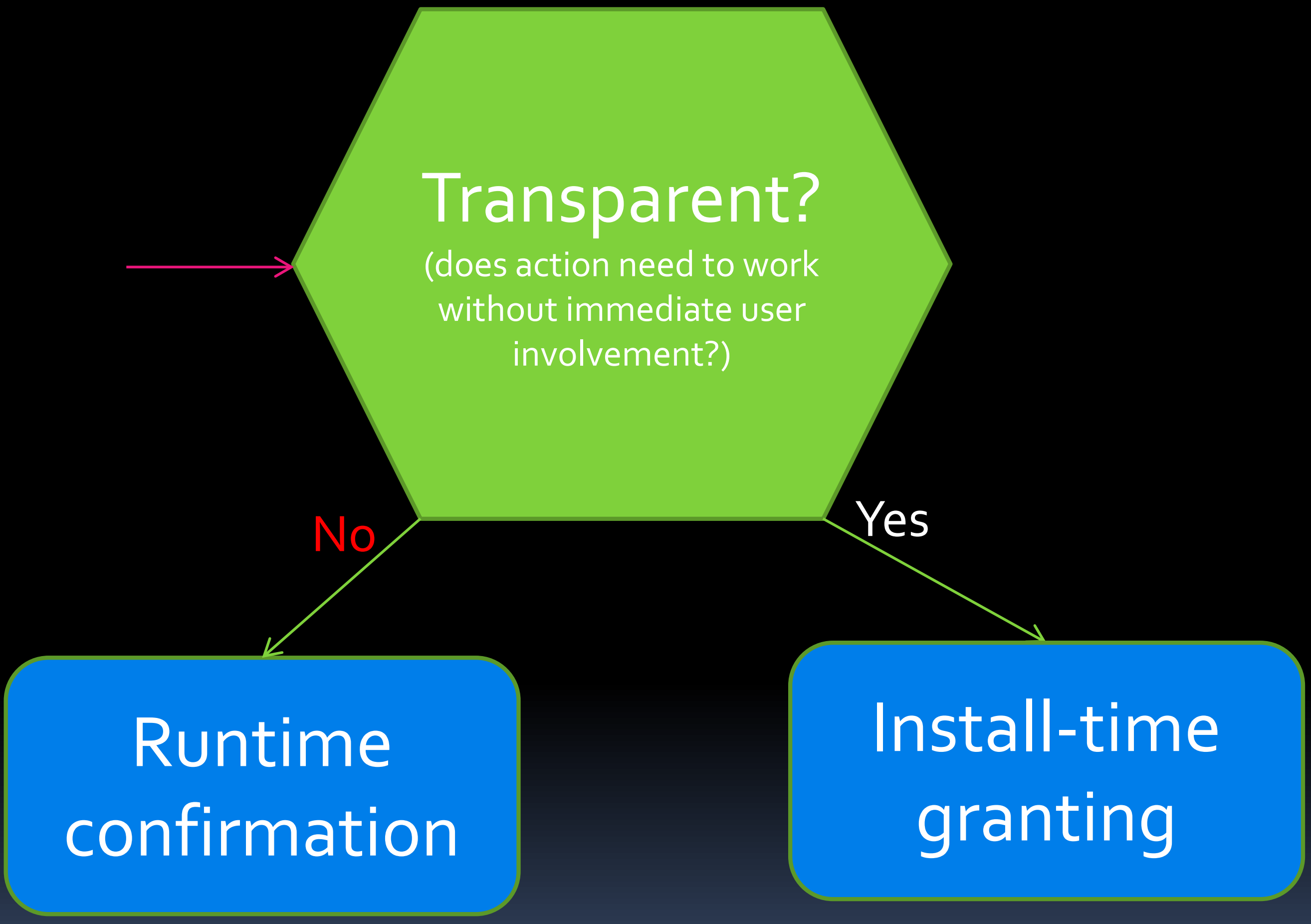
Adapted from Porter Felt et al, HotSec '12

Choosing granting mechanism (2/3)



Adapted from Porter Felt et al, HotSec '12

Choosing granting mechanism (3/3)



Transparent?

(does action need to work without immediate user involvement?)

No

Yes

Runtime confirmation

Install-time granting

Adapted from Porter Felt et al, HotSec '12

Why is usable mobile security different?

Your mobile phone: Not a smaller version of your PC

!=

Your mobile phone: Not a smaller version of your PC

Mobile phone applications have different requirements due to

1. Smaller physical screen size

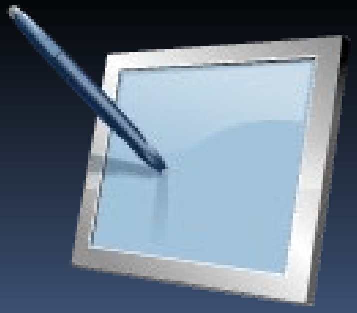
   → Less room for security indicators, notifications etc.

Your mobile phone: Not a smaller version of your PC

Mobile phone applications have different requirements due to

1. Smaller physical screen size
2. Different input mechanisms

Directional pad + keyboard



Touch screen

Keyboard + mouse + …

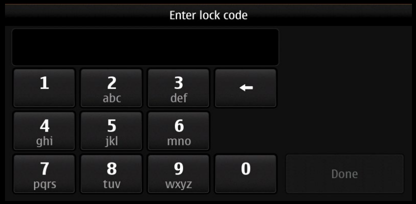
Your mobile phone: Not a smaller version of your PC

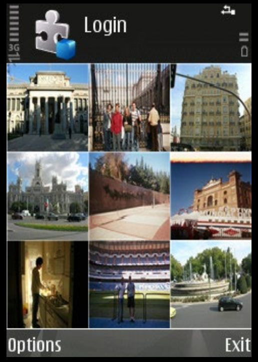
Mobile phone applications have different requirements due to

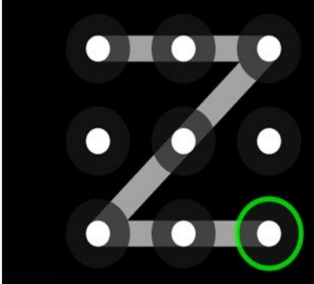
1. Smaller physical screen size
2. Different input mechanisms
3. Limited battery life
4. More prone to theft/loss
5. Slower and less reliable network connectivity
6. (Comparatively) limited computational power

Other usable security problems

Local user authentication







Dunphy et al, "Shoulder-surfing resistance of authentication based on image recognition", SOUPS 2010

Need alternatives that are:

- Faster
- More enjoyable
- Secure enough

Biometrics

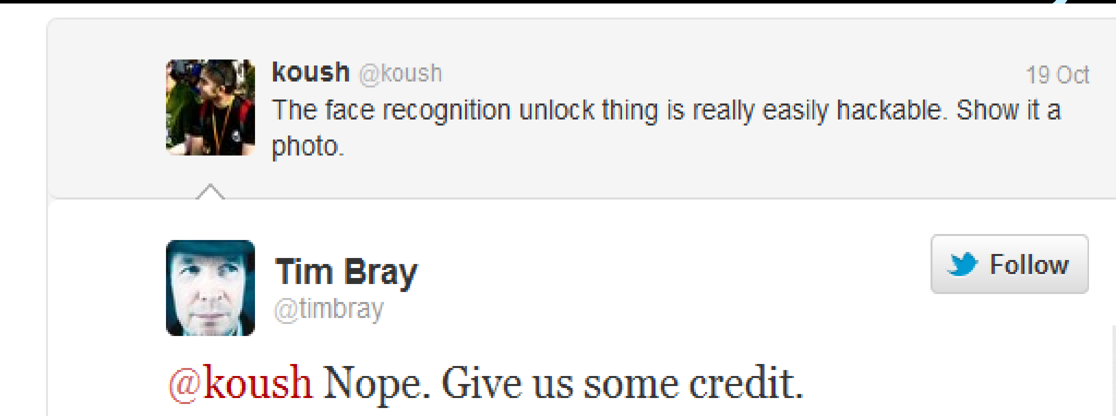
Wearables

?

Cost: users avoid using apps that mandate local authentication (work e-mail!)

Cost: weak PINs

Local user authentication: a cautionary tale

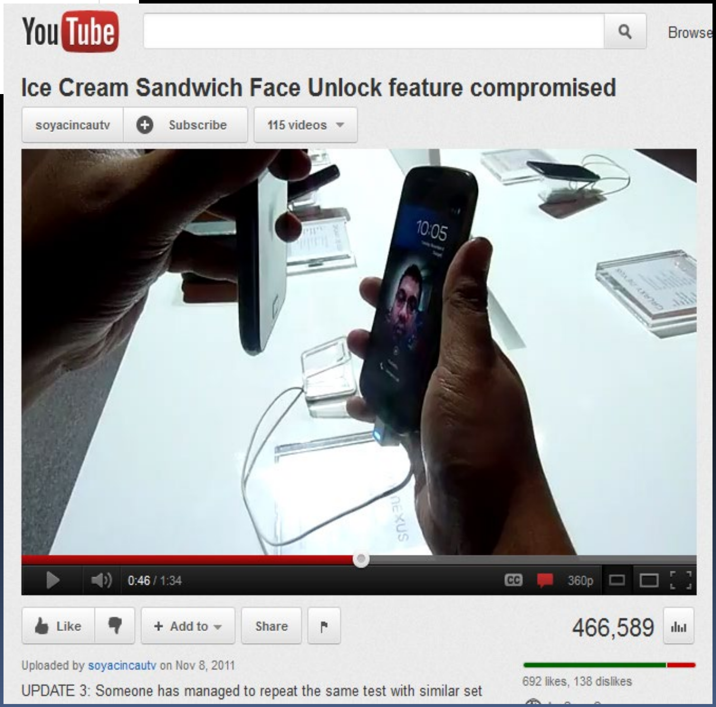


koush @koush 19 Oct

The face recognition unlock thing is really easily hackable. Show it a photo.

Tim Bray @timbray

@koush Nope. Give us some credit.



Ice Cream Sandwich Face Unlock feature compromised

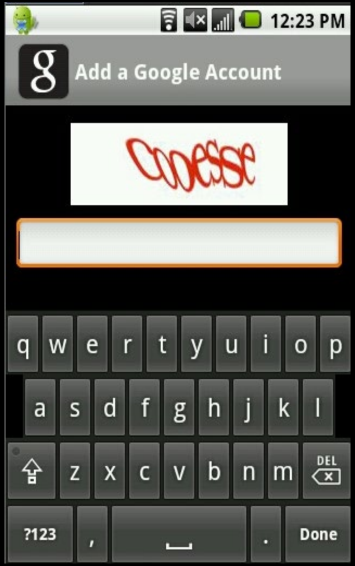
Uploaded by soyacincautv on Nov 8, 2011

692 likes, 138 dislikes

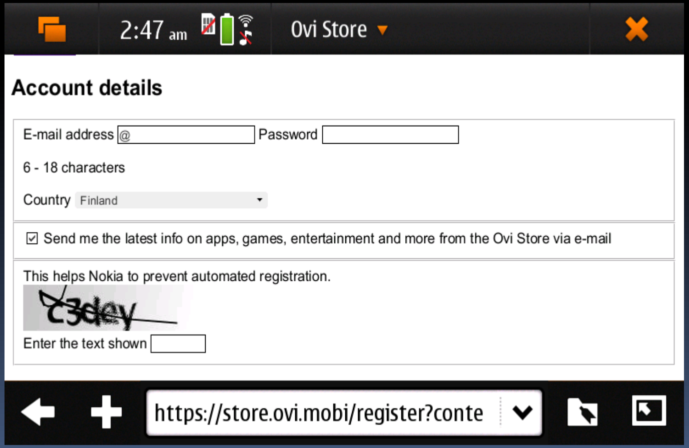
UPDATE 3: Someone has managed to repeat the same test with similar set

http://youtu.be/BwfYSR7HttA

CAPTCHA on mobile devices



Cost:
Estimated 15% drop-off rate when encountering a CAPTCHA on mobile devices



Account details

E-mail address @ Password

6 - 18 characters

Country Finland

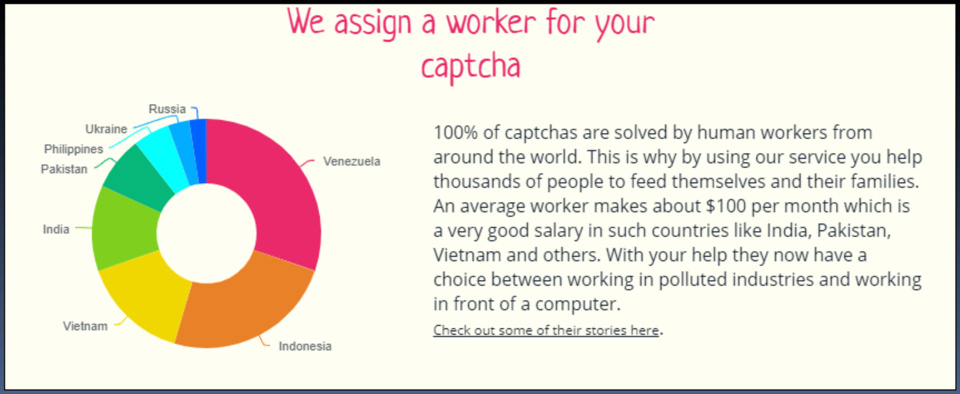
☑ Send me the latest info on apps, games, entertainment and more from the Ovi Store via e-mail

This helps Nokia to prevent automated registration.

Enter the text shown

https://store.ovi.mobi/register?conte

https://anti-captcha.com/



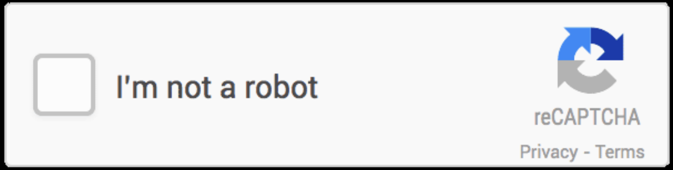
We assign a worker for your captcha

100% of captchas are solved by human workers from around the world. This is why by using our service you help thousands of people to feed themselves and their families. An average worker makes about $100 per month which is a very good salary in such countries like India, Pakistan, Vietnam and others. With your help they now have a choice between working in polluted industries and working in front of a computer.

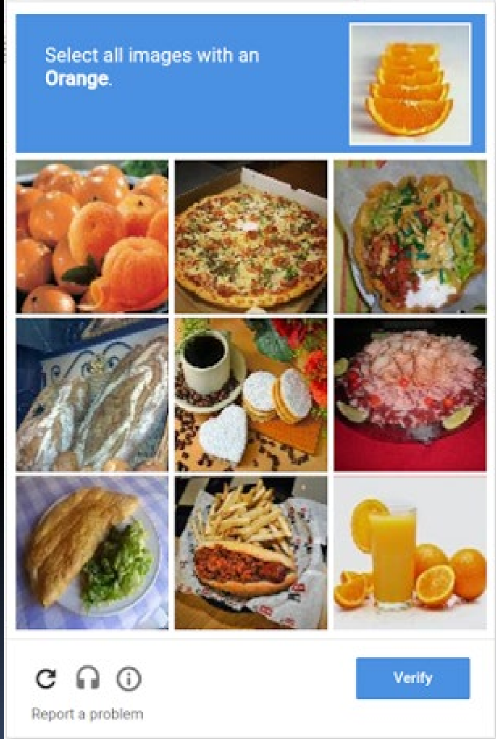
Check out some of their stories here.

CAPTCHA Alternatives

- The problem is real
- Avoid CAPTCHA?
  - reCAPTCHA
  - Device authentication



□ I'm not a robot



Select all images with an **Orange**.

https://support.google.com/recaptcha/?hl=en

Other problem instances

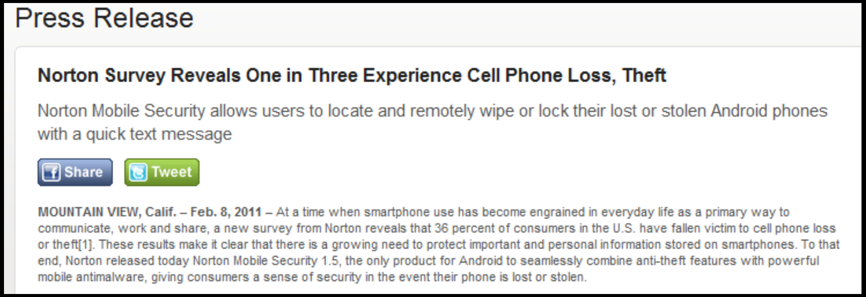
- (Permission granting to apps)
- Local user authentication
- CAPTCHA
- Secure First Connect
- Context-specific access control
- …?

Skip to end

Mobility helps security

- Mobility/portability can help in surprising ways: e.g.,
  - PayPal Bump
  - …
- Mobiles sense location, motion, light/sound, …
  - Use cues from context/history to set sensible access policies ? ("Contextual Security")

An example: Device Lock



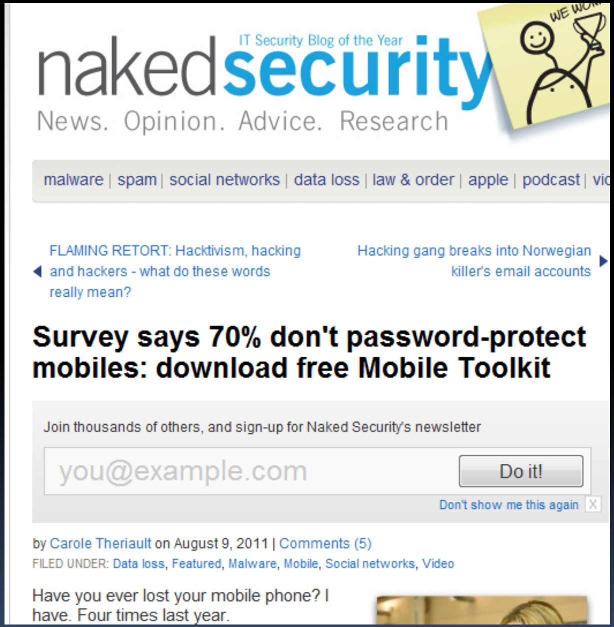
Press Release

Norton Survey Reveals One in Three Experience Cell Phone Loss, Theft

Norton Mobile Security allows users to locate and remotely wipe or lock their lost or stolen Android phones with a quick text message

MOUNTAIN VIEW, Calif. – Feb. 8, 2011 – At a time when smartphone use has become engrained in everyday life as a primary way to communicate, work and share, a new survey from Norton reveals that 36 percent of consumers in the U.S. have fallen victim to cell phone loss or theft[1]. These results make it clear that there is a growing need to protect important and personal information stored on smartphones. To that end, Norton released today Norton Mobile Security 1.5, the only product for Android to seamlessly combine anti-theft features with powerful mobile antimalware, giving consumers a sense of security in the event their phone is lost or stolen.

https://www.symantec.com/about/newsroom/press-releases/2011/symantec_0208_01



nakedsecurity
IT Security Blog of the Year
News. Opinion. Advice. Research
WE WON
malware | spam | social networks | data loss | law & order | apple | podcast | vi

FLAMING RETORT: Hacktivism, hacking and hackers - what do these words really mean?

Hacking gang breaks into Norwegian killer's email accounts

Survey says 70% don't password-protect mobiles: download free Mobile Toolkit

Join thousands of others, and sign-up for Naked Security's newsletter

you@example.com
Do it!
Don't show me this again

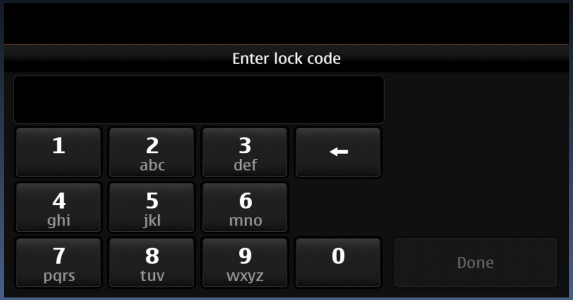
by Carole Theriault on August 9, 2011 | Comments (5)

FILED UNDER: Data loss, Featured, Malware, Mobile, Social networks, Video

Have you ever lost your mobile phone? I have. Four times last year.

http://nakedsecurity.sophos.com/2011/08/09/free-sophos-mobile-security-toolkit/

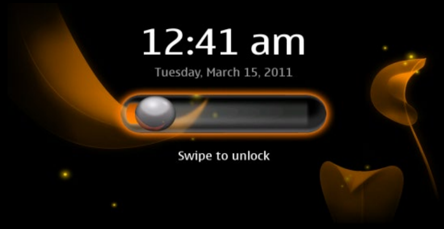
- Intended for theft protection
- Example of one-size-fits-all
  - Lock always kicks in
- Can be annoying in
  - Freezing weather
  - Groggy mornings
  - …

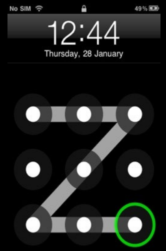


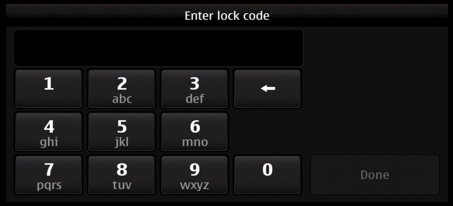
Enter lock code

Better Device Lock via Context Profiling

Timeout and unlocking method adjusted based on estimated familiarity/safety of current context







Long timeout

Medium timeout

Short timeout

Home

Work Cafeteria

Unknown

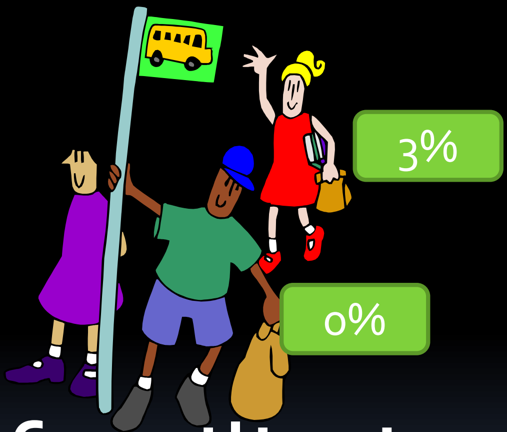
Familiarity of people, things & places

- Devices are proxies for people
- Detect nearby devices & keep track of encounters
- Identify places ("contexts") meaningful to user

A. Gupta et al, "Intuitive Security Policy Configuration in Mobile Devices Using Context Profiling" SocialCom '12
M. Miettinen et al, "**ConXsense: automated context classification for context-aware access control** " ACM ASIACCS '14

Familiarity of people, things & places

Estimate familiarity of a device in a context



Estimate context familiarity based on who/what is nearby

A. Gupta et al, "Intuitive Security Policy Configuration in Mobile Devices Using Context Profiling" SocialCom '12
M. Miettinen et al, "**ConXsense: automated context classification for context-aware access control** " ACM ASIACCS '14

Familiarity of people, things & places

Estimate familiarity of a device in a context

Estimate context familiarity based on who is nearby

How to estimate safety?

A. Gupta et al, "Intuitive Security Policy Configuration in Mobile Devices Using Context Profiling" SocialCom '12
M. Miettinen et al, "**ConXsense: automated context classification for context-aware access control** " ACM ASIACCS '14

Did you learn:

- Improving usability of app authorization
- Other problem instances of usable mobile security

Plan for the course

- Lecture 1: Platform security basics
- Lecture 2: Case study – Android OS Platform Security
- Lecture 3: Mobile platform security
- Lecture 4: Hardware security enablers
- Lecture 5: Usability of platform security
- Lecture 6: Summary and outlook
- Lecture 7: SE Android policies
- Lecture 8: Machine learning and security
- Lecture 8: IoT Security