IMPACT OF USER CHARACTERISTICS ON ATTITUDES TOWARDS AUTOMATIC ANDROID APPLICATION UPDATES

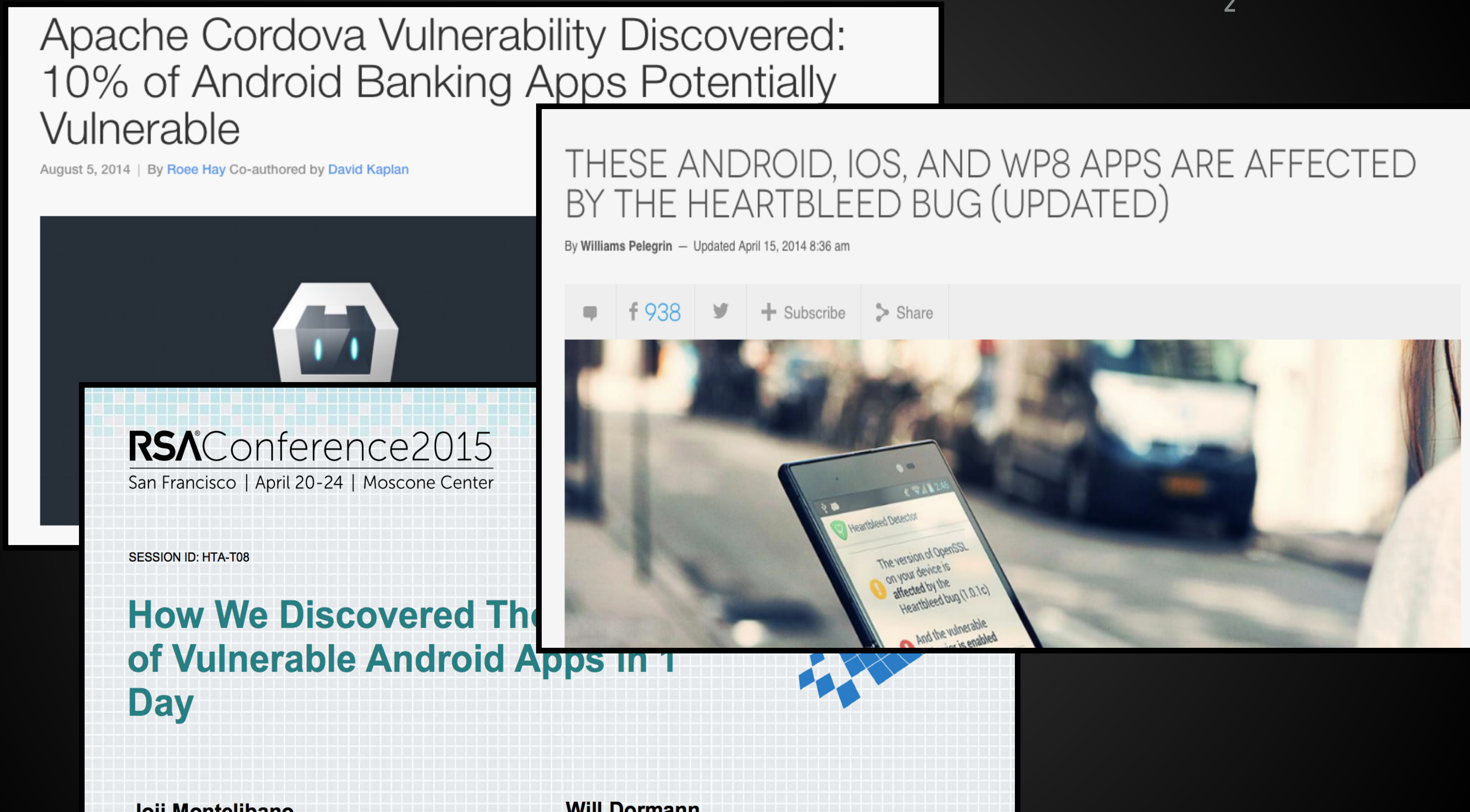
Arunesh Mathur, Marshini Chetty

@aruneshmathur

PRINCETON UNIVERSITY

CITP CENTER FOR INFORMATION TECHNOLOGY POLICY AT PRINCETON UNIVERSITY

UNIVERSITY OF MARYLAND



Apache Cordova Vulnerability Discovered: 10% of Android Banking Apps Potentially Vulnerable

August 5, 2014 | By Roee Hay Co-authored by David Kaplan

THESE ANDROID, IOS, AND WP8 APPS ARE AFFECTED BY THE HEARTBLEED BUG (UPDATED)

By Williams Pelegrin — Updated April 15, 2014 8:36 am

f 938
+ Subscribe
Share
Heartbleed Detector
The version of OpenSSL on your device is affected by the Heartbleed bug (1.0.1c)
And the vulnerable
is enabled

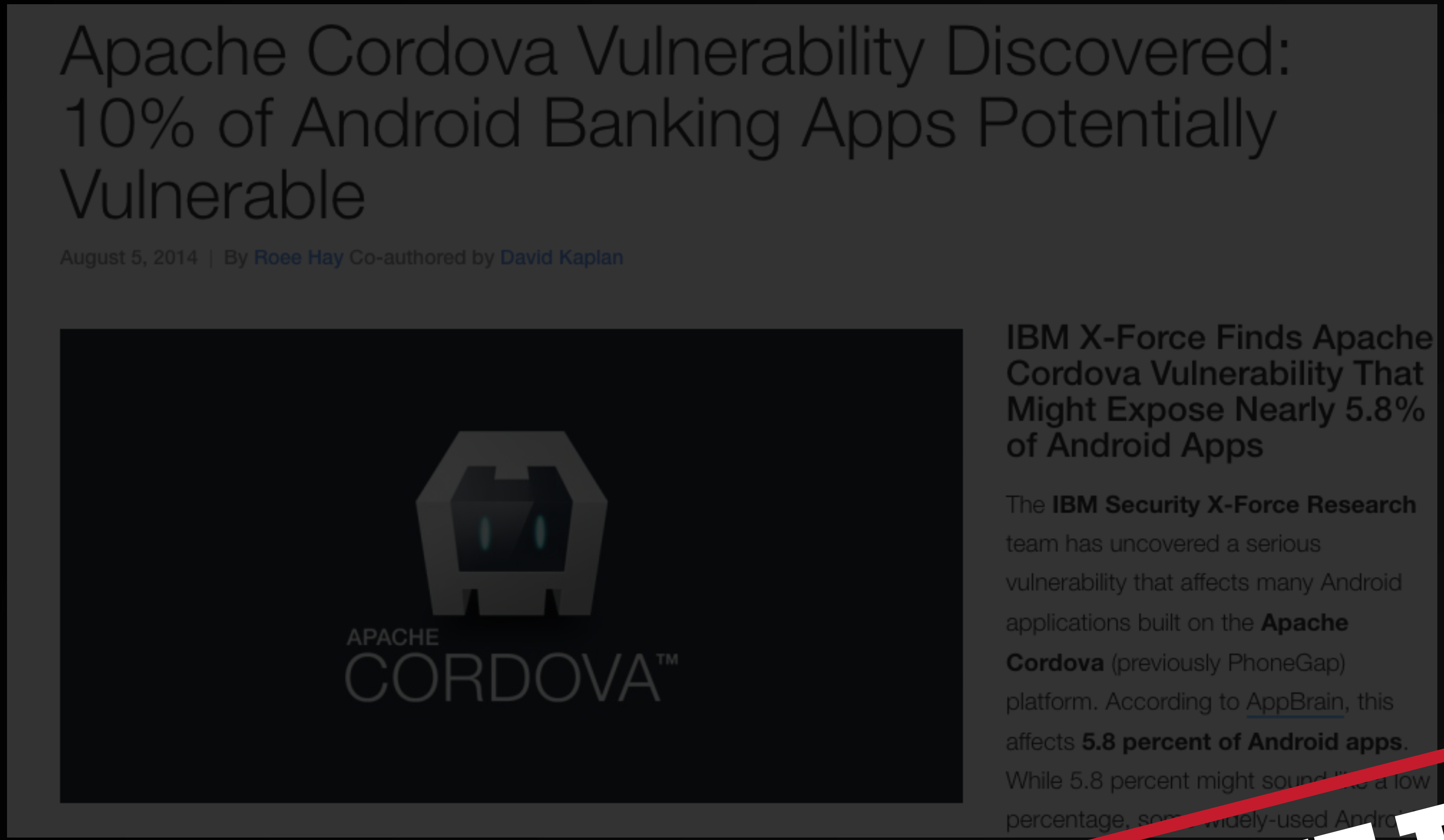
RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: HTA-T08

How We Discovered The of Vulnerable Android Apps in 1 Day

Joji Montelibano

Will Dormann

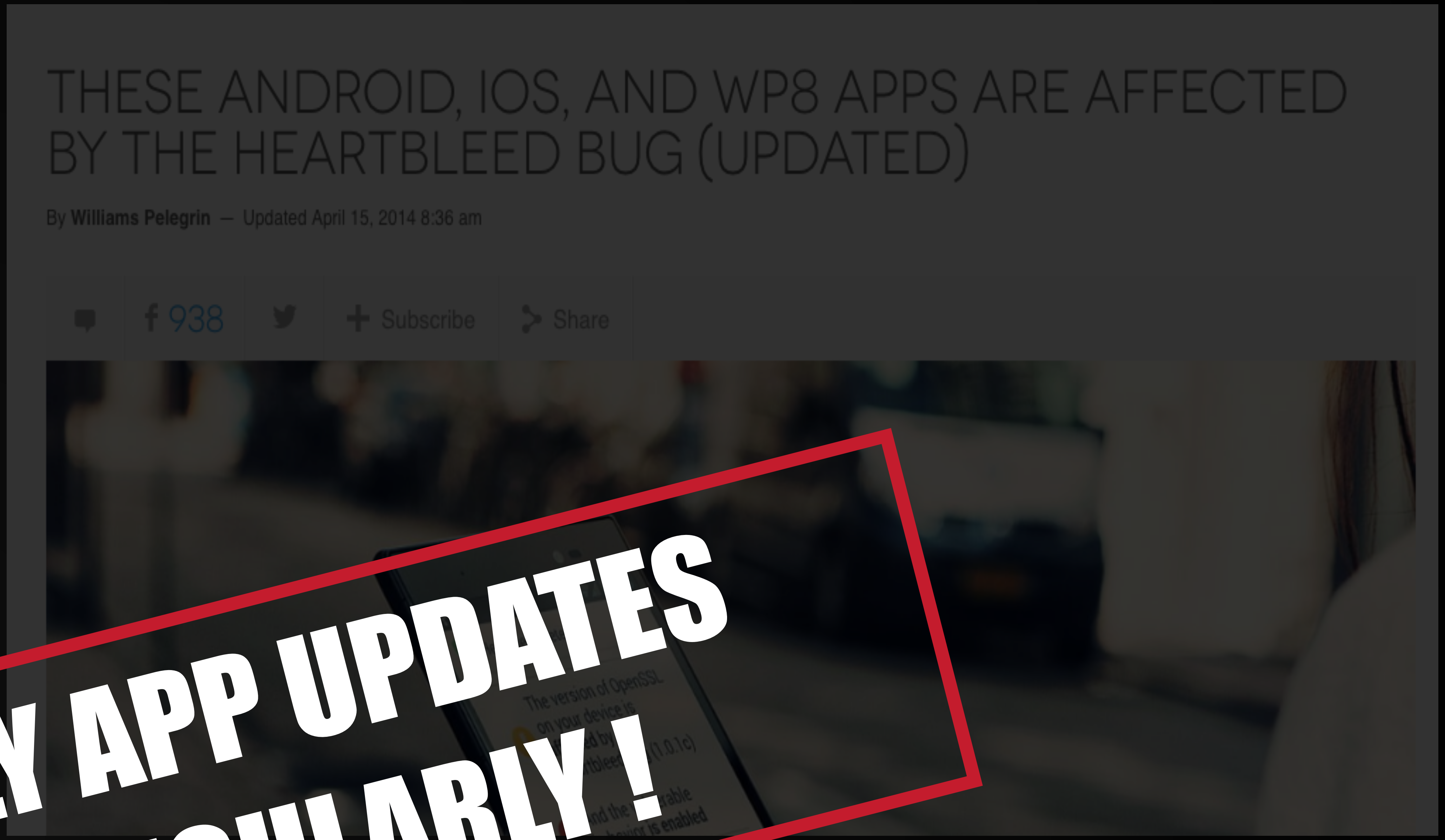


Apache Cordova Vulnerability Discovered: 10% of Android Banking Apps Potentially Vulnerable

August 5, 2014 | By Roee Hay Co-authored by David Kaplan

IBM X-Force Finds Apache Cordova Vulnerability That Might Expose Nearly 5.8% of Android Apps

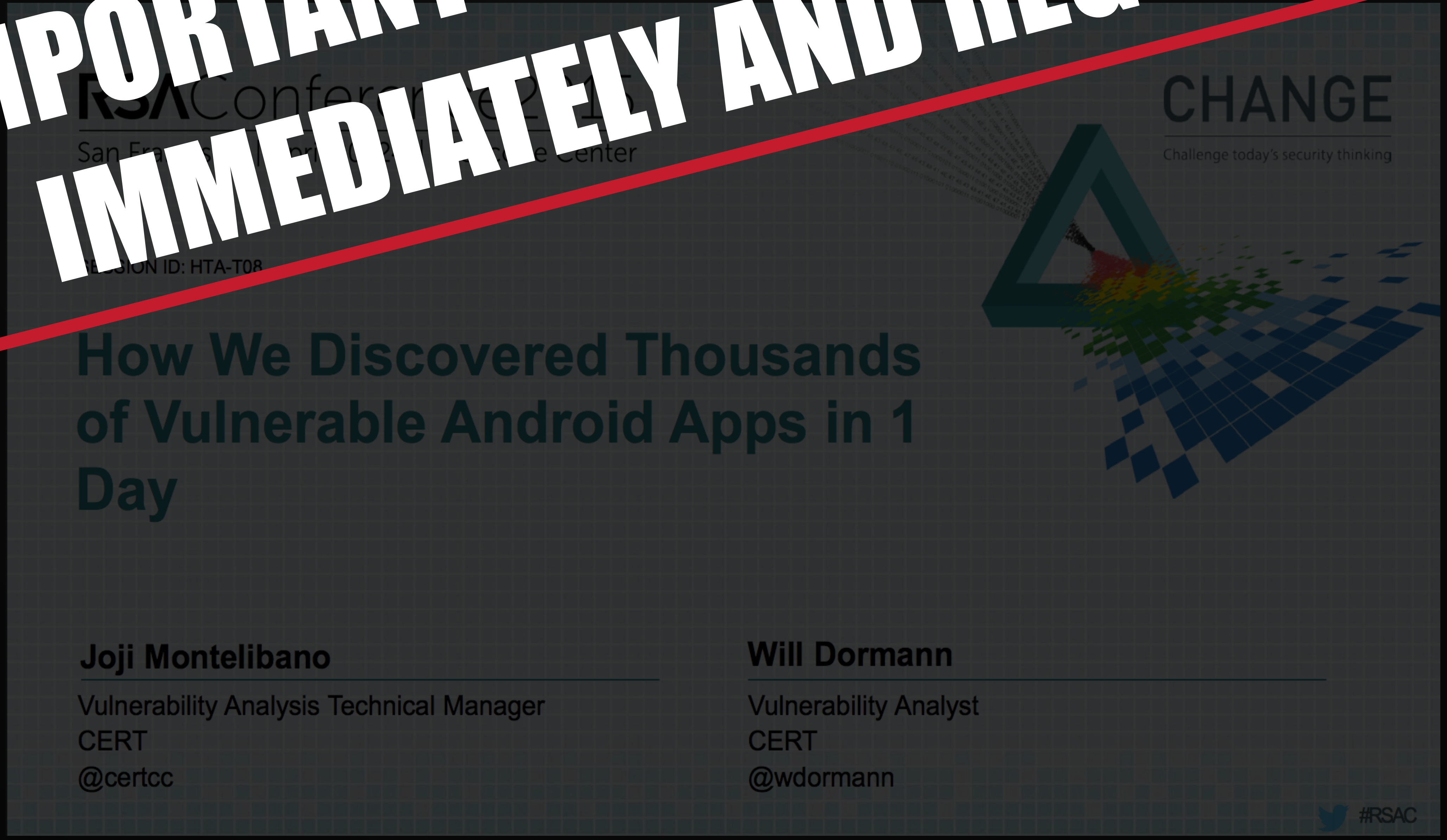
The **IBM Security X-Force Research** team has uncovered a serious vulnerability that affects many Android applications built on the **Apache Cordova** (previously PhoneGap) platform. According to AppBrain, this affects **5.8 percent of Android apps**. While 5.8 percent might sound ... a low percentage, so... widely-used Andro



THESE ANDROID, IOS, AND WP8 APPS ARE AFFECTED BY THE HEARTBLEED BUG (UPDATED)

By Williams Pelegrin — Updated April 15, 2014 8:36 am

IMPORTANT TO APPLY APP UPDATES IMMEDIATELY AND REGULARLY !

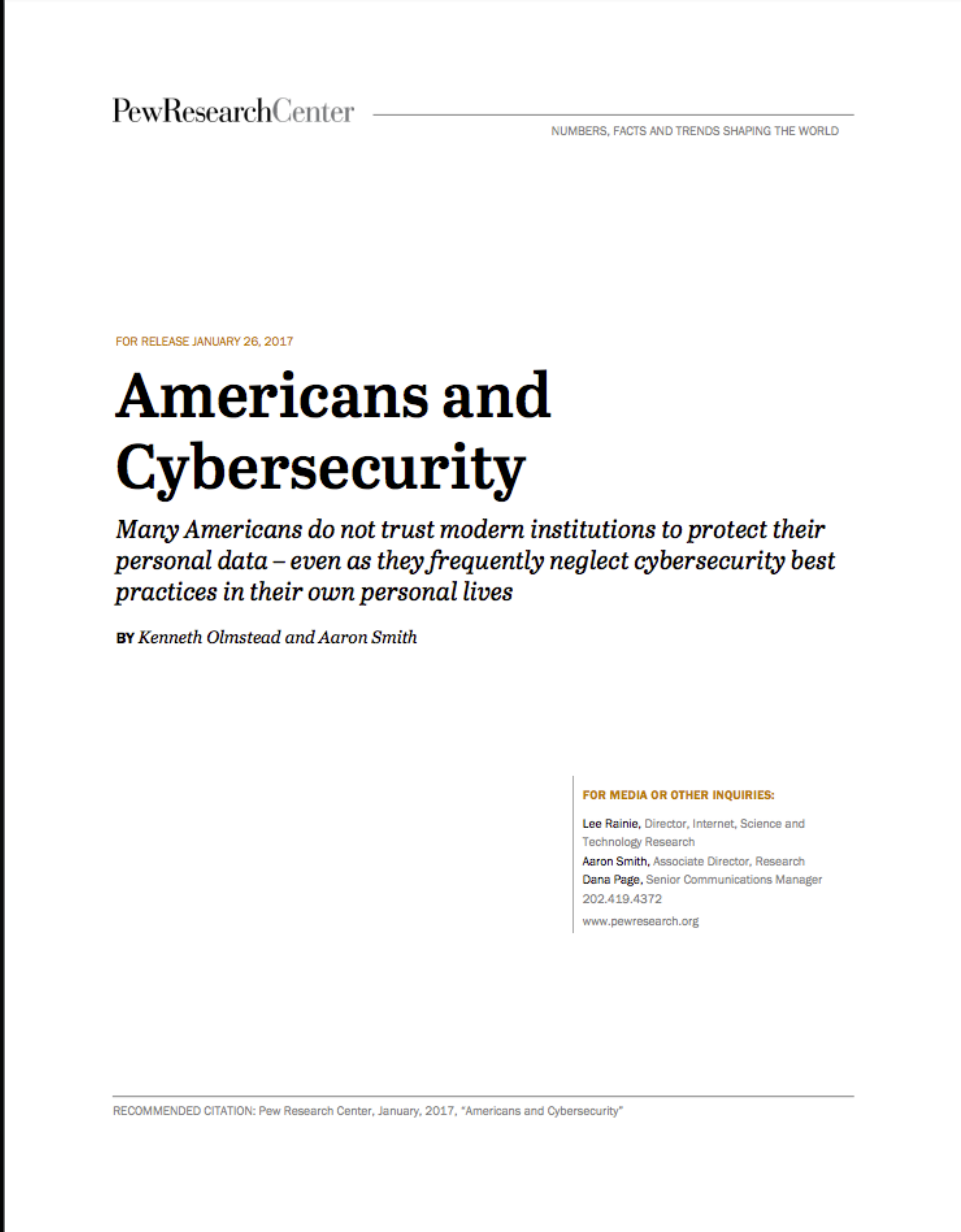


SESSION ID: HTA-T08

How We Discovered Thousands of Vulnerable Android Apps in 1 Day

Joji Montelibano
Vulnerability Analysis Technical Manager
CERT
@certcc

Will Dormann
Vulnerability Analyst
CERT
@wdormann



PewResearchCenter

NUMBERS, FACTS AND TRENDS SHAPING THE WORLD

FOR RELEASE JANUARY 26, 2017

Americans and Cybersecurity

Many Americans do not trust modern institutions to protect their personal data – even as they frequently neglect cybersecurity best practices in their own personal lives

BY *Kenneth Olmstead and Aaron Smith*

FOR MEDIA OR OTHER INQUIRIES:

Lee Rainie, Director, Internet, Science and Technology Research
Aaron Smith, Associate Director, Research
Dana Page, Senior Communications Manager
202.419.4372
www.pewresearch.org

RECOMMENDED CITATION: Pew Research Center, January, 2017, "Americans and Cybersecurity"

To Pin or Not to Pin
Helping App Developers Bullet Proof Their TLS Connections

Marten Oltrogge, Yasemin Acar
DCSEC, Leibniz University Hannover
oltrogge,acar@dcsec.uni-hannover.de

Sergej Dechand, Matthew Smith
USECAP, University Bonn
dechand, smith@cs.uni-bonn.de

Sascha Fahl
FKIE, Fraunhofer
fahl@fkie.fraunhofer.de

Abstract

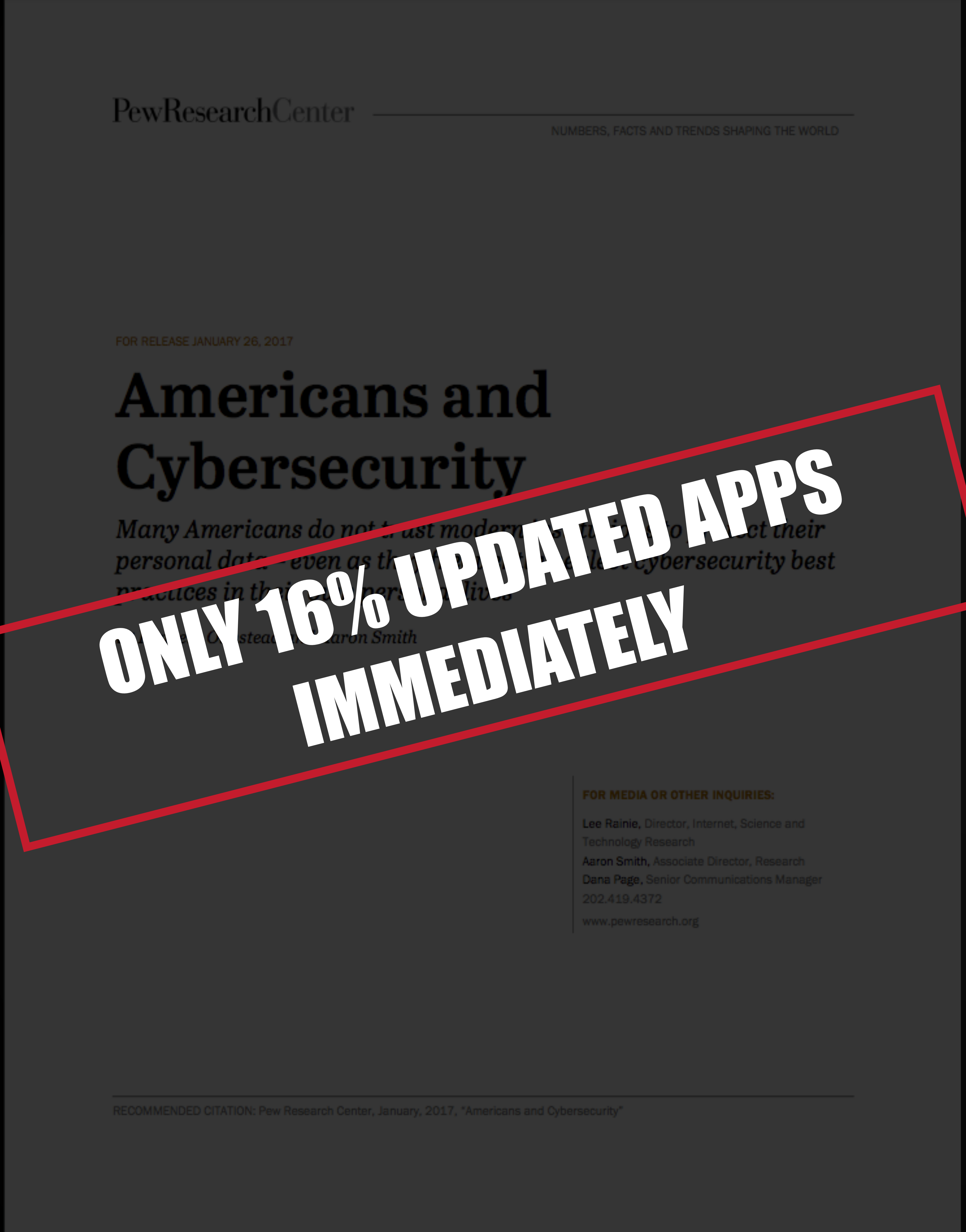
For increased security during TLS certificate validation, a common recommendation is to use a variation of pinning. Especially non-browser software developers are encouraged to limit the number of trusted certificates to a minimum, since the default CA-based approach is known to be vulnerable to serious security threats.
The decision for or against pinning is always a tradeoff between increasing security and keeping maintenance efforts at an acceptable level. In this paper, we present an extensive study on the applicability of pinning for non-browser software by analyzing 639,283 Android apps. Conservatively, we propose pinning as an appropriate strategy for 11,547 (1.8%) apps or for 45,247 TLS connections (4.25%) in our sample set. With a more optimistic classification of borderline cases, we propose pinning for consideration for 58,817 (9.1%) apps or for 140,020 (3.8%[1]) TLS connections. This weakens the assumption that pinning is a widely usable strategy for TLS security in non-browser software. However, in a nominal-actual comparison, we find that only 45 apps actually implement pinning. We collected developer feedback from 45 respondents and learned that only a quarter of them grasp the concept of pinning, but still find pinning too complex to use. Based on their feedback, we built an easy-to-use web-application that supports developers in the decision process and guides them through the correct deployment of a pinning-protected TLS implementation.

1 Introduction

Android is the major platform for mobile users and mobile app developers. Many apps handle sensitive information and deploy the transport layer security protocol (TLS) to protect data in transit. Previous research uncovered security issues with TLS in mobile apps [7, 8, 9, 2, 22] that highlight that developers have problems with implementing correct certificate validation while users are challenged by TLS interstitials. Furthermore, the default TLS implementation on Android receives criticism [24, 18]: Adopted from web-browsers, default TLS certificate validation relies on a huge number of root CAs pre-installed on all Android devices [24]. Hence, all Android apps suffer from the same issues as web-browsers: A single malicious CA is able to conduct Man-In-The-Middle attacks (MITMAs) against all apps trusting the respective certificate. To make things even worse, Fahl et al. [8] uncovered that in 97% of all cases where developers implemented their own certificate validation strategy, they turned off validation entirely and left their apps vulnerable to MITMAs with arbitrary certificates, i.e. every active network attacker was able to attack successfully.

Pinning is often recommended as a general countermeasure to tackle the weakest link in the CA-based infrastructure [1, 14, 17, 8]. We use the term *pinning* in this paper to include both pinning the complete X.509 certificate or only the certificate's public key. Instead of trusting a large set of root CAs that come pre-installed with the operating system, software limits the set of certificates it trusts to *pins*, which can be single leaf certificates, single root CA certificates or a set of certificates. Pinning is a straightforward mechanism and its deployment does not require changes to the current CA infrastructure. However, pinning has not found widespread adoption yet. While limiting the number of trusted certificates drastically increases security, pinning doesn't come for free: Embedding trusted certificates into an app requires app updates whenever the pins change. Hence, the decision whether

[1] This smaller percentage in the optimistic case is caused by a different prevalence of third party library use.



PewResearchCenter

NUMBERS, FACTS AND TRENDS SHAPING THE WORLD

FOR RELEASE JANUARY 26, 2017

Americans and Cybersecurity

Many Americans do not t[illegible]ust moder[illegible] [illegible] [illegible]o [illegible]ct their personal dat[illegible] – even as th[illegible] [illegible] [illegible] cybersecurity best practices in th[illegible] [illegible] [illegible]s

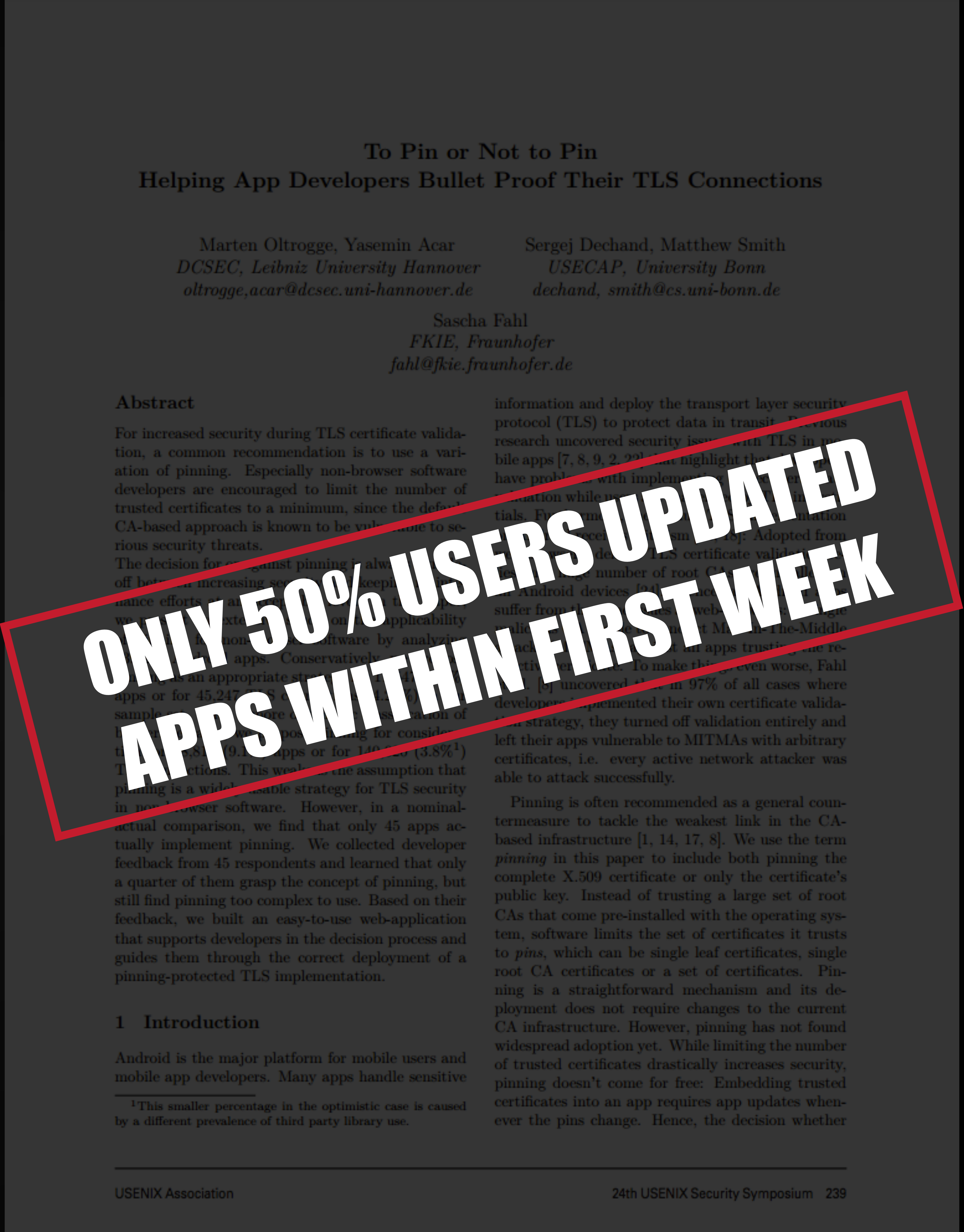
[illegible] O[illegible]stead [illegible] Aaron Smith

ONLY 16% UPDATED APPS IMMEDIATELY

FOR MEDIA OR OTHER INQUIRIES:

Lee Rainie, Director, Internet, Science and Technology Research
Aaron Smith, Associate Director, Research
Dana Page, Senior Communications Manager
202.419.4372
www.pewresearch.org

RECOMMENDED CITATION: Pew Research Center, January, 2017, "Americans and Cybersecurity"



To Pin or Not to Pin
Helping App Developers Bullet Proof Their TLS Connections

Marten Oltrogge, Yasemin Acar
DCSEC, Leibniz University Hannover
oltrogge,acar@dcsec.uni-hannover.de

Sergej Dechand, Matthew Smith
USECAP, University Bonn
dechand, smith@cs.uni-bonn.de

Sascha Fahl
FKIE, Fraunhofer
fahl@fkie.fraunhofer.de

ONLY 50% USERS UPDATED APPS WITHIN FIRST WEEK

Abstract

For increased security during TLS certificate validation, a common recommendation is to use a variation of pinning. Especially non-browser software developers are encouraged to limit the number of trusted certificates to a minimum, since the defa[illegible] CA-based approach is known to be vu[illegible] to serious security threats.

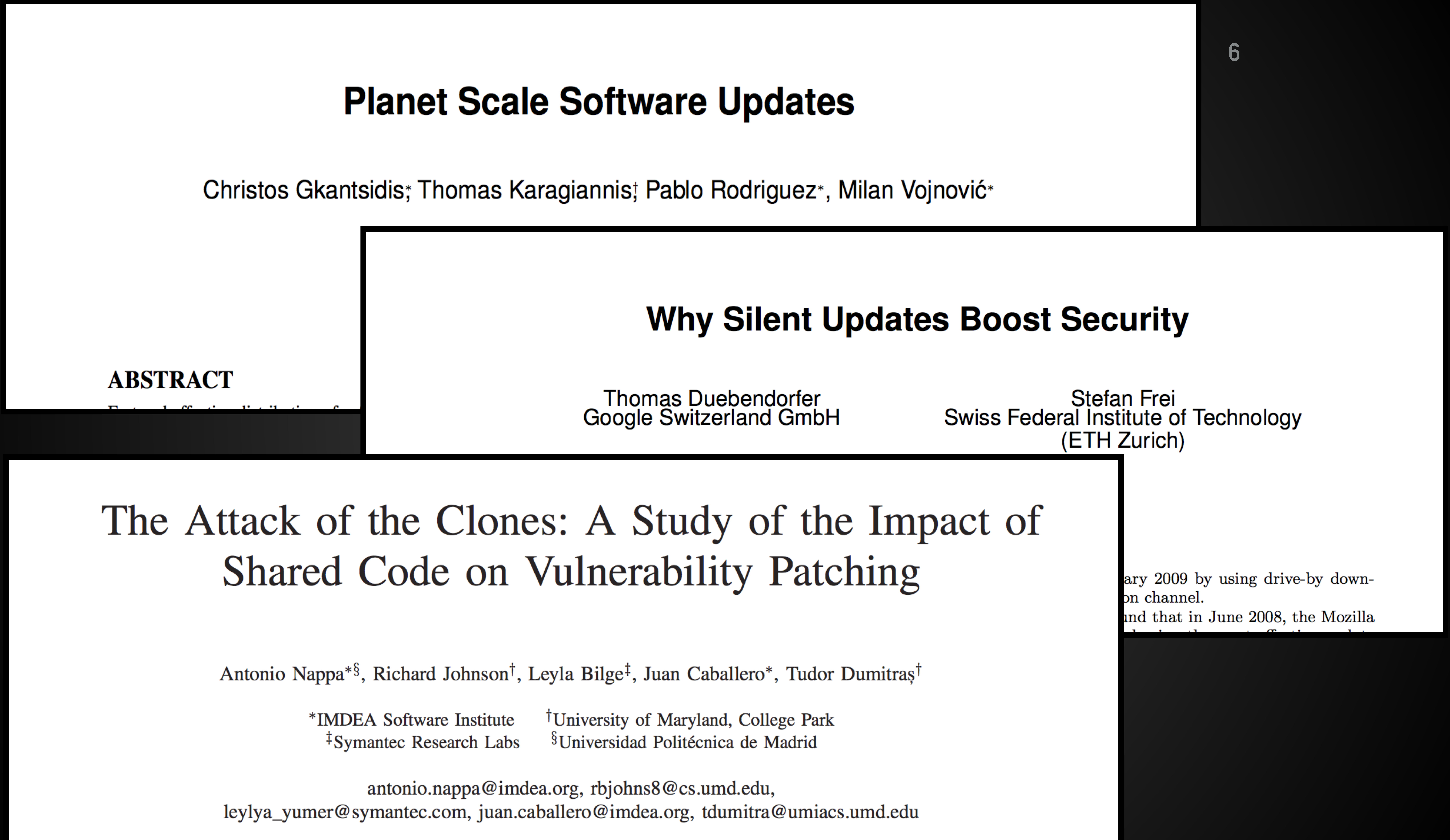
The decision for [illegible] against pinning i[illegible] alw[illegible] [illegible] off [illegible] increasing se[illegible] [illegible] keepi[illegible] [illegible]nance efforts [illegible] [illegible] [illegible] we [illegible] [illegible] exte[illegible] [illegible] on [illegible] applicability [illegible] [illegible] non-[illegible] software by analyzing [illegible] apps. Conservatively [illegible] [illegible] as an appropriate str[illegible] [illegible] apps or for 45,247 [illegible] [illegible] [illegible] sample [illegible] [illegible] [illegible] [illegible] [illegible] pos[illegible] [illegible] for conside[illegible] [illegible] (9.1[illegible]) apps or for 14[illegible] (3.8%[1]) T[illegible] [illegible]ctions. This wea[illegible] the assumption that pinning is a wide[illegible] usable strategy for TLS security in no[illegible] [illegible]owser software. However, in a nominal-actual comparison, we find that only 45 apps actually implement pinning. We collected developer feedback from 45 respondents and learned that only a quarter of them grasp the concept of pinning, but still find pinning too complex to use. Based on their feedback, we built an easy-to-use web-application that supports developers in the decision process and guides them through the correct deployment of a pinning-protected TLS implementation.

1 Introduction

Android is the major platform for mobile users and mobile app developers. Many apps handle sensitive information and deploy the transport layer security protocol (TLS) to protect data in transit. P[illegible]vious research uncovered security iss[illegible] with TLS in mobile apps [7, 8, 9, 2, 2[illegible]] [illegible] highlight th[illegible] [illegible] have probl[illegible] with impleme[illegible] [illegible] validation while [illegible] [illegible] tials. Fu[illegible] [illegible] [illegible] [illegible]ntation [illegible] recei[illegible] [illegible]sm [illegible], 18]: Adopted from [illegible] de[illegible] TLS certificate validati[illegible] [illegible] [illegible] number of root CA[illegible] [illegible] Android devices [24][illegible] [illegible] suffer from th[illegible] [illegible] web-[illegible] [illegible] malic[illegible] [illegible] Man-In-The-Middle [illegible] [illegible] all apps trusti[illegible] [illegible] re-[illegible]ctiv[illegible] [illegible]. To make thi[illegible] even worse, Fahl [illegible] [8] uncovered [illegible] in 97% of all cases where developers [illegible]plemented their own certificate valida[illegible] strategy, they turned off validation entirely and left their apps vulnerable to MITMAs with arbitrary certificates, i.e. every active network attacker was able to attack successfully.

Pinning is often recommended as a general countermeasure to tackle the weakest link in the CA-based infrastructure [1, 14, 17, 8]. We use the term *pinning* in this paper to include both pinning the complete X.509 certificate or only the certificate's public key. Instead of trusting a large set of root CAs that come pre-installed with the operating system, software limits the set of certificates it trusts to *pins*, which can be single leaf certificates, single root CA certificates or a set of certificates. Pinning is a straightforward mechanism and its deployment does not require changes to the current CA infrastructure. However, pinning has not found widespread adoption yet. While limiting the number of trusted certificates drastically increases security, pinning doesn't come for free: Embedding trusted certificates into an app requires app updates whenever the pins change. Hence, the decision whether

[1] This smaller percentage in the optimistic case is caused by a different prevalence of third party library use.



Planet Scale Software Updates

Christos Gkantsidis*, Thomas Karagiannis‡, Pablo Rodriguez*, Milan Vojnović*

ABSTRACT

Why Silent Updates Boost Security

Thomas Duebendorfer
Google Switzerland GmbH

Stefan Frei
Swiss Federal Institute of Technology
(ETH Zurich)

ary 2009 by using drive-by down-
on channel.
und that in June 2008, the Mozilla

The Attack of the Clones: A Study of the Impact of Shared Code on Vulnerability Patching

Antonio Nappa*§, Richard Johnson†, Leyla Bilge‡, Juan Caballero*, Tudor Dumitraș†

*IMDEA Software Institute †University of Maryland, College Park
‡Symantec Research Labs §Universidad Politécnica de Madrid

antonio.nappa@imdea.org, rbjohns8@cs.umd.edu,
leylya_yumer@symantec.com, juan.caballero@imdea.org, tdumitra@umiacs.umd.edu

US-CERT
UNITED STATES COMPUTER
EMERGENCY READINESS TEAM

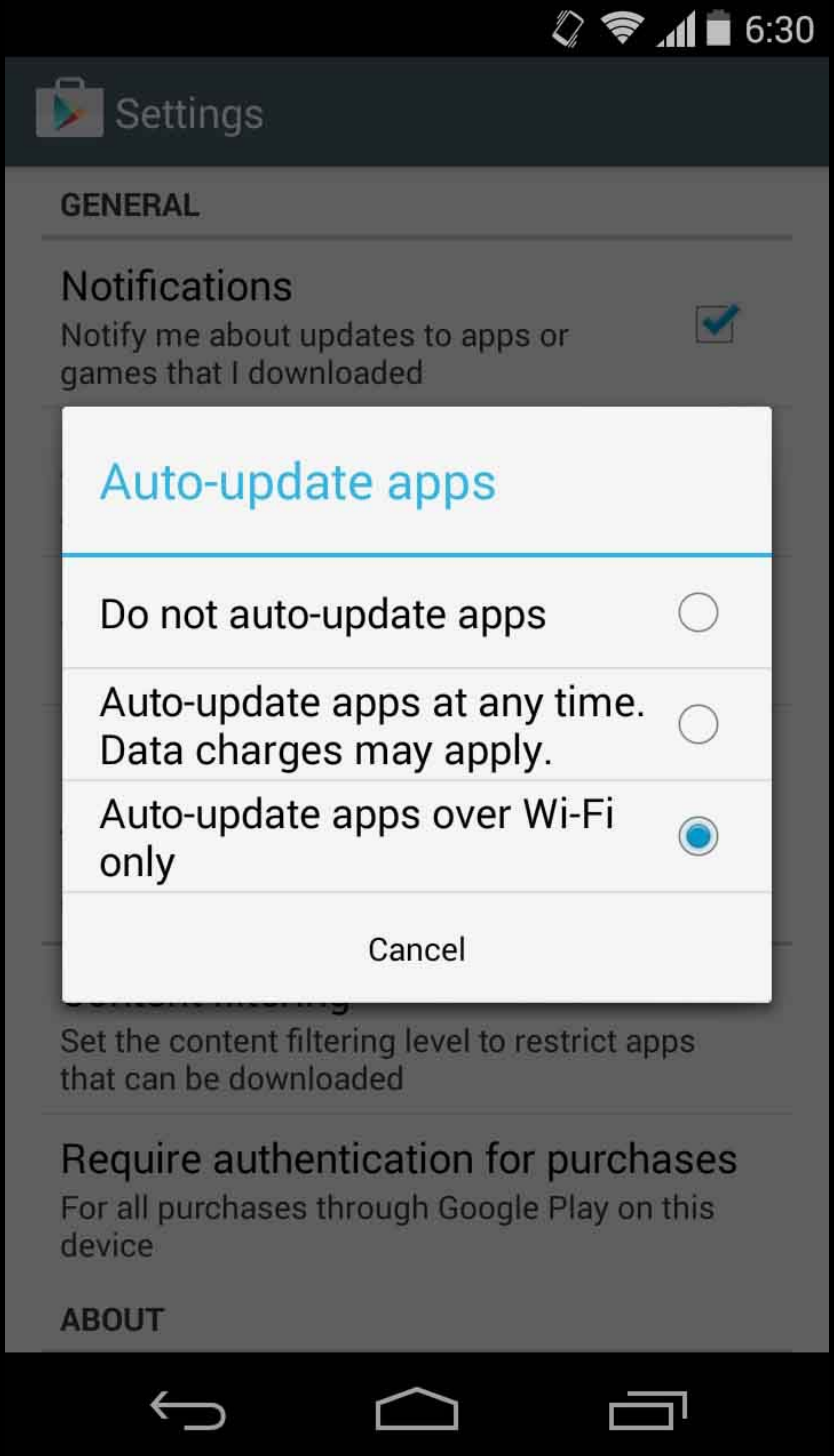
> Enable automatic updates if your vendors offer it; that will ensure your software is always updated, and you won’t have to remember to do it yourself.

CISCO

> Greater use of automatic updating may be one solution to the outdated software problem

Symantec

> Running out-of-date versions can put you at risk from being exploited by web-based attacks. Select automatic updates wherever possible.



6:30

Settings

GENERAL

Notifications

Notify me about updates to apps or games that I downloaded ☑

Auto-update apps

Do not auto-update apps ○

Auto-update apps at any time. Data charges may apply. ○

Auto-update apps over Wi-Fi only ●

Cancel

Set the content filtering level to restrict apps that can be downloaded

Require authentication for purchases

For all purchases through Google Play on this device

ABOUT

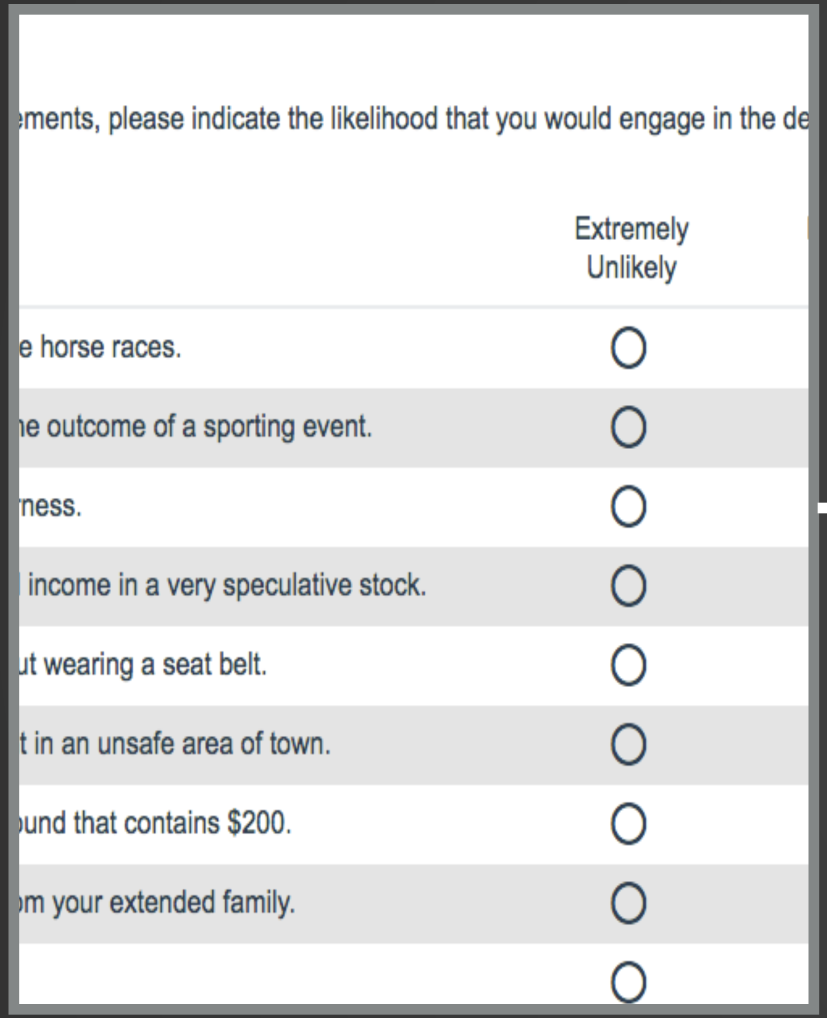
Research Questions

- What user characteristics differentiate those Android users who avoid auto-updates from those who do auto-update their applications?
- What user characteristics explain Android users' preferences towards auto-updating their applications?

User characteristics?

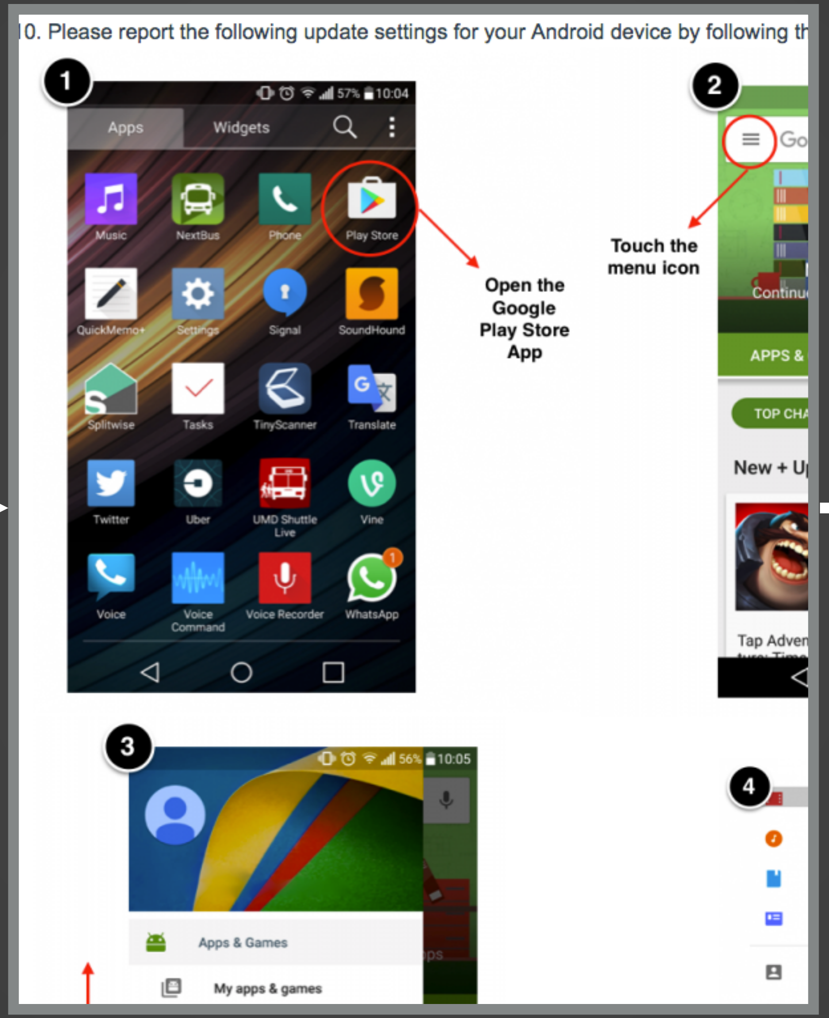
- Past Negative Software Updating Experience [Vaniea *CHI* '14, Vaniea *CHI* '16, Forget *SOUPS* '16]
- Psychometric Traits [Egelman *CHI* '15]
  - Risk Taking
  - Consideration of Future Consequences
  - Curiosity and Inquisitiveness
- Application Specific Factors [Mathur *SOUPS* '16]
  - Trust in App
  - Frequency of Use of App
  - Importance of App
  - Satisfaction with App
- Demographics

Survey



ements, please indicate the likelihood that you would engage in the de

	Extremely Unlikely
e horse races.	○
he outcome of a sporting event.	○
ness.	○
income in a very speculative stock.	○
ut wearing a seat belt.	○
t in an unsafe area of town.	○
und that contains $200.	○
m your extended family.	○
	○



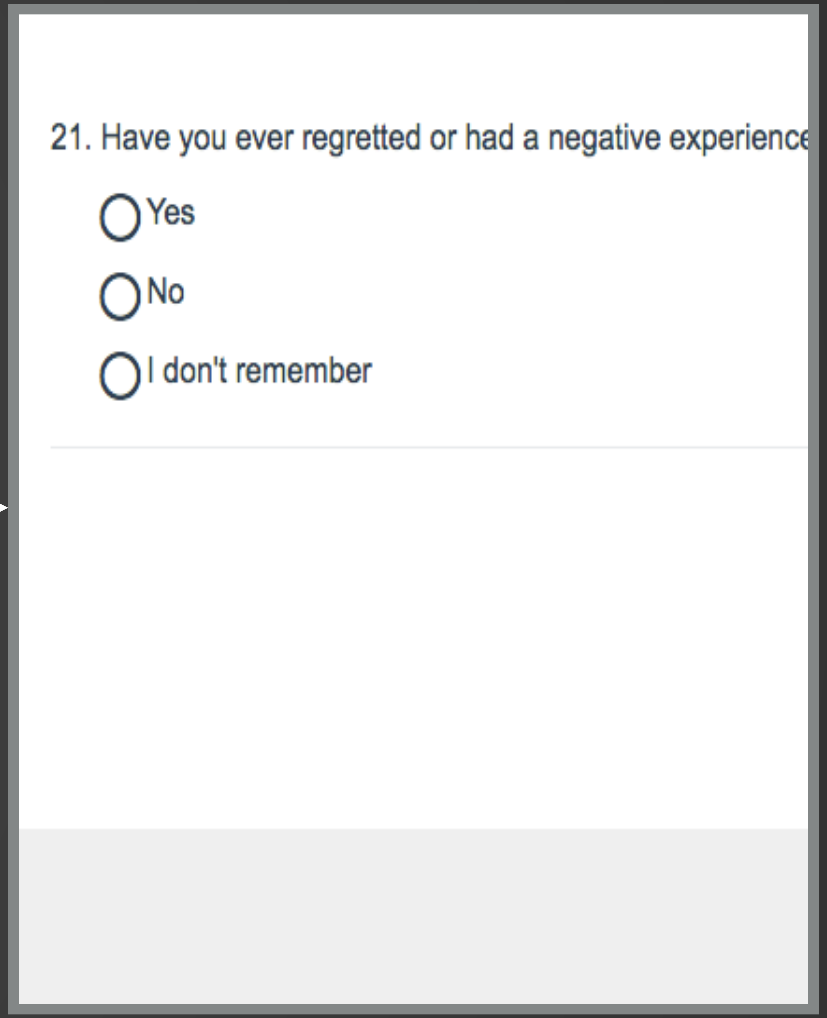
0. Please report the following update settings for your Android device by following th

1 Open the Google Play Store App

2 Touch the menu icon

3

4



21. Have you ever regretted or had a negative experience

○ Yes

○ No

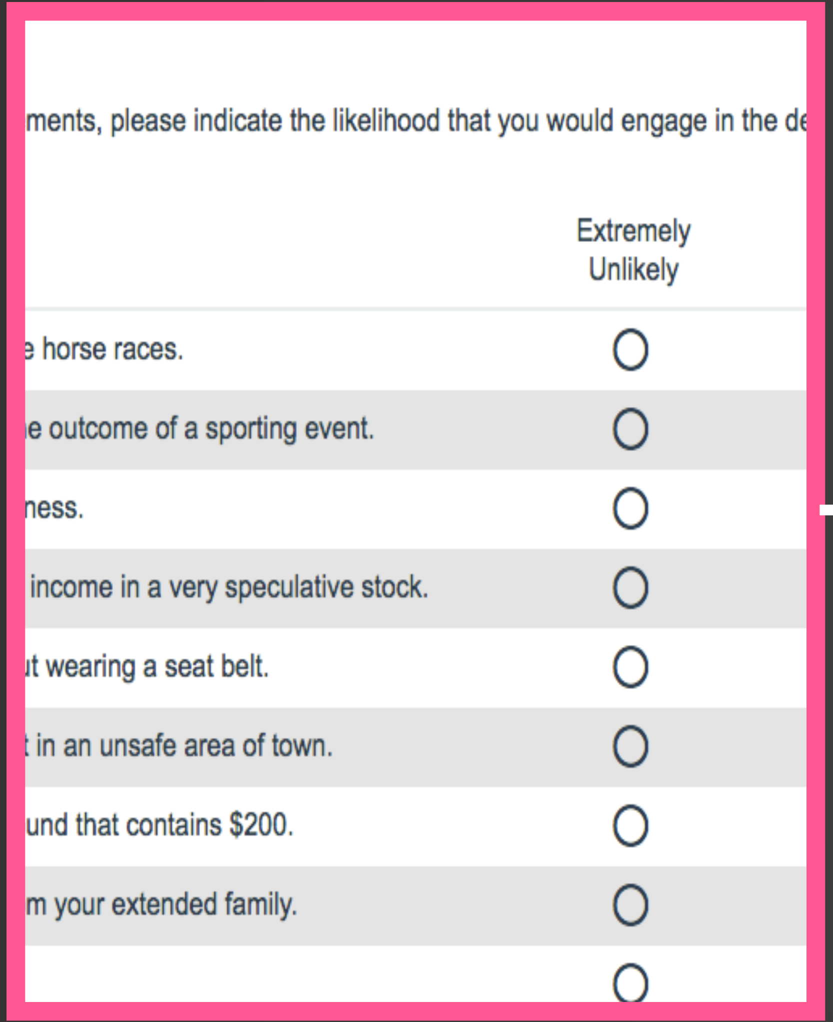
○ I don't remember

Part One:
Psychometric
Scales

Part Two:
Update settings
& Preferences

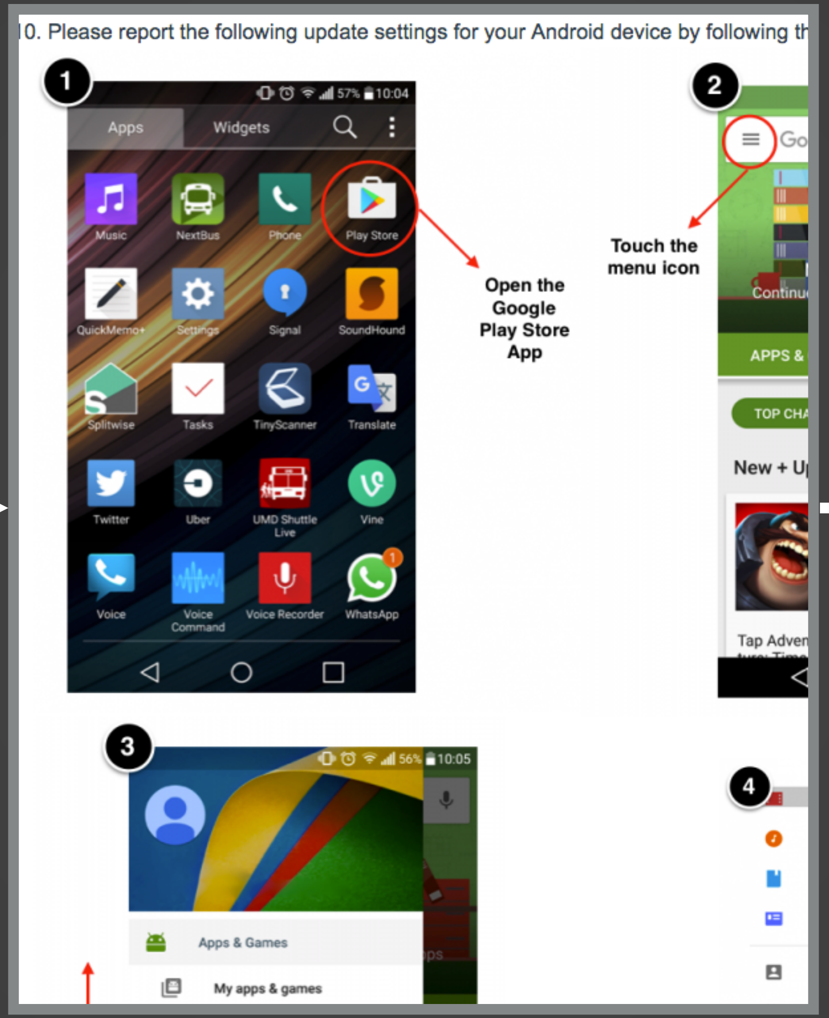
Part Three:
Past Update
Experiences

Survey



ments, please indicate the likelihood that you would engage in the de

	Extremely Unlikely
e horse races.	○
e outcome of a sporting event.	○
ness.	○
income in a very speculative stock.	○
t wearing a seat belt.	○
t in an unsafe area of town.	○
und that contains $200.	○
m your extended family.	○
	○



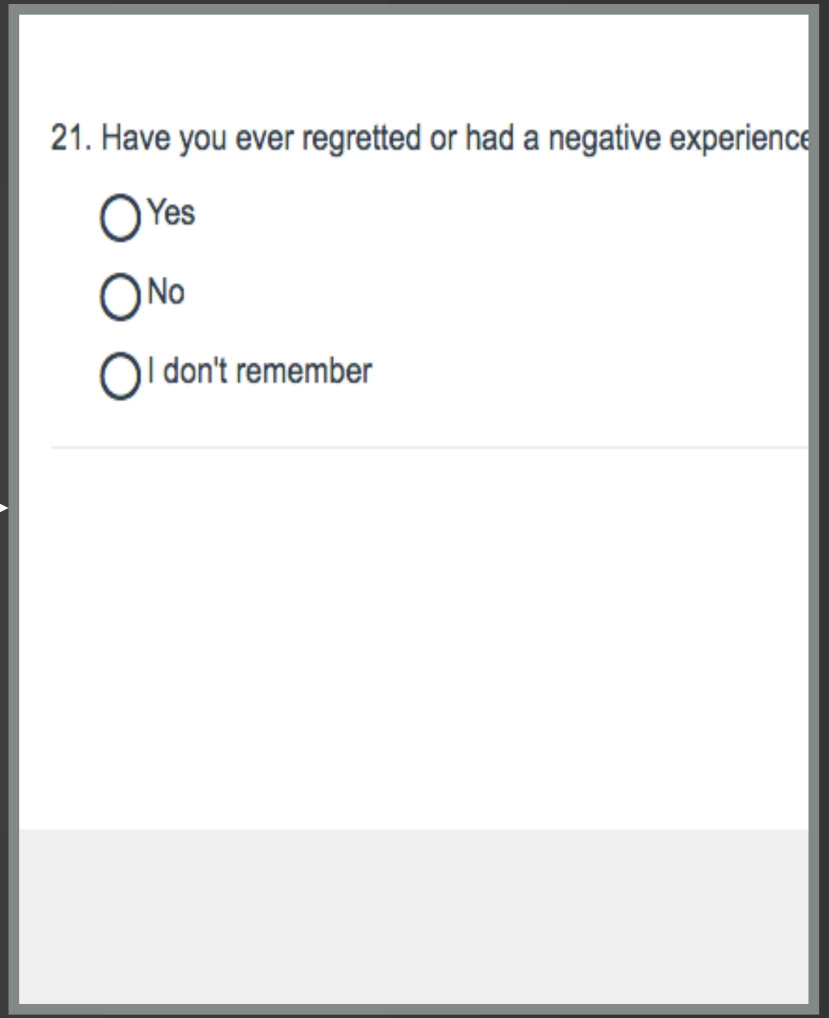
10. Please report the following update settings for your Android device by following th

1 Open the Google Play Store App

2 Touch the menu icon

3

4



21. Have you ever regretted or had a negative experience

○ Yes

○ No

○ I don't remember

Part One: Psychometric Scales

Part Two: Update settings & Preferences

Part Three: Past Update Experiences

Survey: Part One

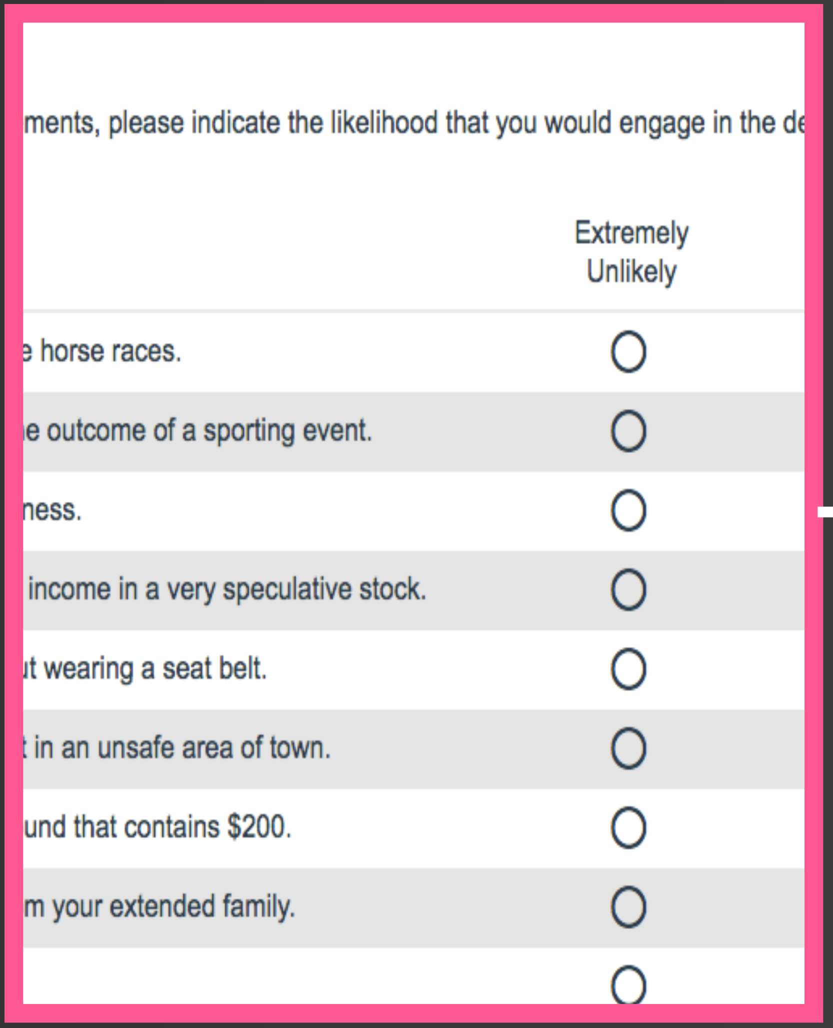
- Psychometric Scales
  - Domain Specific Risk Taking (DoSpeRT) Scale
  - Need For Cognition (NFC) scale
  - Consideration for Future Consequences (CFC) scale
  - Resistance to Change (RTC) scale
- Past Security Behavior
  - Security Behavior Intentions (SeBIS) scale

Survey: Part One

Order of Scales &
Questions Randomized

- Psychometric Scales
  - Domain Specific Risk Taking (DoSpeRT) Scale
  - Need For Cognition (NFC) scale
  - Consideration for Future Consequences (CFC) scale
  - Resistance to Change (RTC) scale
- Past Security Behavior
  - Security Behavior Intentions (SeBIS) scale

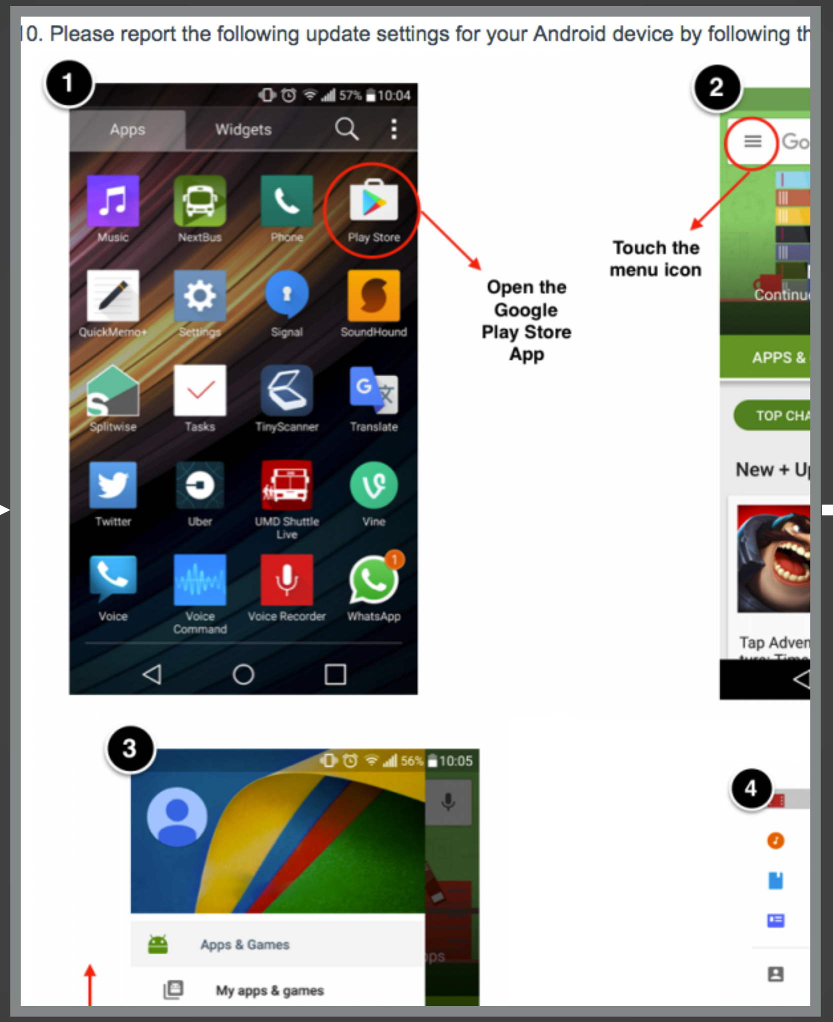
Survey



ments, please indicate the likelihood that you would engage in the de

	Extremely Unlikely
e horse races.	○
e outcome of a sporting event.	○
ness.	○
income in a very speculative stock.	○
ıt wearing a seat belt.	○
t in an unsafe area of town.	○
und that contains $200.	○
m your extended family.	○
	○

Part One: Psychometric Scales



10. Please report the following update settings for your Android device by following th

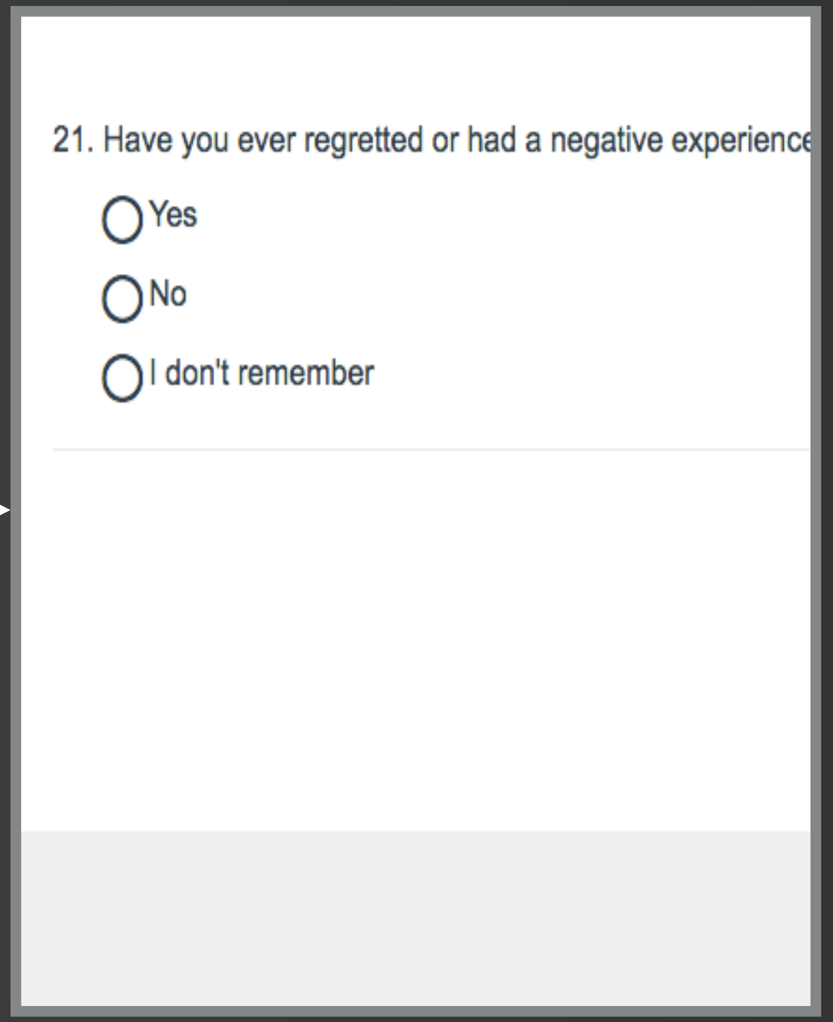
1 Open the Google Play Store App

2 Touch the menu icon

3

4

Part Two: Update settings & Preferences



21. Have you ever regretted or had a negative experience

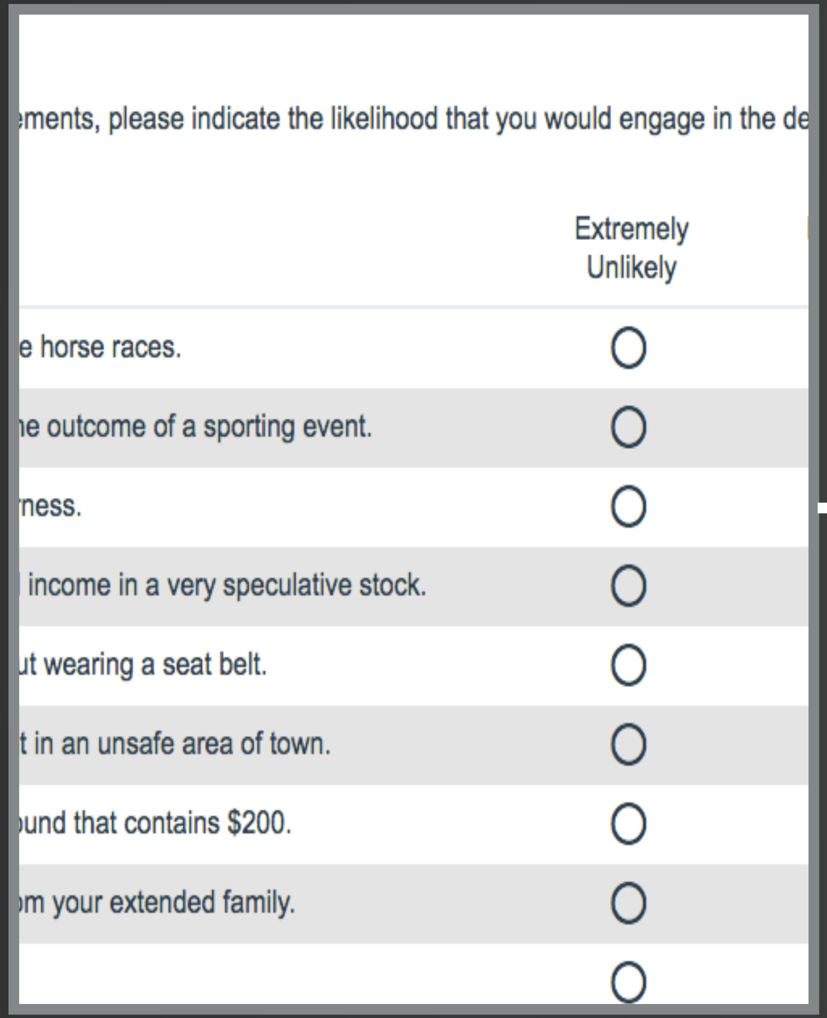
○ Yes

○ No

○ I don't remember

Part Three: Past Update Experiences

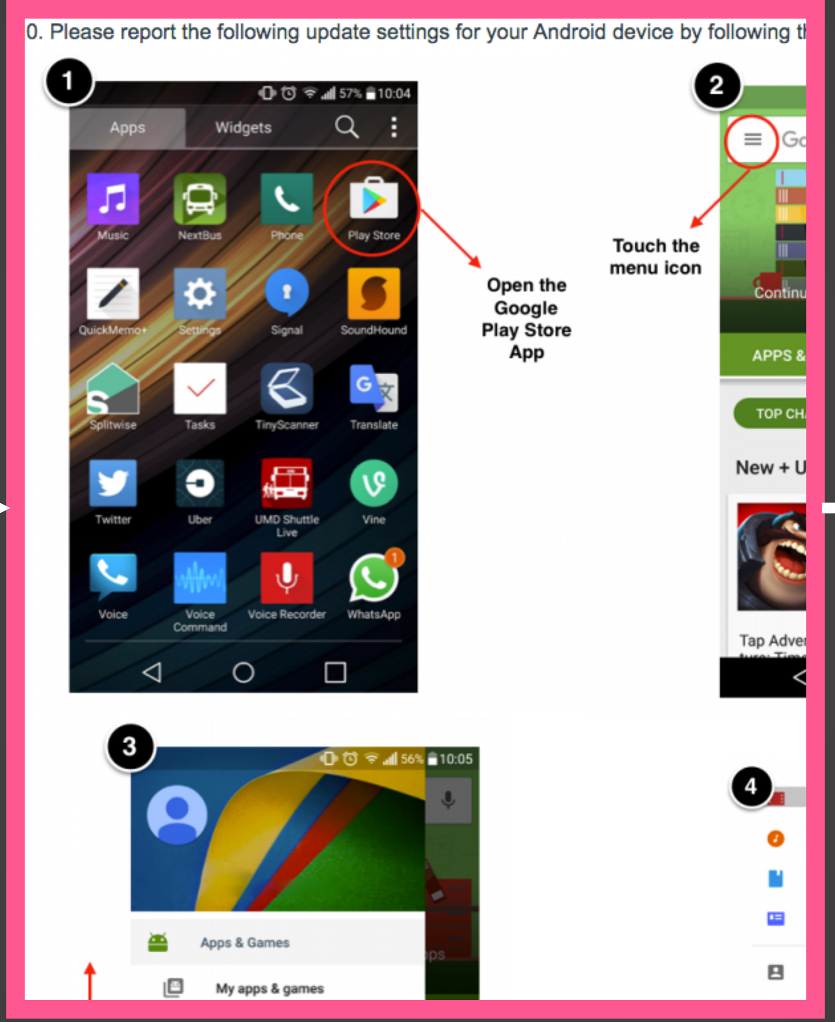
Survey



ements, please indicate the likelihood that you would engage in the de

	Extremely Unlikely
e horse races.	○
he outcome of a sporting event.	○
ness.	○
income in a very speculative stock.	○
ut wearing a seat belt.	○
t in an unsafe area of town.	○
ound that contains $200.	○
om your extended family.	○
	○

Part One:
Psychometric
Scales



0. Please report the following update settings for your Android device by following t

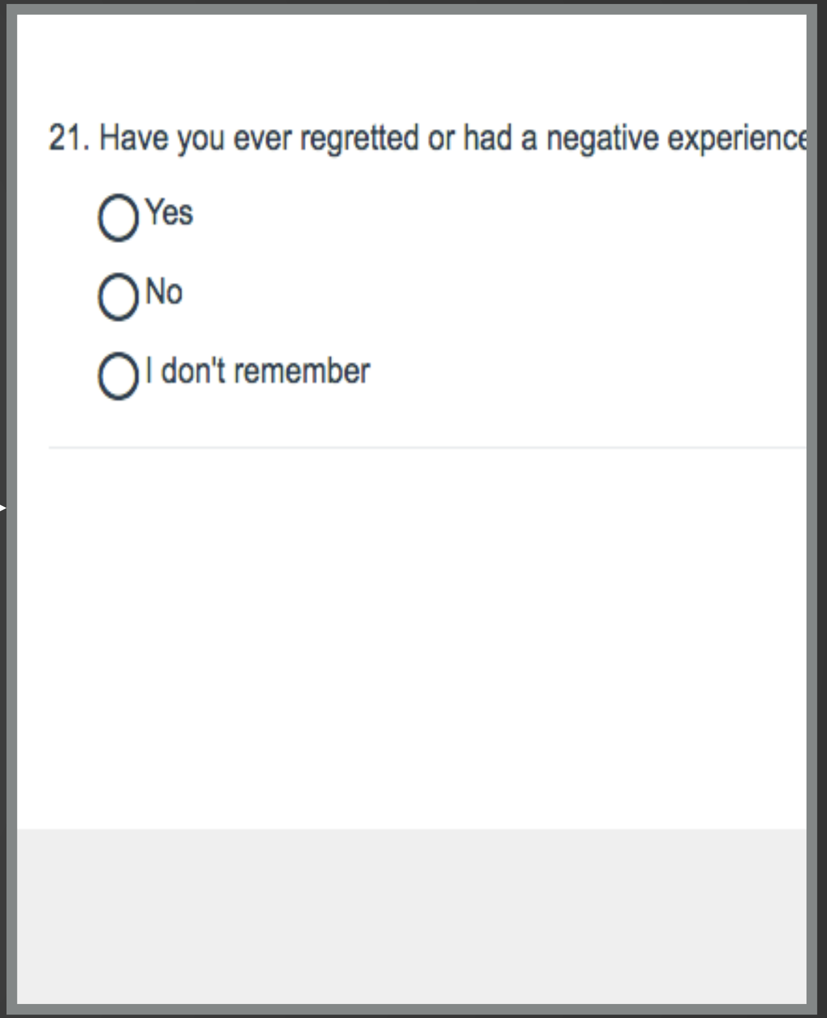
1 Open the Google Play Store App

2 Touch the menu icon

3

4

**Part Two:
Update settings
& Preferences**



21. Have you ever regretted or had a negative experience

○ Yes

○ No

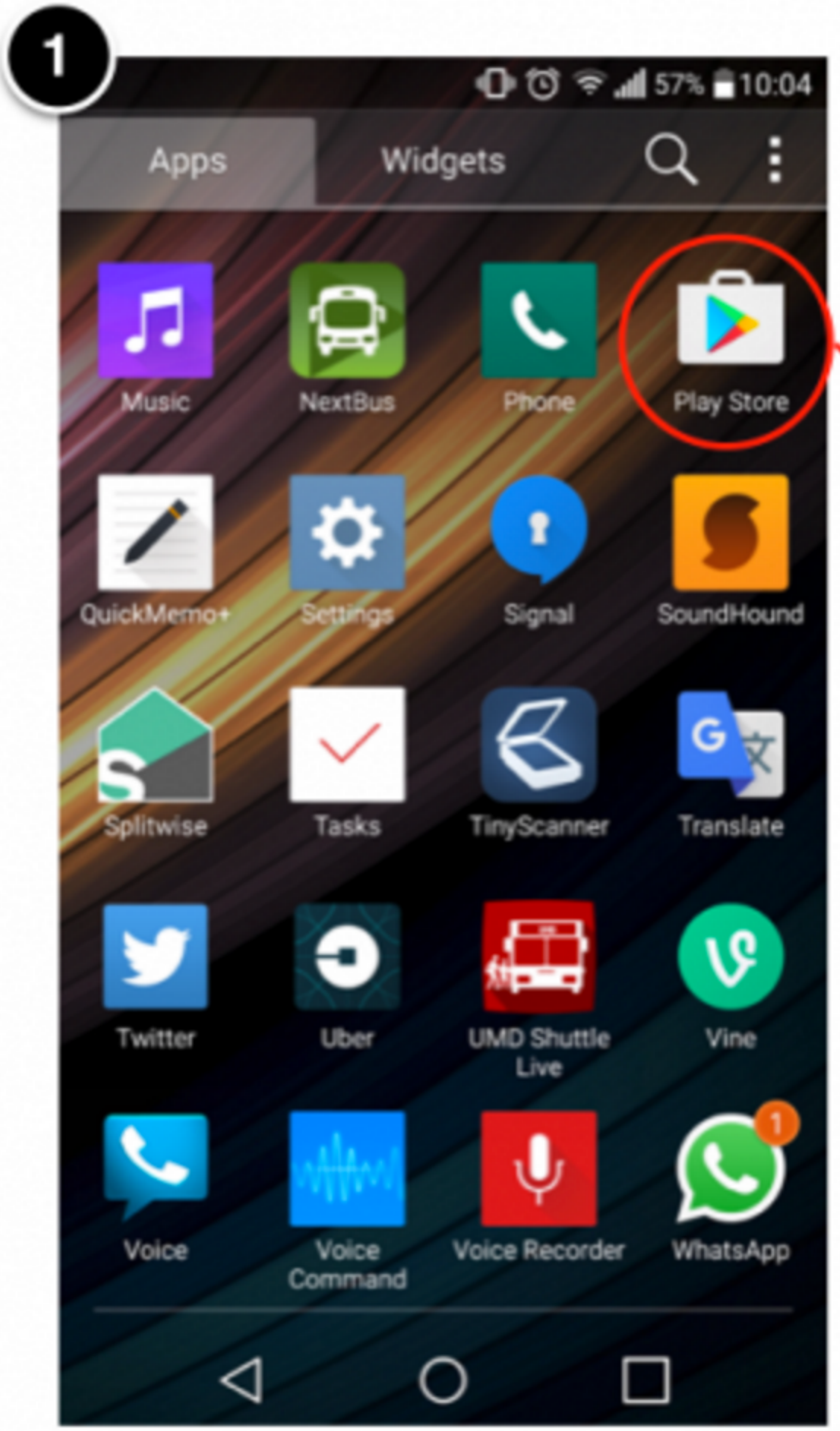
○ I don't remember

Part Three:
Past Update
Experiences

Survey: Part Two

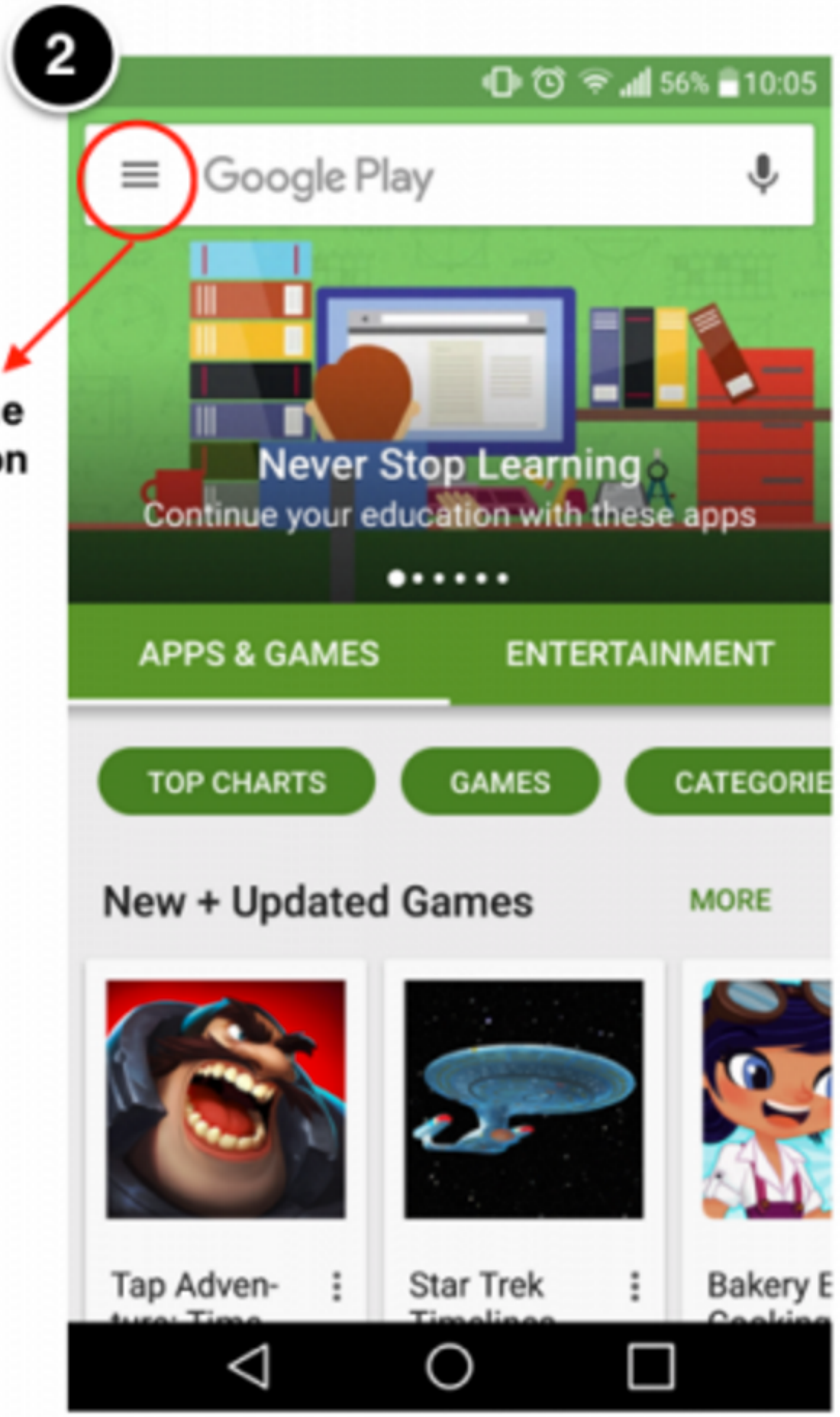
- Report Android Update Settings
  - Using labelled instructions

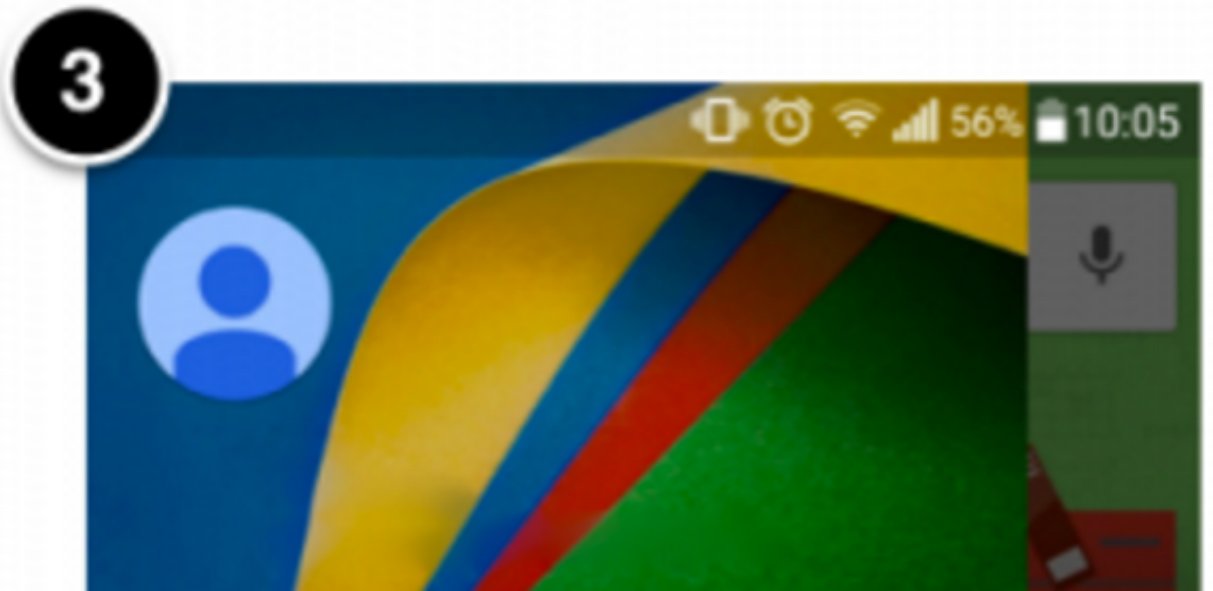
10. Please report the following update settings for your Android device by following the instructions in the images below.

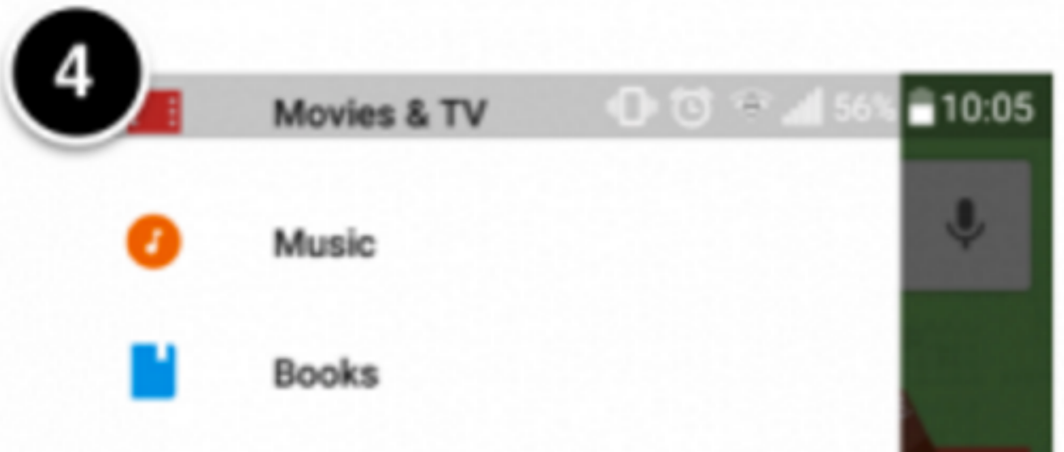


Open the Google Play Store App

Touch the menu icon





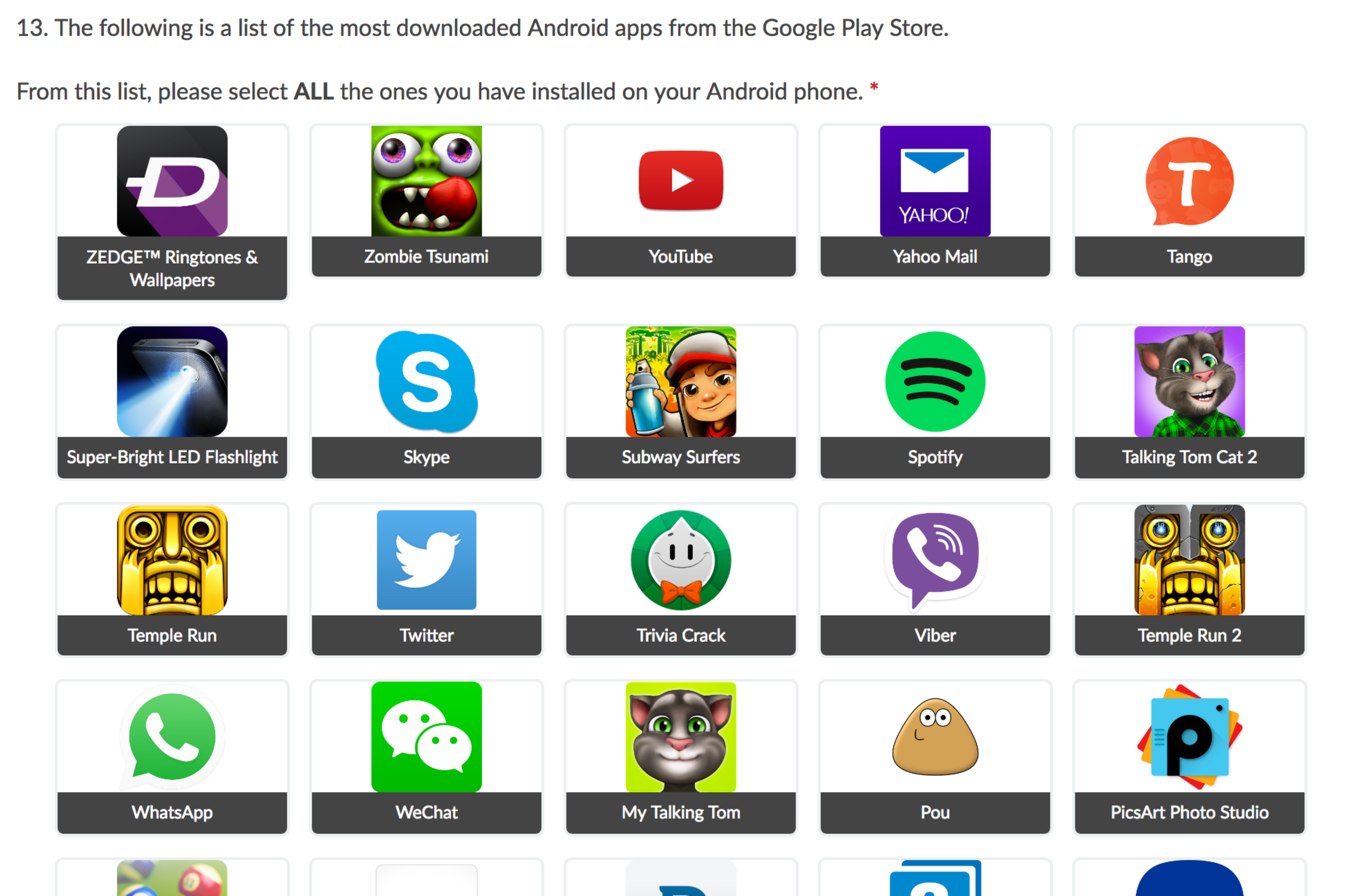


Survey: Part Two

- Report Android Update Settings
  - Using labelled instructions

Survey: Part Two

- Report Android Update Settings
  - Using labelled instructions
- Report Installed Android Applications



13. The following is a list of the most downloaded Android apps from the Google Play Store.

From this list, please select **ALL** the ones you have installed on your Android phone. *

ZEDGE™ Ringtones & Wallpapers	Zombie Tsunami	YouTube	Yahoo Mail	Tango
Super-Bright LED Flashlight	Skype	Subway Surfers	Spotify	Talking Tom Cat 2
Temple Run	Twitter	Trivia Crack	Viber	Temple Run 2
WhatsApp	WeChat	My Talking Tom	Pou	PicsArt Photo Studio

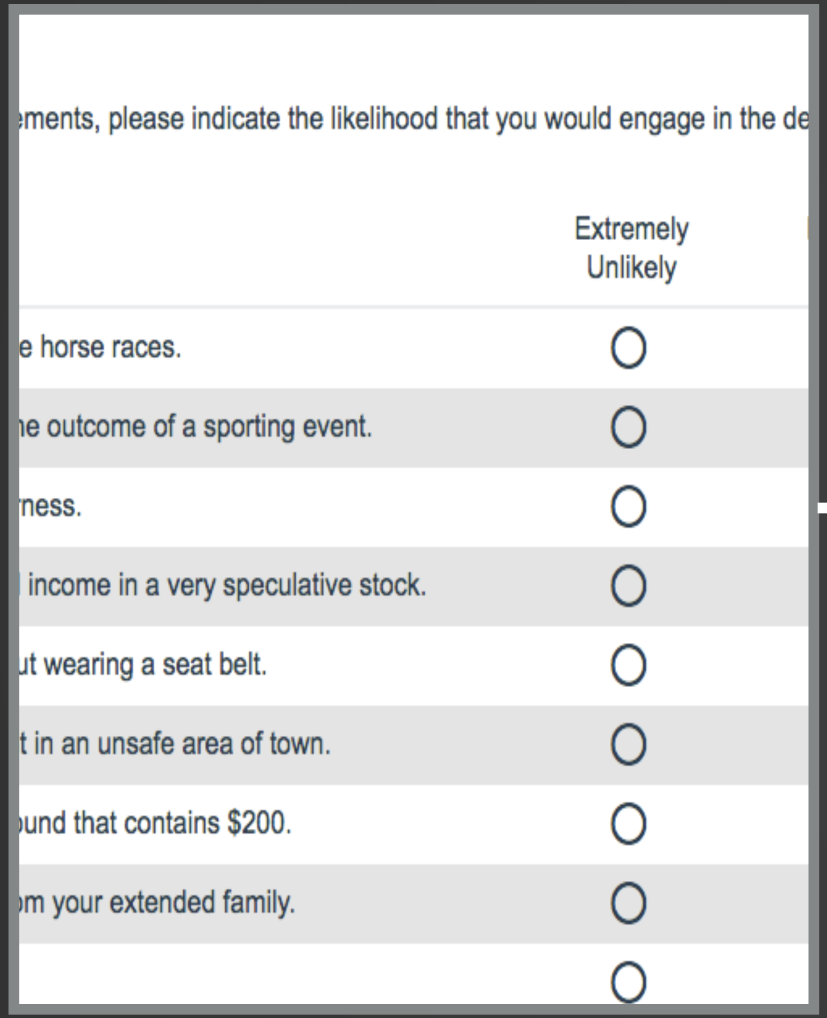
Survey: Part Two

- Report Android Update Settings
  - Using labelled instructions
- Report Installed Android Applications

Survey: Part Two

- Report Android Update Settings
  - Using labelled instructions
- Report Installed Android Applications. For a Maximum of 10 Sampled Applications:
  - Comfort auto-updating security and non-security updates (0 - 100)
  - Importance of, Trust in, Frequency of Use of, and Satisfaction with the Application (1 - 5)

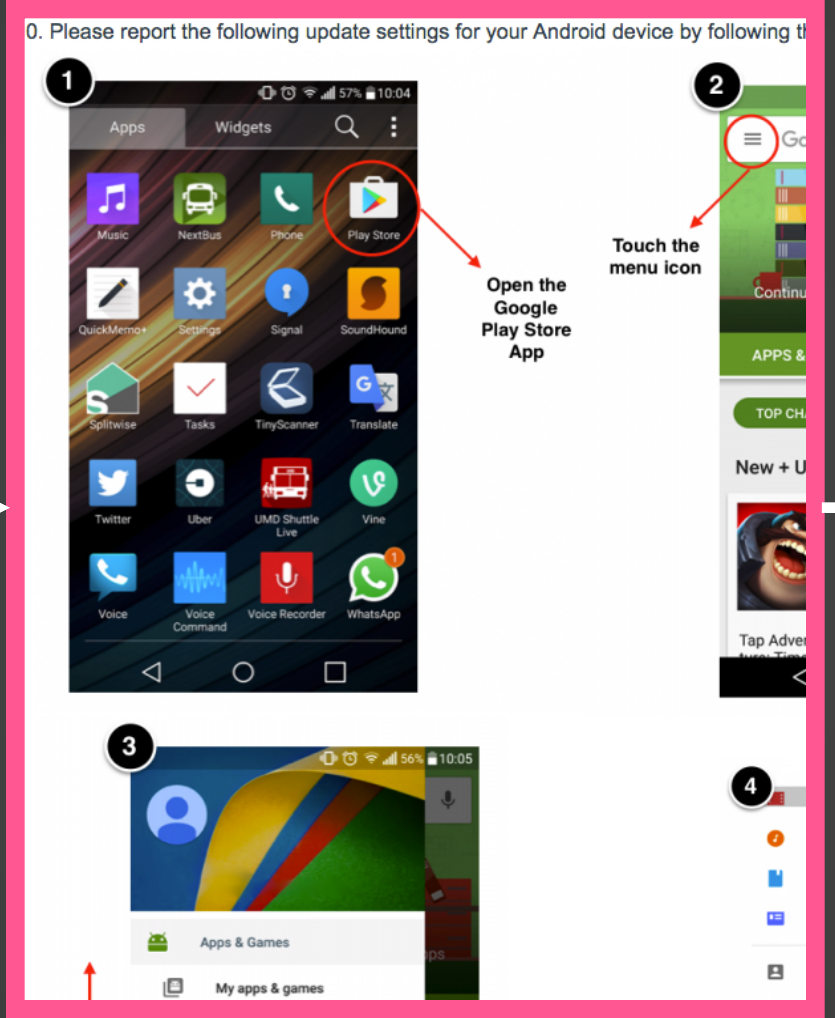
Survey



ements, please indicate the likelihood that you would engage in the de

	Extremely Unlikely
e horse races.	○
ne outcome of a sporting event.	○
ness.	○
income in a very speculative stock.	○
ut wearing a seat belt.	○
t in an unsafe area of town.	○
und that contains $200.	○
m your extended family.	○
	○

Part One:
Psychometric
Scales



0. Please report the following update settings for your Android device by following t

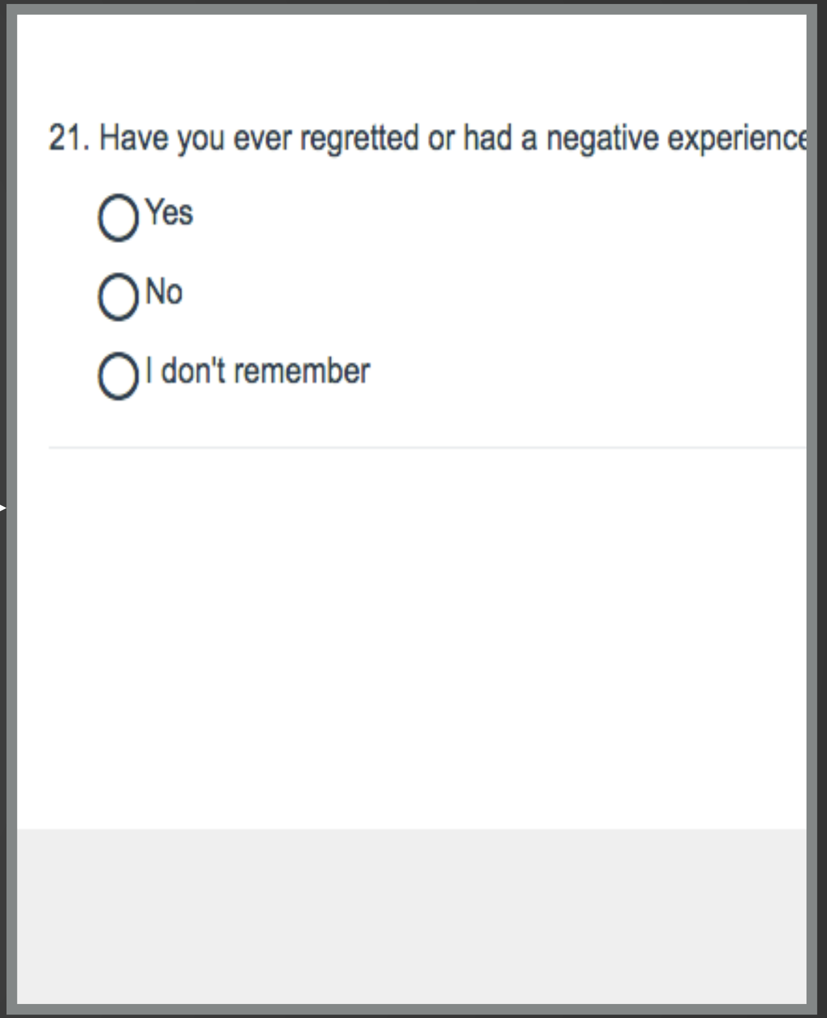
1 Open the Google Play Store App

2 Touch the menu icon

3

4

Part Two:
Update settings
& Preferences



21. Have you ever regretted or had a negative experience

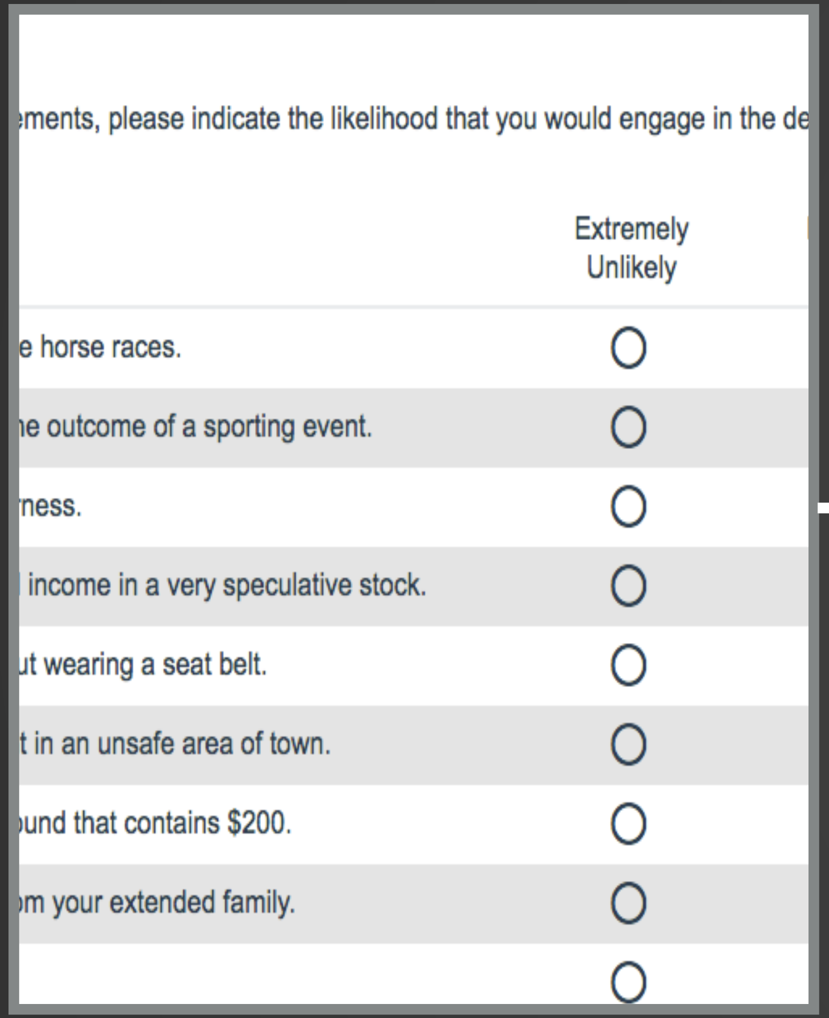
○ Yes

○ No

○ I don't remember

Part Three:
Past Update
Experiences

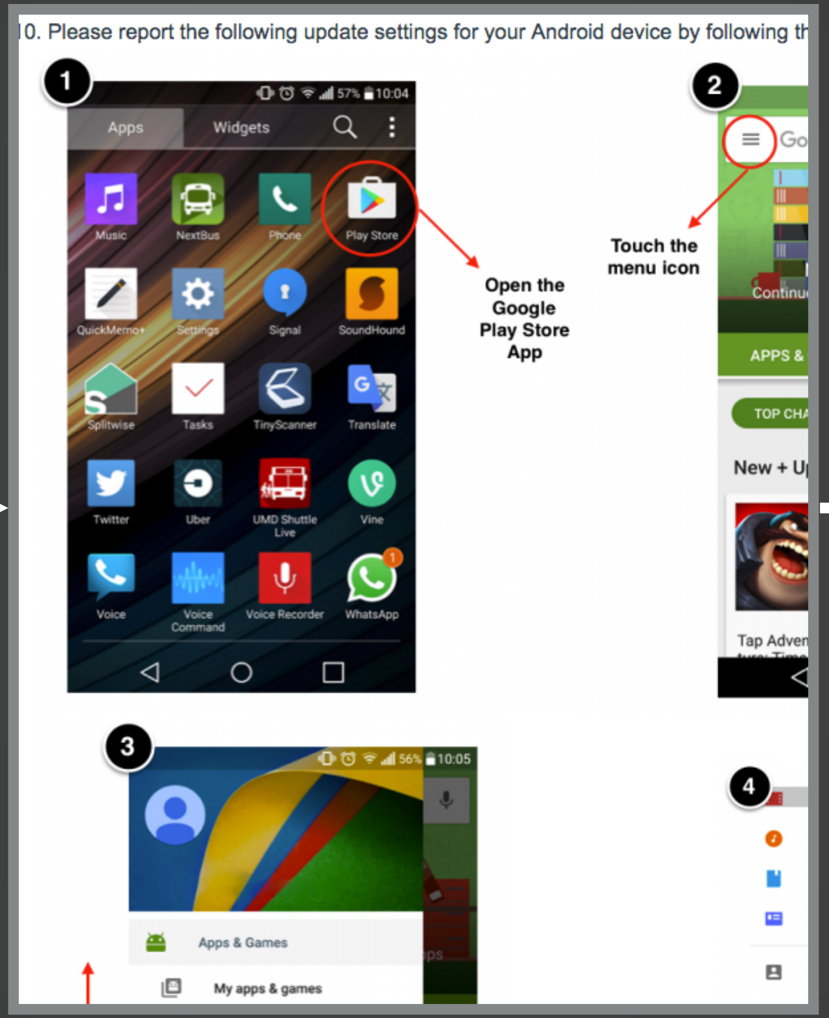
Survey



ments, please indicate the likelihood that you would engage in the de

	Extremely Unlikely
e horse races.	○
he outcome of a sporting event.	○
ness.	○
income in a very speculative stock.	○
ut wearing a seat belt.	○
t in an unsafe area of town.	○
und that contains $200.	○
m your extended family.	○
	○

Part One: Psychometric Scales



10. Please report the following update settings for your Android device by following th

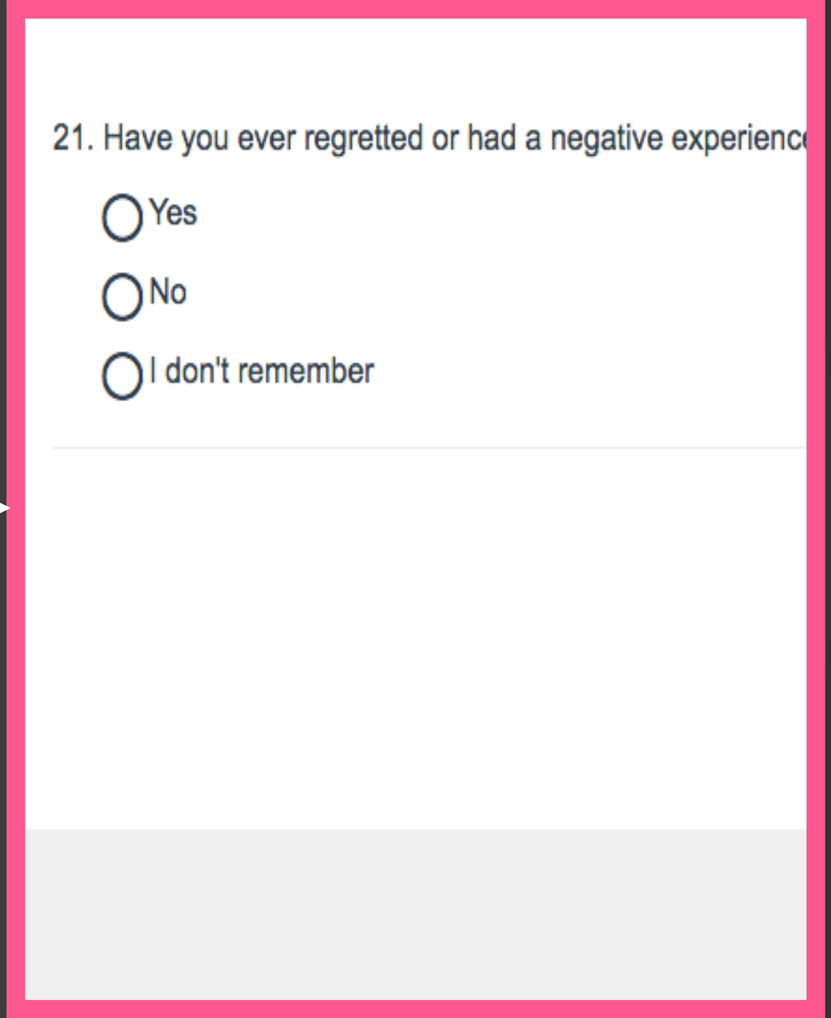
1 Open the Google Play Store App

2 Touch the menu icon

3

4

Part Two: Update settings & Preferences



21. Have you ever regretted or had a negative experienc

○ Yes

○ No

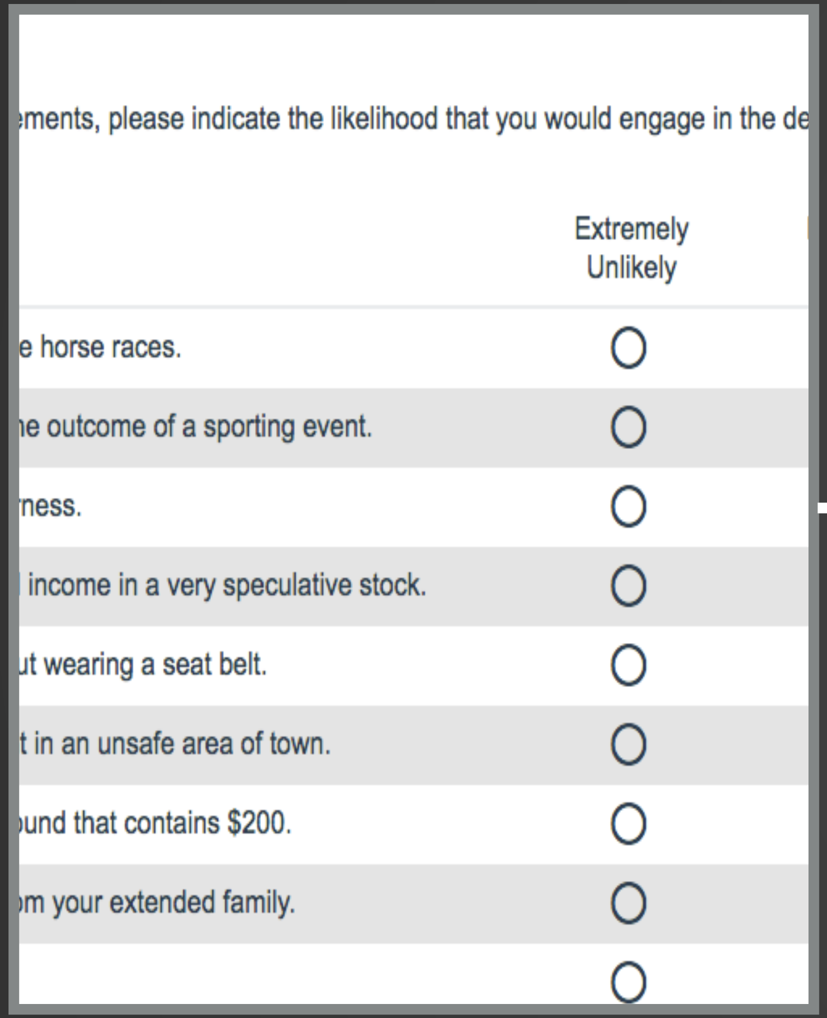
○ I don't remember

Part Three: Past Update Experiences

Survey: Part Three

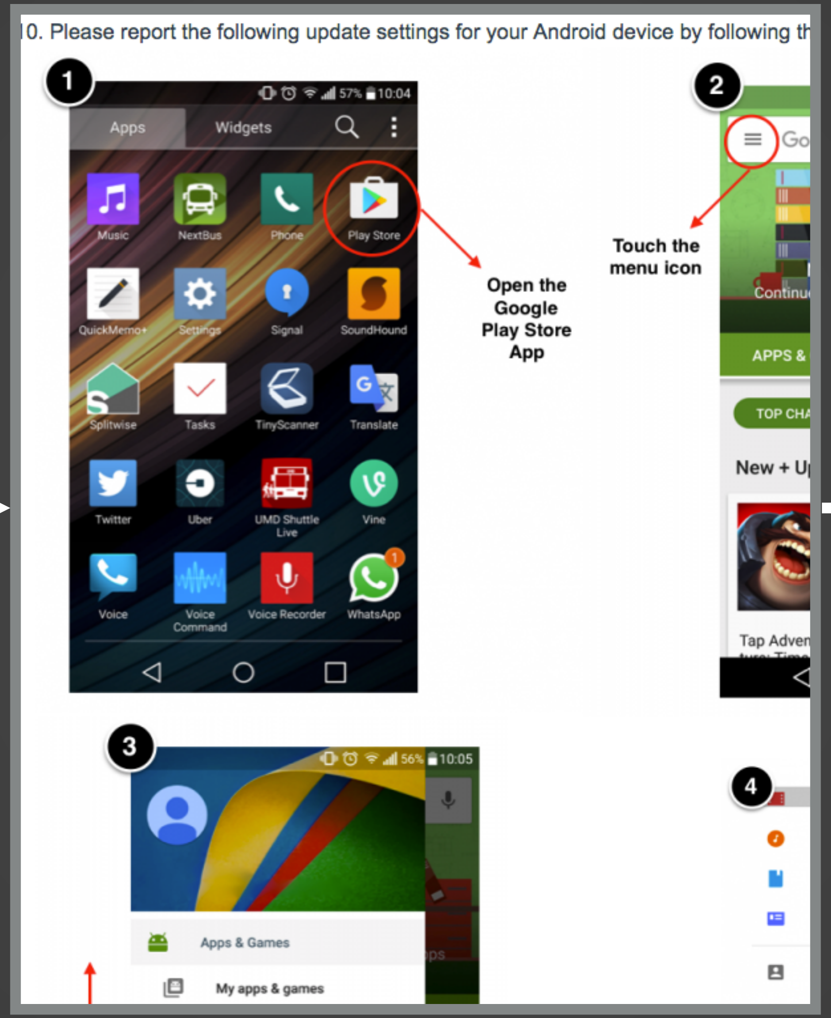
- Past Negative Software Updating Experience?
  - Across any device, software
- Demographics
  - Age, Gender, Education

Survey



ments, please indicate the likelihood that you would engage in the de

	Extremely Unlikely
e horse races.	○
ne outcome of a sporting event.	○
ness.	○
income in a very speculative stock.	○
ut wearing a seat belt.	○
t in an unsafe area of town.	○
und that contains $200.	○
m your extended family.	○
	○



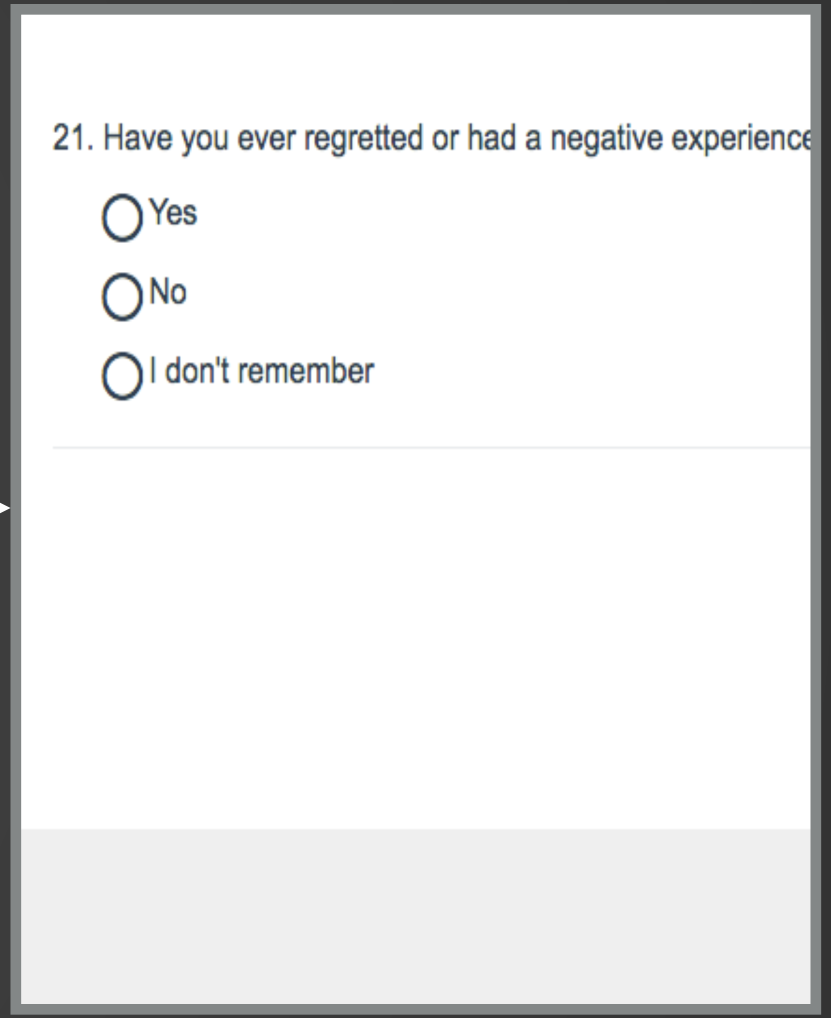
10. Please report the following update settings for your Android device by following th

1 Open the Google Play Store App

2 Touch the menu icon

3

4



21. Have you ever regretted or had a negative experience

○ Yes

○ No

○ I don't remember

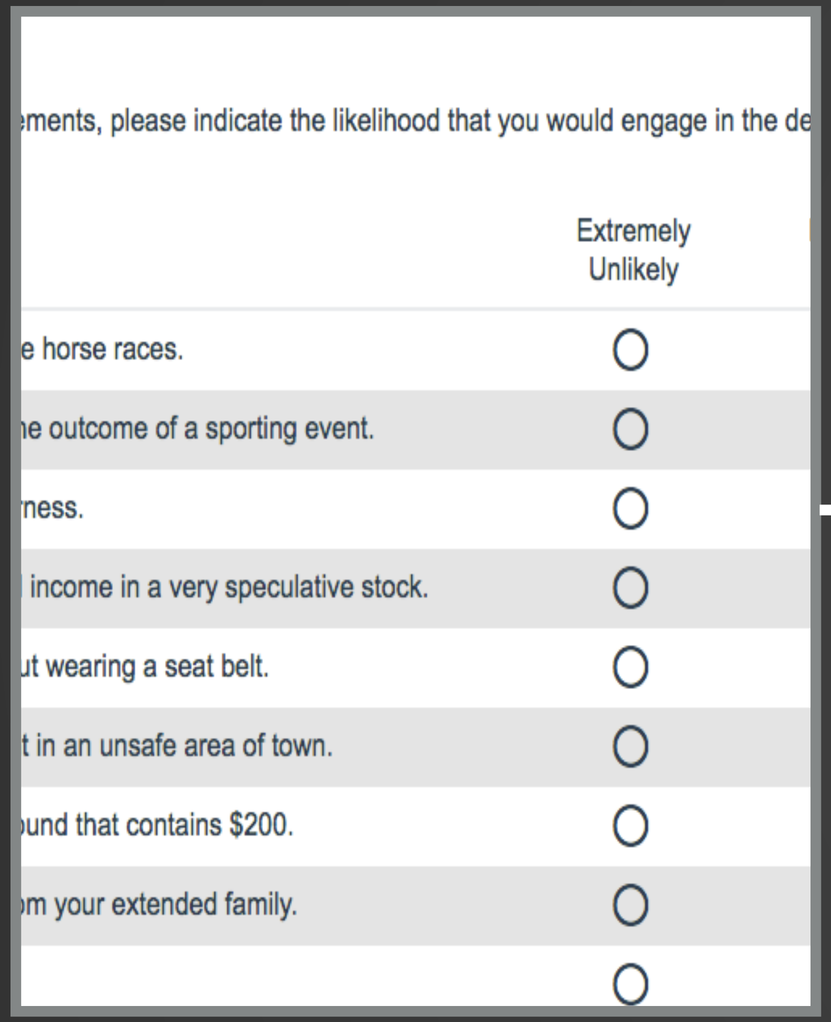
Part One: Psychometric Scales

Part Two: Update settings & Preferences

Part Three: Past Update Experiences

Survey

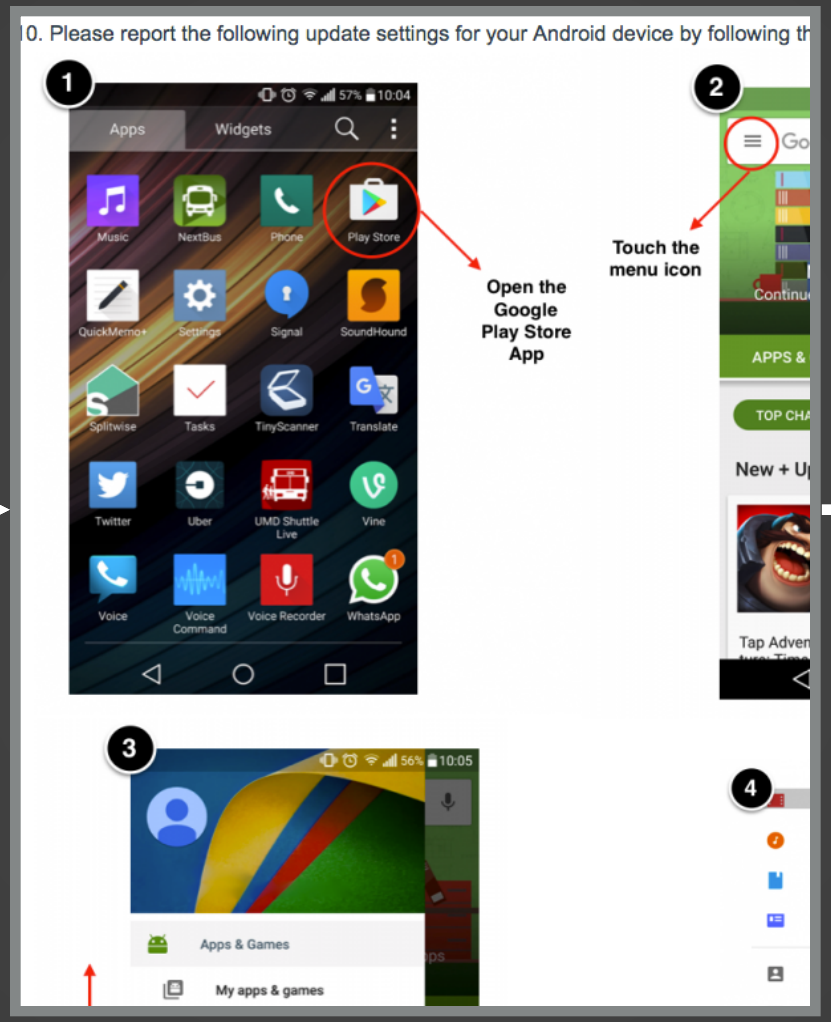
Always last



ments, please indicate the likelihood that you would engage in the de

	Extremely Unlikely
e horse races.	○
he outcome of a sporting event.	○
ness.	○
income in a very speculative stock.	○
ut wearing a seat belt.	○
t in an unsafe area of town.	○
und that contains $200.	○
m your extended family.	○
	○

Part One: Psychometric Scales



10. Please report the following update settings for your Android device by following th

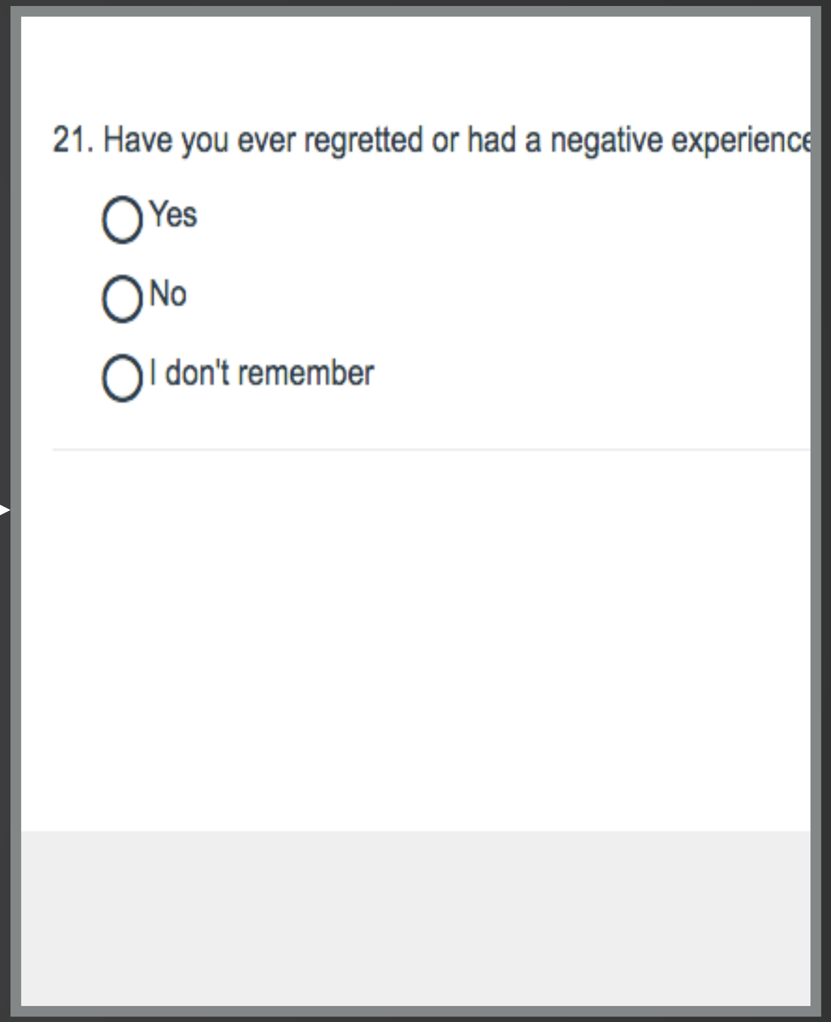
1 Open the Google Play Store App

2 Touch the menu icon

3

4

Part Two: Update settings & Preferences



21. Have you ever regretted or had a negative experience

○ Yes

○ No

○ I don't remember

Part Three: Past Update Experiences

Participants

- Recruited through Amazon Mechanical Turk
- N = 477
- Age: 69.2% between 18-34
- Gender: 62.3% Male

Participants

- Recruited through Amazon Mechanical Turk
- N = 477
- Age: 69.2% between 18-34
- Gender: 62.3% Male
- 67% Reported Auto-updating applications

Question *One*: What user characteristics differentiate those Android users who avoid auto-updates from those who do auto-update their applications?

Analysis: Logistic regression

- Dependent Variable: Auto-update or Not
- Independent Variables: User characteristics
  - Psychometric scales, SeBIS scores
  - Past Negative Experience with Software Updating
  - Demographics

Results

Outcome: Did not Auto-update

Predictor	Odds Ratio	Odds Ratio 95% C.I.	p-value
Negative Experience [Yes]	2.81	1.75, 4.56	< 0.0001
DoSpeRT–Investment	0.79	0.66, 0.94	< 0.01
DoSpeRT–Ethical	0.75	0.62, 0.91	< 0.01
SeBIS–Proactive Awareness	1.42	1.01, 2.01	0.04

Results

Outcome: Did not Auto-update

Predictor	Odds Ratio	Odds Ratio 95% C.I.	p-value
Negative Experience [Yes]	2.81	1.75, 4.56	< 0.0001

Avoiding Auto-updates is associated with Past Negative Experiences with Software updates.

Results

Negative Experience	Frequency
Version prior to update worked better	36.4%
The update introduced new bugs	34.3%
The update modified the user interface	27.6%
The update took a long time to install	11.3%
The update used up a lot of data	10.7%

Results

> P34: Windows 10, or garbage time, breaks pretty much every time it updates.
>
> P145: The update I downloaded made other apps buggy.
>
> P298: The iTunes update deleted my password and I could not get it back and it would not let me know what it was. I also lost all the music I had purchased.

Results

Outcome: Did not Auto-update

Predictor	Odds Ratio	Odds Ratio 95% C.I.	p-value
Negative Experience [Yes]	2.81	1.75, 4.56	< 0.0001
DoSpeRT–Investment	0.79	0.66, 0.94	< 0.01
DoSpeRT–Ethical	0.75	0.62, 0.91	< 0.01
SeBIS–Proactive Awareness	1.42	1.01, 2.01	0.04

Results

Outcome: Did not Auto-update

Predictor	Odds Ratio	Odds Ratio 95% C.I.	p-value
DoSpeRT–Investment	0.79	0.66, 0.94	< 0.01
DoSpeRT–Ethical	0.75	0.62, 0.91	< 0.01

Avoiding Auto-updates is associated with Lower Risk Taking Behavior.

Results

Outcome: Did not Auto-update

Predictor	Odds Ratio	Odds Ratio 95% C.I.	p-value
SeBIS–Proactive Awareness	1.42	1.01, 2.01	0.04

Avoiding Auto-updates is associated with Greater Proactive Security Behavior.

Question *Two*: What user characteristics explain Android users’ preferences towards auto-updating their applications?

Analysis: Linear Mixed Effects Model

- Dependent Variable: Comfort Score
- Independent Variables: User characteristics
  - Psychometric scales, SeBIS scores
  - Past Negative Experience with Software Updating
  - Demographics
  - Importance, Trust, Frequency of Use, Satisfaction

Analysis: Linear Mixed Effects Model

Participants, Applications were Random Factors.

- Dependent Variable: Comfort Score
- Independent Variables: User characteristics
  - Psychometric scales, SeBIS scores
  - Past Negative Experience with Software Updating
  - Demographics
  - Importance, Trust, Frequency of Use, Satisfaction

Results

Outcome: Comfort Score with Auto-updating

Predictor	Estimate	Estimate 95% C.I.	p-value
Negative Experience [Yes]	–7.39	–11.49, –3.29	< 0.001
Update Type [Security]	6.76	6.03, 7.49	< 0.0001
Trust	7.29	6.61, 7.96	< 0.0001

Results

Outcome: Comfort Score with Auto-updating

Predictor	Estimate	Estimate 95% C.I.	p-value
Negative Experience [Yes]	–7.39	–11.49, –3.29	< 0.001

Past Negative Experience with Software Updates made Auto-updating Less Comfortable.

Results

Outcome: Comfort Score with Auto-updating

Predictor	Estimate	Estimate 95% C.I.	p-value
Update Type [Security]	6.76	6.03, 7.49	< 0.0001

Security Updates Made Auto-updating More Comfortable.

Results

Outcome: Comfort Score with Auto-updating

Predictor	Estimate	Estimate 95% C.I.	p-value
Trust	7.29	6.61, 7.96	< 0.0001

Trust in Application Made Auto-updating More Comfortable.

Implication #1

- Improve Auto-update Interfaces: Make Update Rollbacks/Recovery More Accessible
    - May increase confidence in auto-updating
- Open Questions:
    - Security vs Non-security updates
    - Inform users about effects of rollback
    - Rollback until when?

Implication #2

- Examine Update Development Practices:
  - Beyond end-users: How do software developers decide, build and test updates?
  - How do these practices lead to negative experiences for end-users?

Implication #3

- Improve Auto-update Interfaces: Design and evaluate messaging using risk-taking traits
  - Financial risk: “*Not switching auto-updates on for security updates increases the chances of someone gaining access to your bank account or stealing your credit card information*”
- Open Questions:
  - Medium, timing of messages & evaluation

Implication #4

- Personalize Mobile Auto-update Systems:
  - Use Trust and Security updates as factors to decide which applications to auto-update
- Open Questions:
  - What are some proxies for trust in an application, and can these be inferred?

IMPACT OF USER CHARACTERISTICS ON ATTITUDES TOWARDS AUTOMATIC ANDROID APPLICATION UPDATES

Arunesh Mathur

@aruneshmathur

http://aruneshmathur.co.in

PRINCETON UNIVERSITY

CITP
CENTER FOR INFORMATION TECHNOLOGY POLICY
AT PRINCETON UNIVERSITY

UNIVERSITY OF MARYLAND