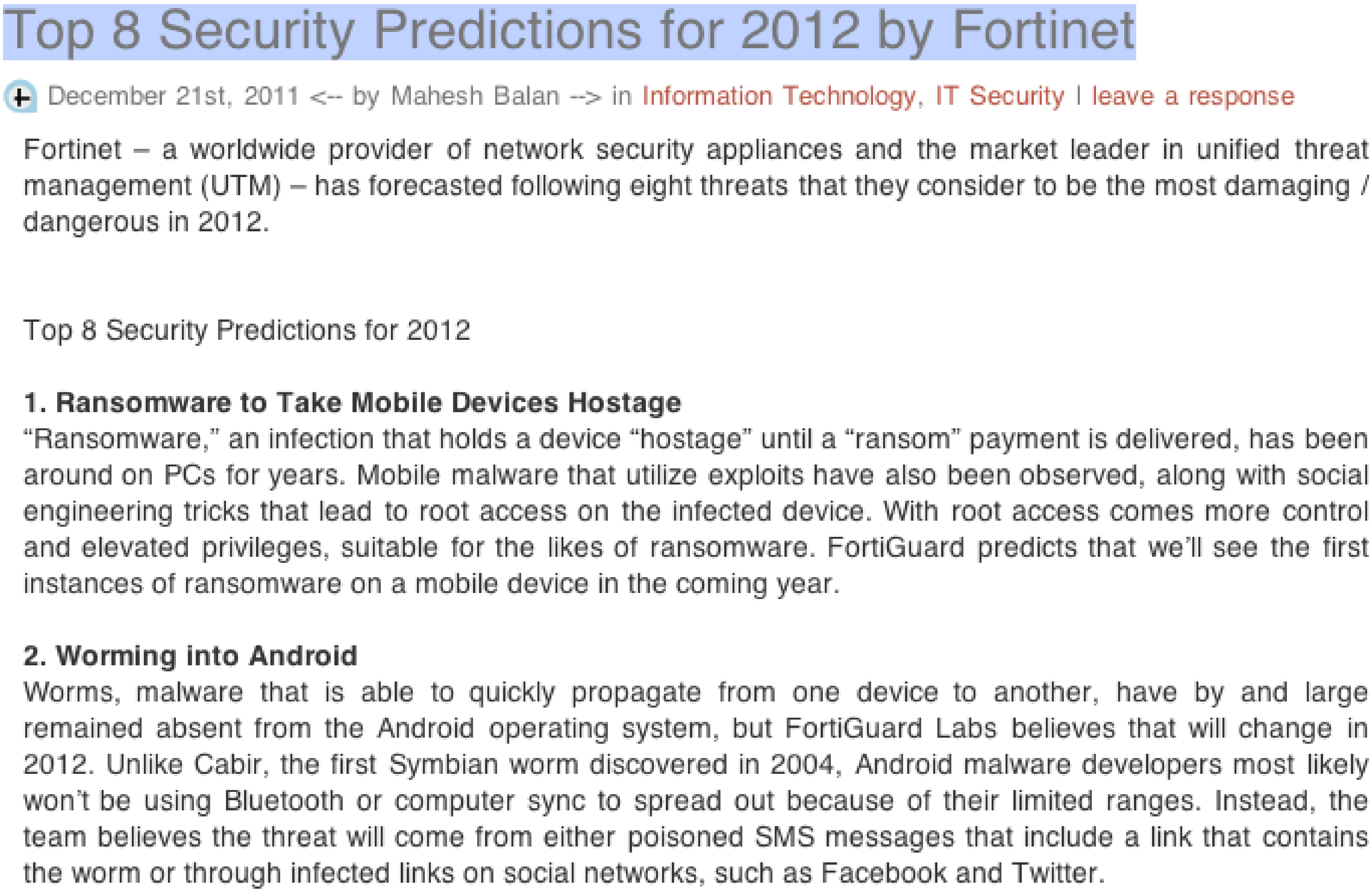
software pilots
TRIFORK.

Sikre apps på iOS og Android

Mads Jensen & Søren Toft
@ArbitraryJensen & @SorenToft

"Next vulnerability shift will go from WebApp to Mobile. It'll take at least another 5-7yrs though."

Jeremiah Grossman



Top 8 Security Predictions for 2012 by Fortinet

December 21st, 2011 <-- by Mahesh Balan --> in Information Technology, IT Security | leave a response

Fortinet – a worldwide provider of network security appliances and the market leader in unified threat management (UTM) – has forecasted following eight threats that they consider to be the most damaging / dangerous in 2012.

Top 8 Security Predictions for 2012

1. Ransomware to Take Mobile Devices Hostage
"Ransomware," an infection that holds a device "hostage" until a "ransom" payment is delivered, has been around on PCs for years. Mobile malware that utilize exploits have also been observed, along with social engineering tricks that lead to root access on the infected device. With root access comes more control and elevated privileges, suitable for the likes of ransomware. FortiGuard predicts that we'll see the first instances of ransomware on a mobile device in the coming year.

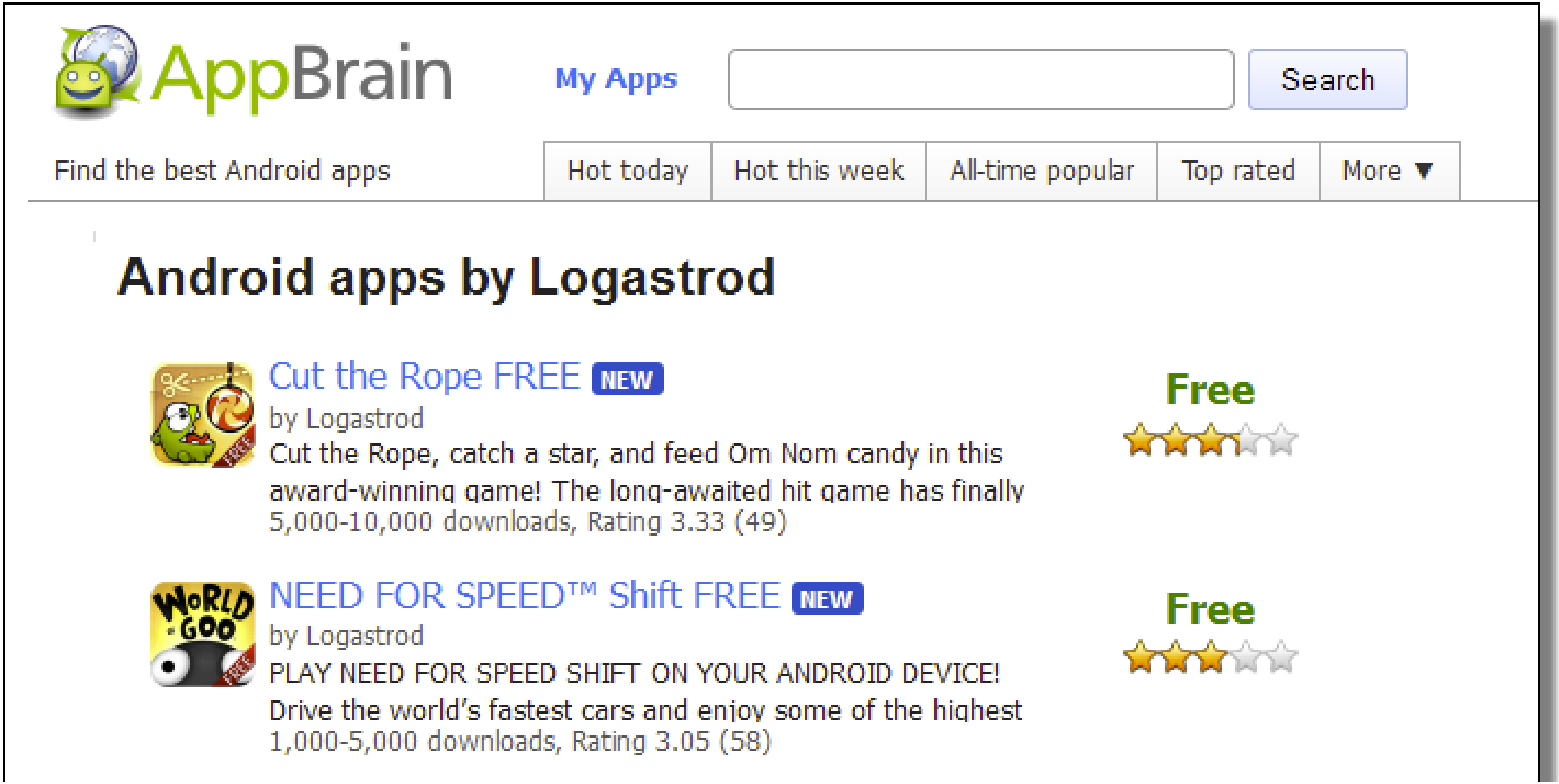
2. Worming into Android
Worms, malware that is able to quickly propagate from one device to another, have by and large remained absent from the Android operating system, but FortiGuard Labs believes that will change in 2012. Unlike Cabir, the first Symbian worm discovered in 2004, Android malware developers most likely won't be using Bluetooth or computer sync to spread out because of their limited ranges. Instead, the team believes the threat will come from either poisoned SMS messages that include a link that contains the worm or through infected links on social networks, such as Facebook and Twitter.

Premium Rate SMS Trojans in Google's Android Market

Posted by Sean @ 15:33 GMT | Comments

Premium rate SMS trojans were discovered in Google's Android Market earlier today.

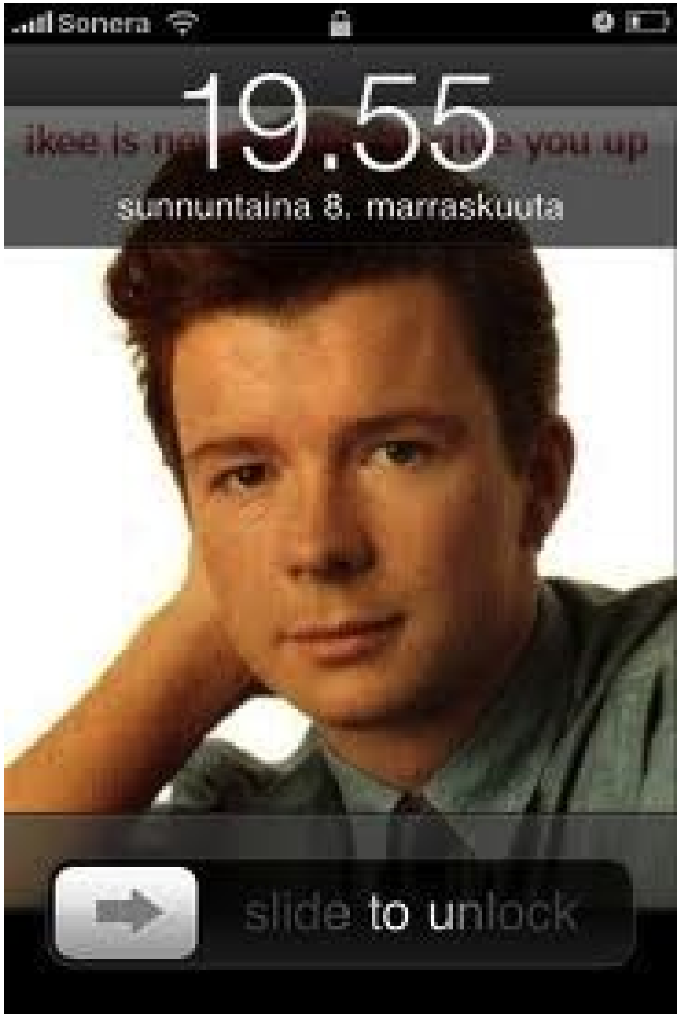
The developer, named "Logastrod", offered supposed free versions of many popular applications. And while Google has shut down the official market account, sites such as AppBrain still list the downloads.

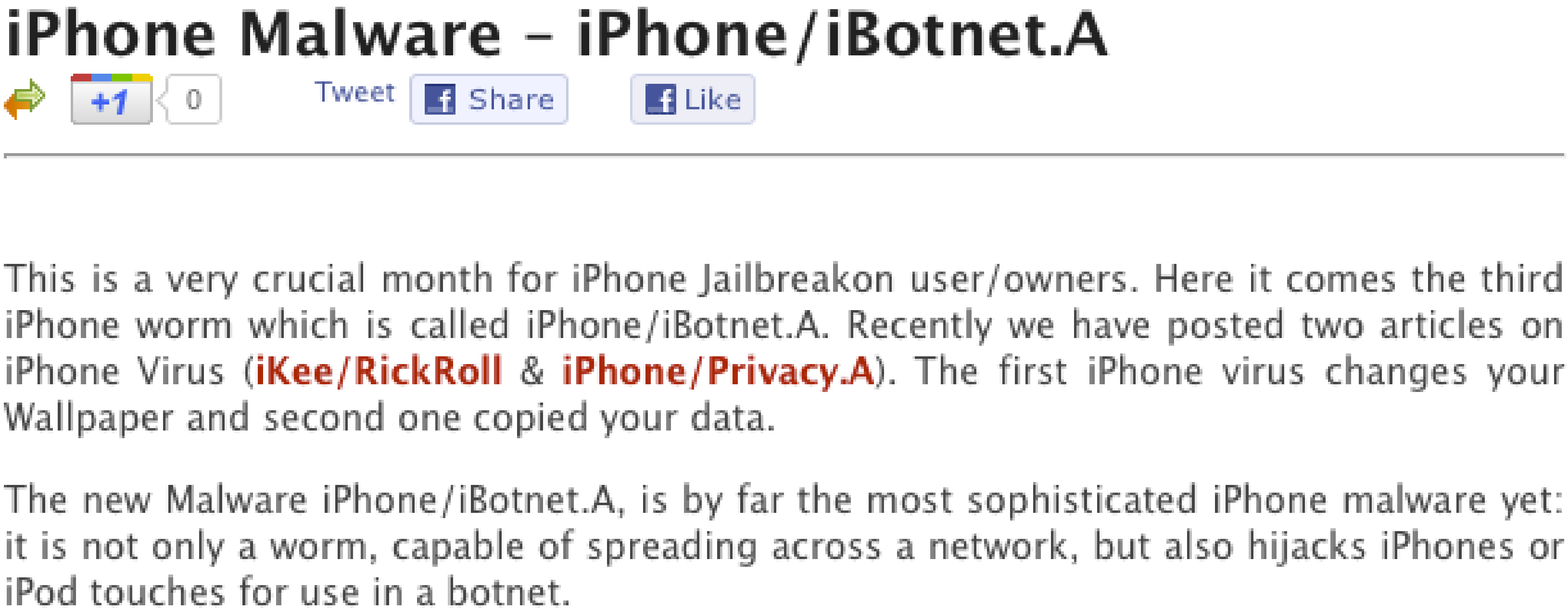


Android apps by Logastrod

Cut the Rope FREE NEW
by Logastrod
Cut the Rope, catch a star, and feed Om Nom candy in this award-winning game! The long-awaited hit game has finally
5,000-10,000 downloads, Rating 3.33 (49)
Free

NEED FOR SPEED™ Shift FREE NEW
by Logastrod
PLAY NEED FOR SPEED SHIFT ON YOUR ANDROID DEVICE! Drive the world's fastest cars and enjoy some of the highest
1,000-5,000 downloads, Rating 3.05 (58)
Free

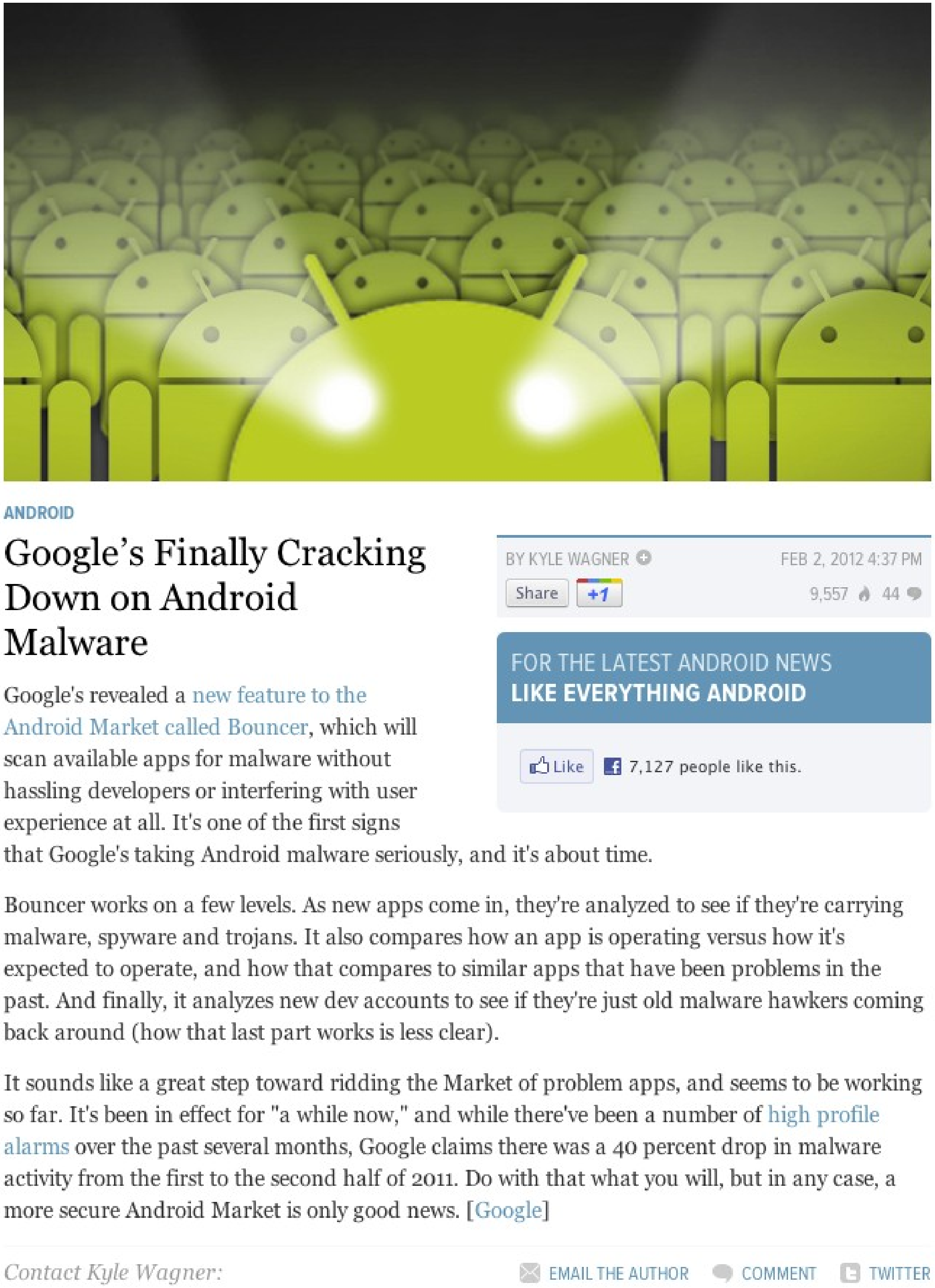

Sonera
19.55
ikee is ne
e you up
sunnuntaina 8. marraskuuta
slide to unlock



iPhone Malware – iPhone/iBotnet.A

This is a very crucial month for iPhone Jailbreakon user/owners. Here it comes the third iPhone worm which is called iPhone/iBotnet.A. Recently we have posted two articles on iPhone Virus (**iKee/RickRoll** & **iPhone/Privacy.A**). The first iPhone virus changes your Wallpaper and second one copied your data.

The new Malware iPhone/iBotnet.A, is by far the most sophisticated iPhone malware yet: it is not only a worm, capable of spreading across a network, but also hijacks iPhones or iPod touches for use in a botnet.



ANDROID

Google's Finally Cracking Down on Android Malware

BY KYLE WAGNER ⊕ FEB 2, 2012 4:37 PM

Share +1 9,557 44

FOR THE LATEST ANDROID NEWS
LIKE EVERYTHING ANDROID

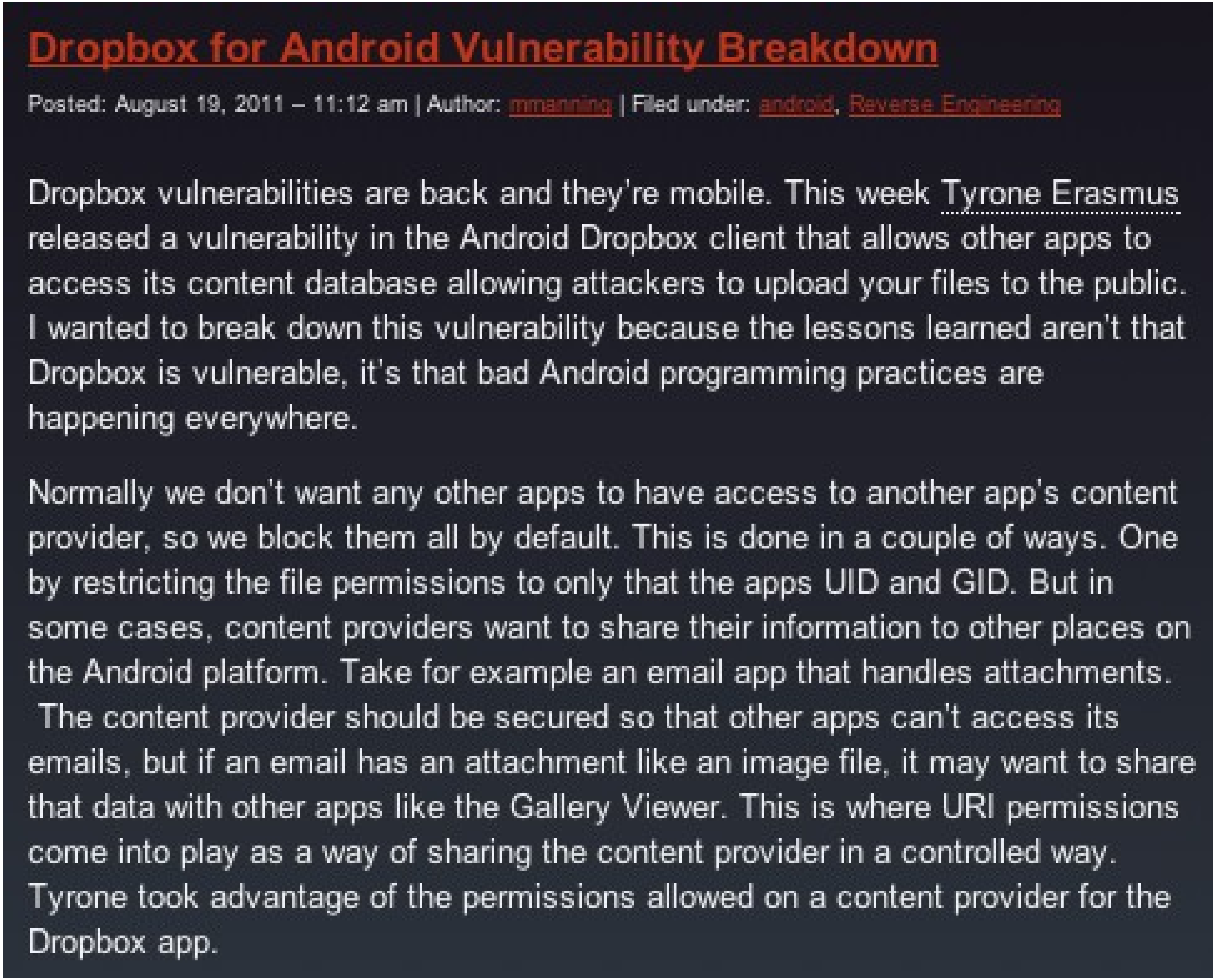
Like 7,127 people like this.

Google's revealed a new feature to the Android Market called Bouncer, which will scan available apps for malware without hassling developers or interfering with user experience at all. It's one of the first signs that Google's taking Android malware seriously, and it's about time.

Bouncer works on a few levels. As new apps come in, they're analyzed to see if they're carrying malware, spyware and trojans. It also compares how an app is operating versus how it's expected to operate, and how that compares to similar apps that have been problems in the past. And finally, it analyzes new dev accounts to see if they're just old malware hawkers coming back around (how that last part works is less clear).

It sounds like a great step toward ridding the Market of problem apps, and seems to be working so far. It's been in effect for "a while now," and while there've been a number of high profile alarms over the past several months, Google claims there was a 40 percent drop in malware activity from the first to the second half of 2011. Do with that what you will, but in any case, a more secure Android Market is only good news. [Google]

Contact Kyle Wagner: EMAIL THE AUTHOR COMMENT TWITTER

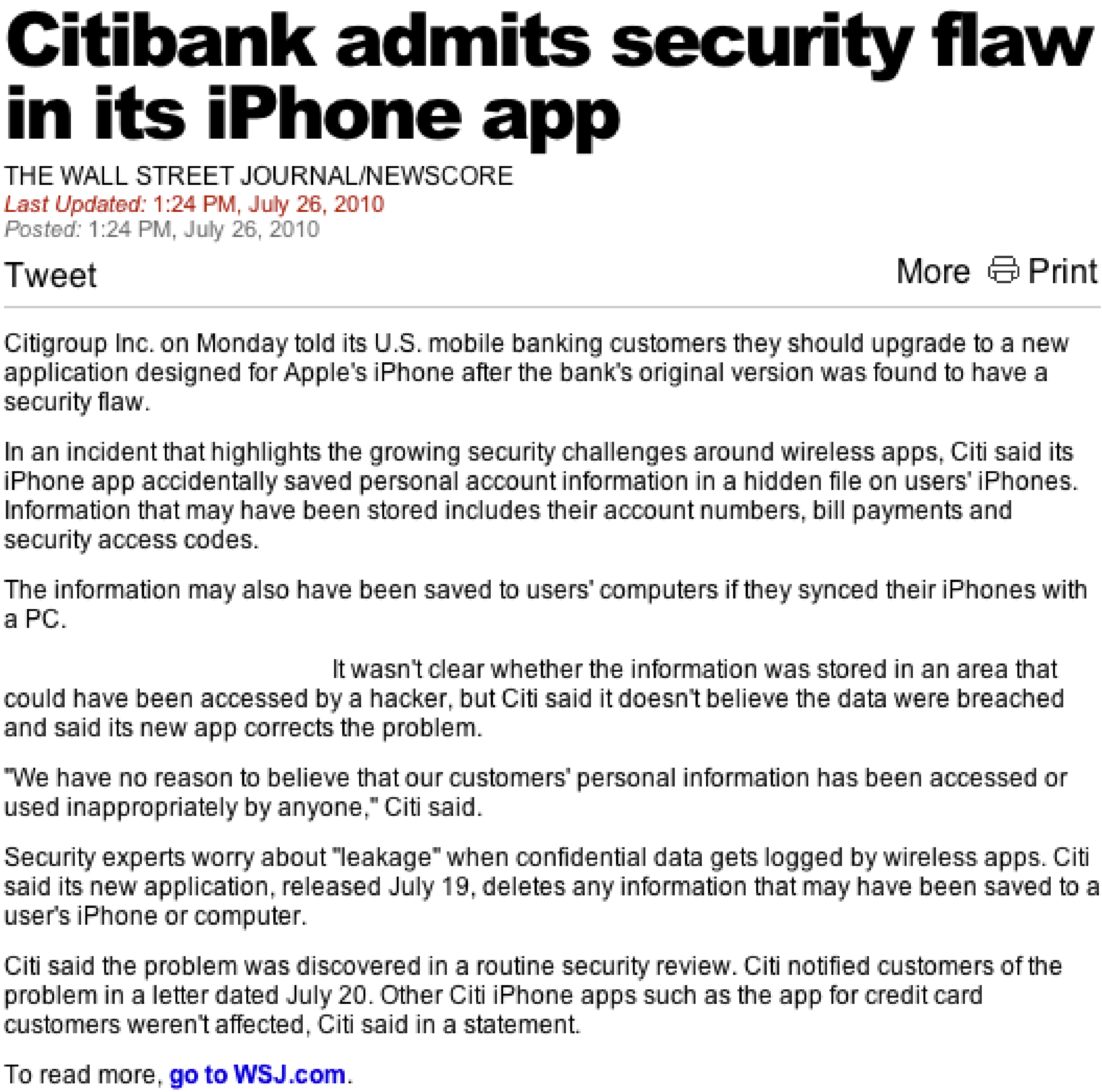


Dropbox for Android Vulnerability Breakdown

Posted: August 19, 2011 – 11:12 am | Author: mmanning | Filed under: android, Reverse Engineering

Dropbox vulnerabilities are back and they're mobile. This week Tyrone Erasmus released a vulnerability in the Android Dropbox client that allows other apps to access its content database allowing attackers to upload your files to the public. I wanted to break down this vulnerability because the lessons learned aren't that Dropbox is vulnerable, it's that bad Android programming practices are happening everywhere.

Normally we don't want any other apps to have access to another app's content provider, so we block them all by default. This is done in a couple of ways. One by restricting the file permissions to only that the apps UID and GID. But in some cases, content providers want to share their information to other places on the Android platform. Take for example an email app that handles attachments. The content provider should be secured so that other apps can't access its emails, but if an email has an attachment like an image file, it may want to share that data with other apps like the Gallery Viewer. This is where URI permissions come into play as a way of sharing the content provider in a controlled way. Tyrone took advantage of the permissions allowed on a content provider for the Dropbox app.



Citibank admits security flaw in its iPhone app

THE WALL STREET JOURNAL/NEWSCORE

Last Updated: 1:24 PM, July 26, 2010

Posted: 1:24 PM, July 26, 2010

Citigroup Inc. on Monday told its U.S. mobile banking customers they should upgrade to a new application designed for Apple's iPhone after the bank's original version was found to have a security flaw.

In an incident that highlights the growing security challenges around wireless apps, Citi said its iPhone app accidentally saved personal account information in a hidden file on users' iPhones. Information that may have been stored includes their account numbers, bill payments and security access codes.

The information may also have been saved to users' computers if they synced their iPhones with a PC.

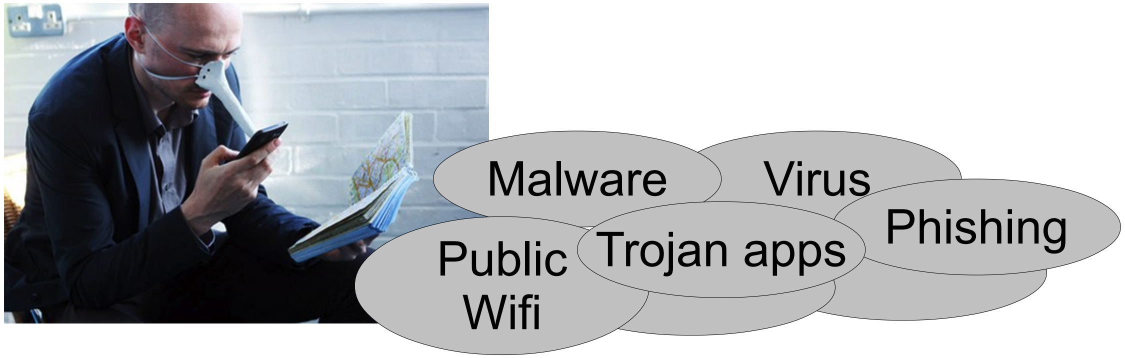
It wasn't clear whether the information was stored in an area that could have been accessed by a hacker, but Citi said it doesn't believe the data were breached and said its new app corrects the problem.

"We have no reason to believe that our customers' personal information has been accessed or used inappropriately by anyone," Citi said.

Security experts worry about "leakage" when confidential data gets logged by wireless apps. Citi said its new application, released July 19, deletes any information that may have been saved to a user's iPhone or computer.

Citi said the problem was discovered in a routine security review. Citi notified customers of the problem in a letter dated July 20. Other Citi iPhone apps such as the app for credit card customers weren't affected, Citi said in a statement.

To read more, **go to WSJ.com**.



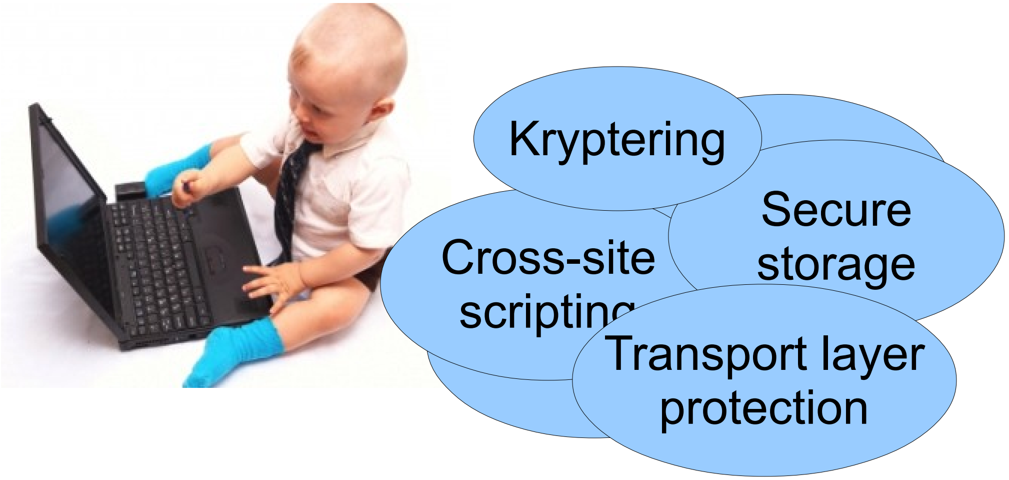
Malware

Virus

Phishing

Public Wifi

Trojan apps

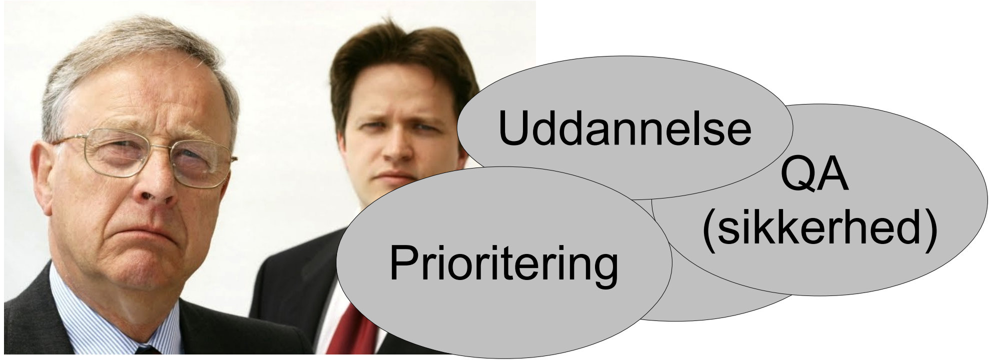


Kryptering

Secure storage

Cross-site scripting

Transport layer protection



Uddannelse

QA (sikkerhed)

Prioritering

DANMA

KOMPUTER

2·2012

PRIS: 71,95

WWW.KOMPUTER.DK

DE BEDSTE TIPS OM SIKKERHED

FØLG 22 ENKLE RÅD OG FÅ DEN SIKRESTE PC NOGENSINDE!

Side 48

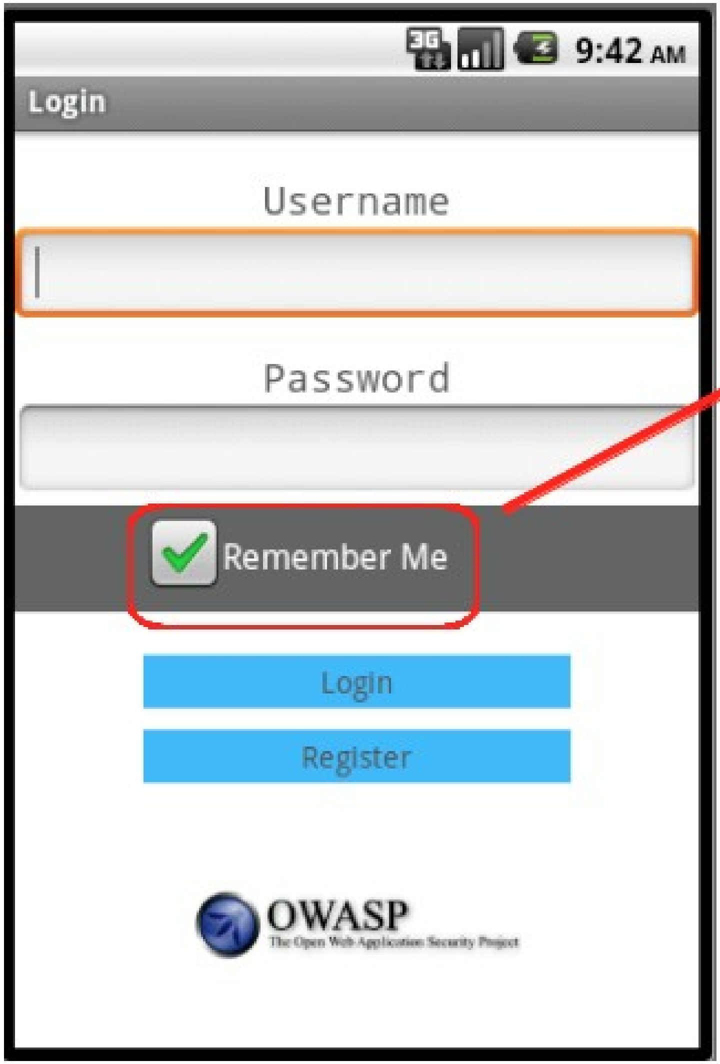
KOMPUTER

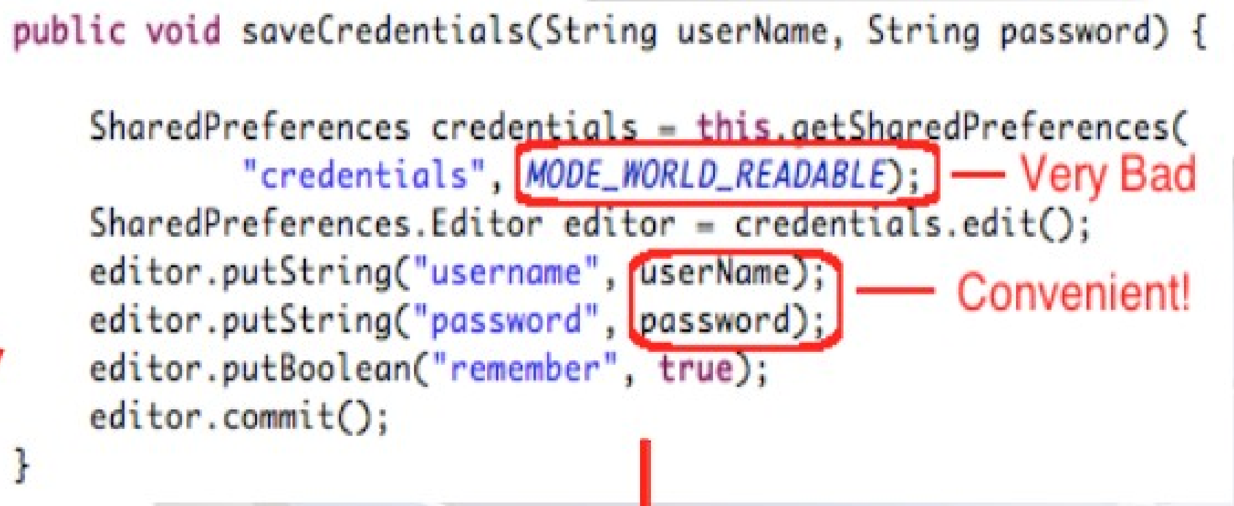
OWASP – Top 10 mobile risks

(release candidate v. 1.0)

1. Insecure Data Storage
2. Weak Server Side Controls
3. Insufficient Transport Layer Protection
4. Client Side Injection
5. Poor Authorization and Authentication
6. Improper Session Handling
7. Security Decisions Via Untrusted Inputs
8. Side Channel Data Leakage
9. Broken Cryptography
10. Sensitive Information Disclosure

1 Insecure data storage





```
public void saveCredentials(String userName, String password) {

    SharedPreferences credentials = this.getSharedPreferences(
            "credentials", MODE_WORLD_READABLE);
    SharedPreferences.Editor editor = credentials.edit();
    editor.putString("username", userName);
    editor.putString("password", password);
    editor.putBoolean("remember", true);
    editor.commit();
}
```

Very Bad

Convenient!

```
[myData writeToURL: location options:
NSDataWritingFileProtectionComplete error:
&error];
```

Gem ikke steder hvor andre kan læse enten implicit eller eksplicit.

- **Android**:
  - SD kort
  - Context.MODE_WORLD_READABLE
- **IOS**:
  - ~/Documents
  - ~/Library/Preferences
  - ~/Library/Application Support

Krypter data

- På disk
- I hukommelsen
- Hvor gemmes nøglen?

Overvej (ikke at bruge) key-chain

Skriv til app'ens SQLLite database

Skriv til enhedens interne lager og husk
Context.MODE_PRIVATE

Hvis i absolut behøver at gemme på SD
kortet så krypter data.

HUSK IKKE AT GEMME NØGLEN PÅ SD KORTET!!!

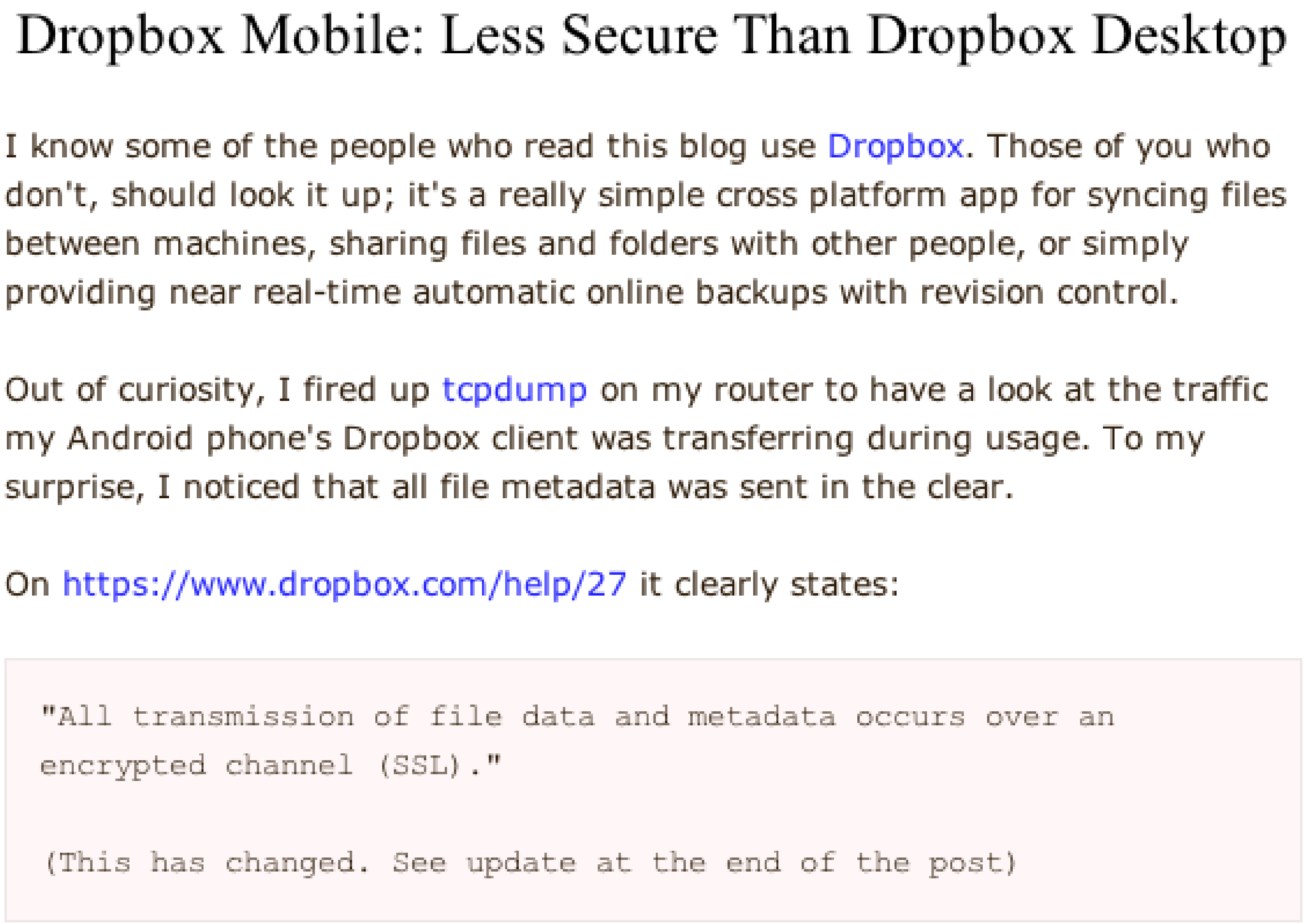
MEN overvej om i kan undvære at gemme data på enheden

2 Weak server side controls

....ikke så meget er ændret

3

Insufficient Transport Layer Protection



Dropbox Mobile: Less Secure Than Dropbox Desktop

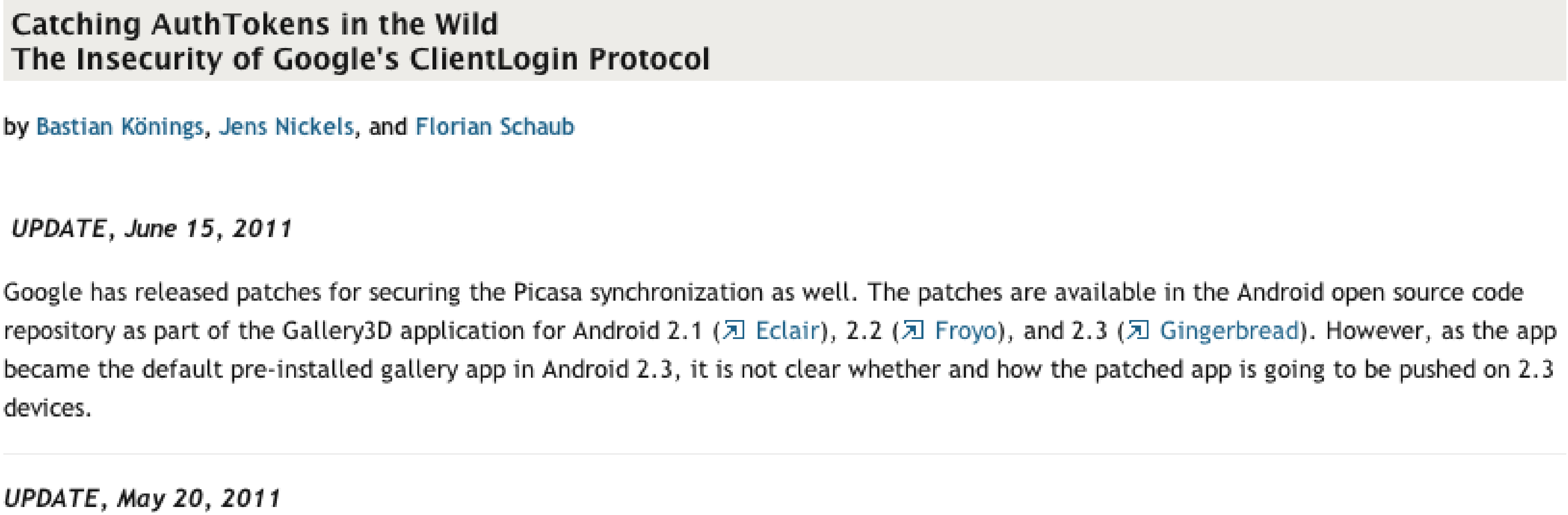
I know some of the people who read this blog use Dropbox. Those of you who don't, should look it up; it's a really simple cross platform app for syncing files between machines, sharing files and folders with other people, or simply providing near real-time automatic online backups with revision control.

Out of curiosity, I fired up tcpdump on my router to have a look at the traffic my Android phone's Dropbox client was transferring during usage. To my surprise, I noticed that all file metadata was sent in the clear.

On https://www.dropbox.com/help/27 it clearly states:

```
"All transmission of file data and metadata occurs over an
encrypted channel (SSL)."

(This has changed. See update at the end of the post)
```



Catching AuthTokens in the Wild
The Insecurity of Google's ClientLogin Protocol

by Bastian Könings, Jens Nickels, and Florian Schaub

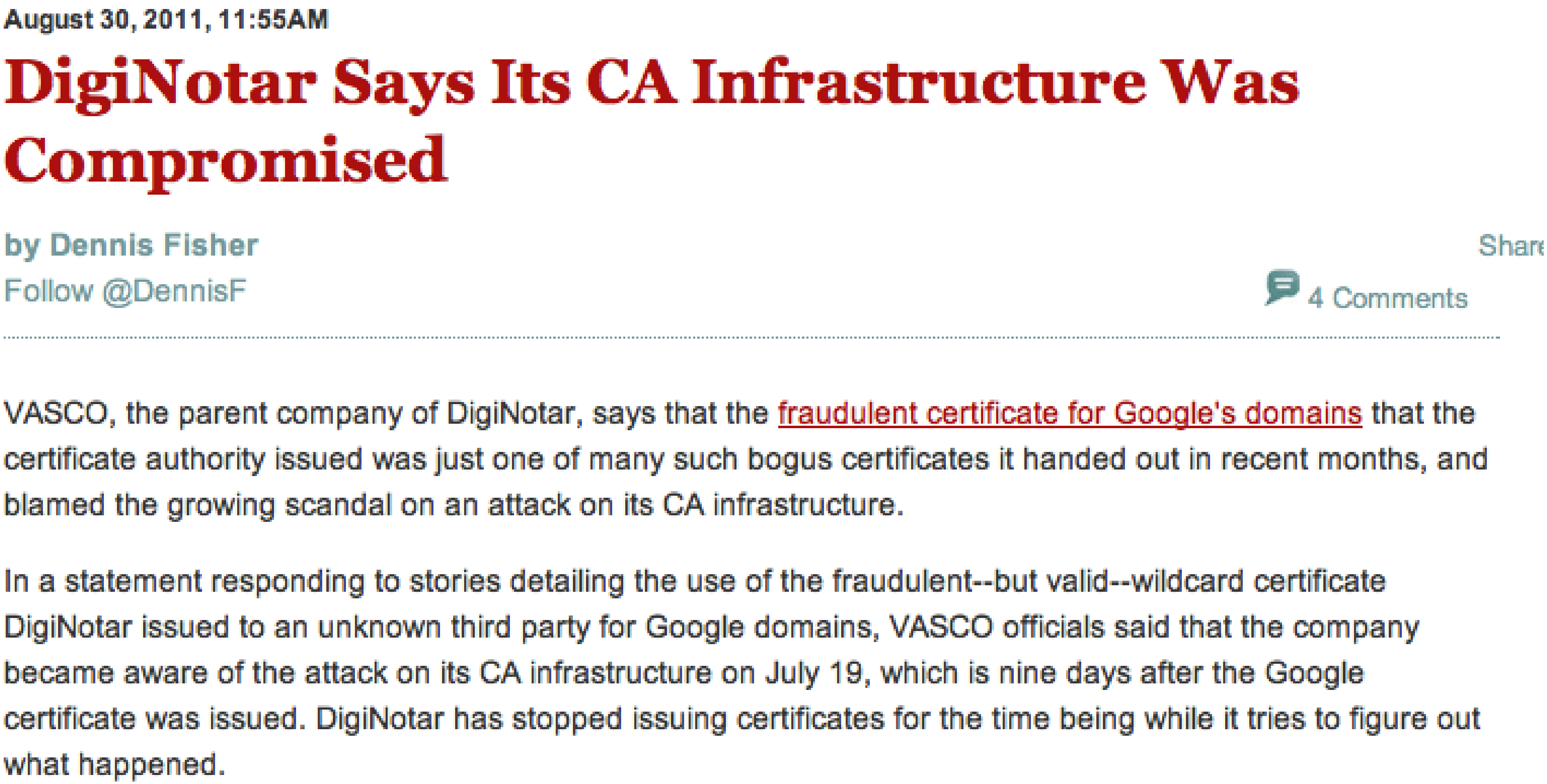
UPDATE, June 15, 2011

Google has released patches for securing the Picasa synchronization as well. The patches are available in the Android open source code repository as part of the Gallery3D application for Android 2.1 (↗ Eclair), 2.2 (↗ Froyo), and 2.3 (↗ Gingerbread). However, as the app became the default pre-installed gallery app in Android 2.3, it is not clear whether and how the patched app is going to be pushed on 2.3 devices.

UPDATE, May 20, 2011

- Hvis i har følsomme data så husk https:// frem for http.
- Endnu bedre brug https på alt.

“Vi benytter https og trust mod en kendt CA – er det så godt nok?”



August 30, 2011, 11:55AM

DigiNotar Says Its CA Infrastructure Was Compromised

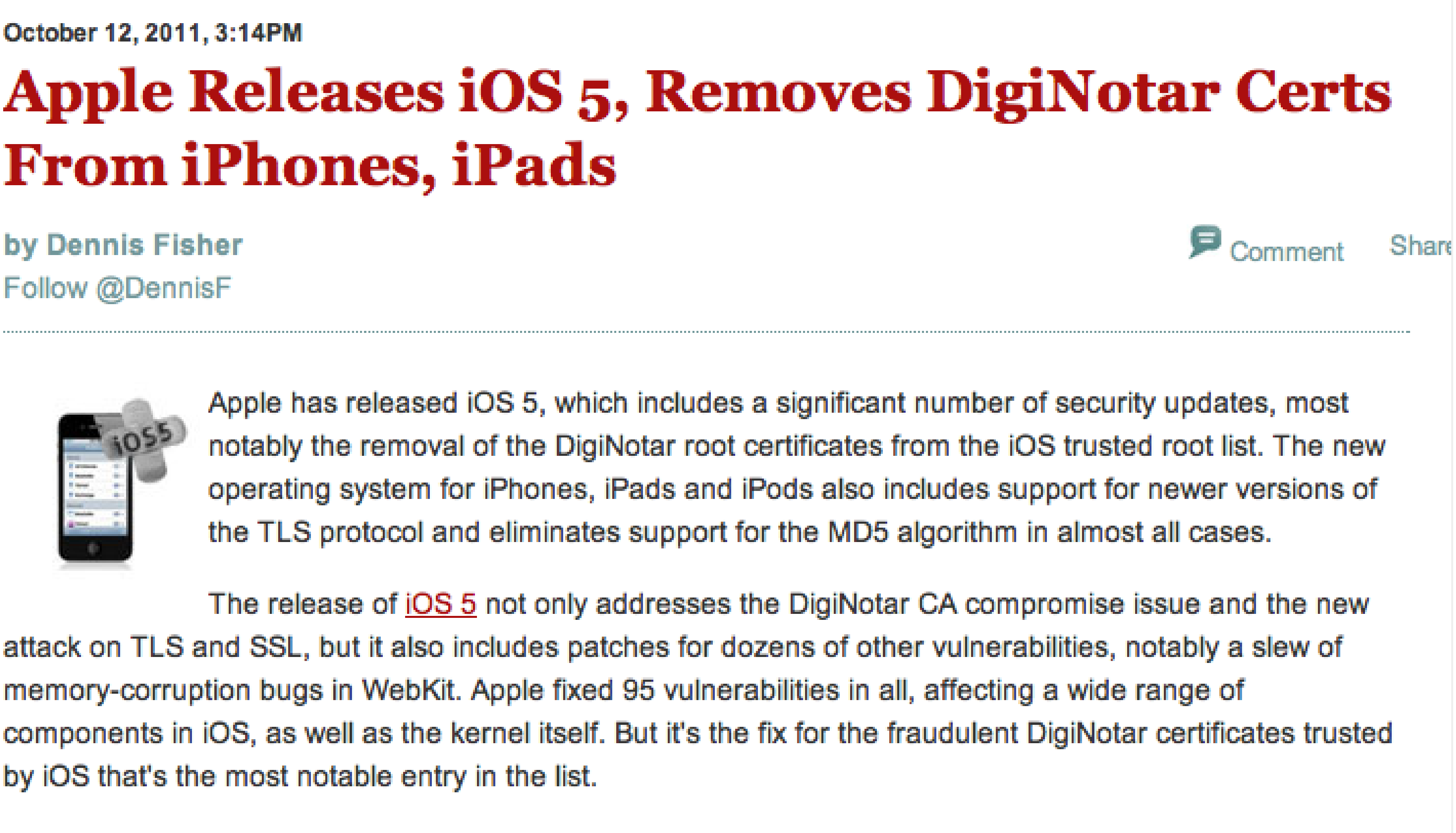
by Dennis Fisher
Follow @DennisF

Shar

4 Comments

VASCO, the parent company of DigiNotar, says that the fraudulent certificate for Google's domains that the certificate authority issued was just one of many such bogus certificates it handed out in recent months, and blamed the growing scandal on an attack on its CA infrastructure.

In a statement responding to stories detailing the use of the fraudulent--but valid--wildcard certificate DigiNotar issued to an unknown third party for Google domains, VASCO officials said that the company became aware of the attack on its CA infrastructure on July 19, which is nine days after the Google certificate was issued. DigiNotar has stopped issuing certificates for the time being while it tries to figure out what happened.



October 12, 2011, 3:14PM

Apple Releases iOS 5, Removes DigiNotar Certs From iPhones, iPads

by Dennis Fisher
Follow @DennisF

Apple has released iOS 5, which includes a significant number of security updates, most notably the removal of the DigiNotar root certificates from the iOS trusted root list. The new operating system for iPhones, iPads and iPods also includes support for newer versions of the TLS protocol and eliminates support for the MD5 algorithm in almost all cases.

The release of iOS 5 not only addresses the DigiNotar CA compromise issue and the new attack on TLS and SSL, but it also includes patches for dozens of other vulnerabilities, notably a slew of memory-corruption bugs in WebKit. Apple fixed 95 vulnerabilities in all, affecting a wide range of components in iOS, as well as the kernel itself. But it's the fix for the fraudulent DigiNotar certificates trusted by iOS that's the most notable entry in the list.

Stærk kryptering er ikke nok

- Validér certifikater
- ...og hvis forbindelsen ikke kan valideres?

Pas på med at validere mod telefonens trust

SSL pinning

- Option 1: Stol ikke på nogen CA

- Option 2: Stol kun på een CA

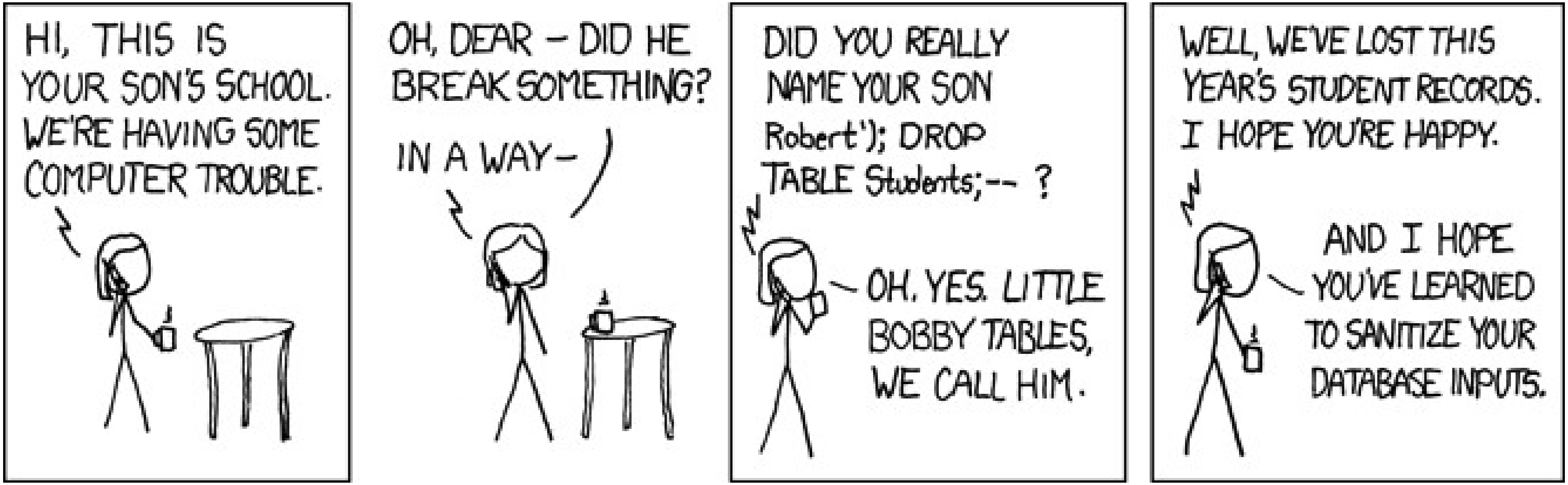
http://blog.thoughtcrime.org/authenticity-is-broken-in-ssl-but-your-app-ha

eller... http://tinyurl.com/6w3ykxu

Lad os kigge på noget kode...

http://blog.wingsofhermes.org/?p=58

4 Client side injection


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

XSS

CSRF

SQLi,

.....

stadig gældende...specielt ved web views

“Vores app har ingen webviews....”

Persistent XSS kan stadig være et problem i server setup for din app

Client Side Injection

- Escape input data
- Brug prepared statements
- Tænk hele vejen rundt

(...også admin tools)

5

Poor Authorization and Authentication

Hvad er der galt her?

```
if (isPermanentlyAuthorized(deviceID)) {
  int sessionToken = generateSessionToken();
  bean.setSessionToken(sessionToken)
  bean.setUserName(userName);
  ...
}
```

Stol ikke på potentielle kompromitterede værdier

IMEI

IMSI

UDID

6

Improper Session Handling

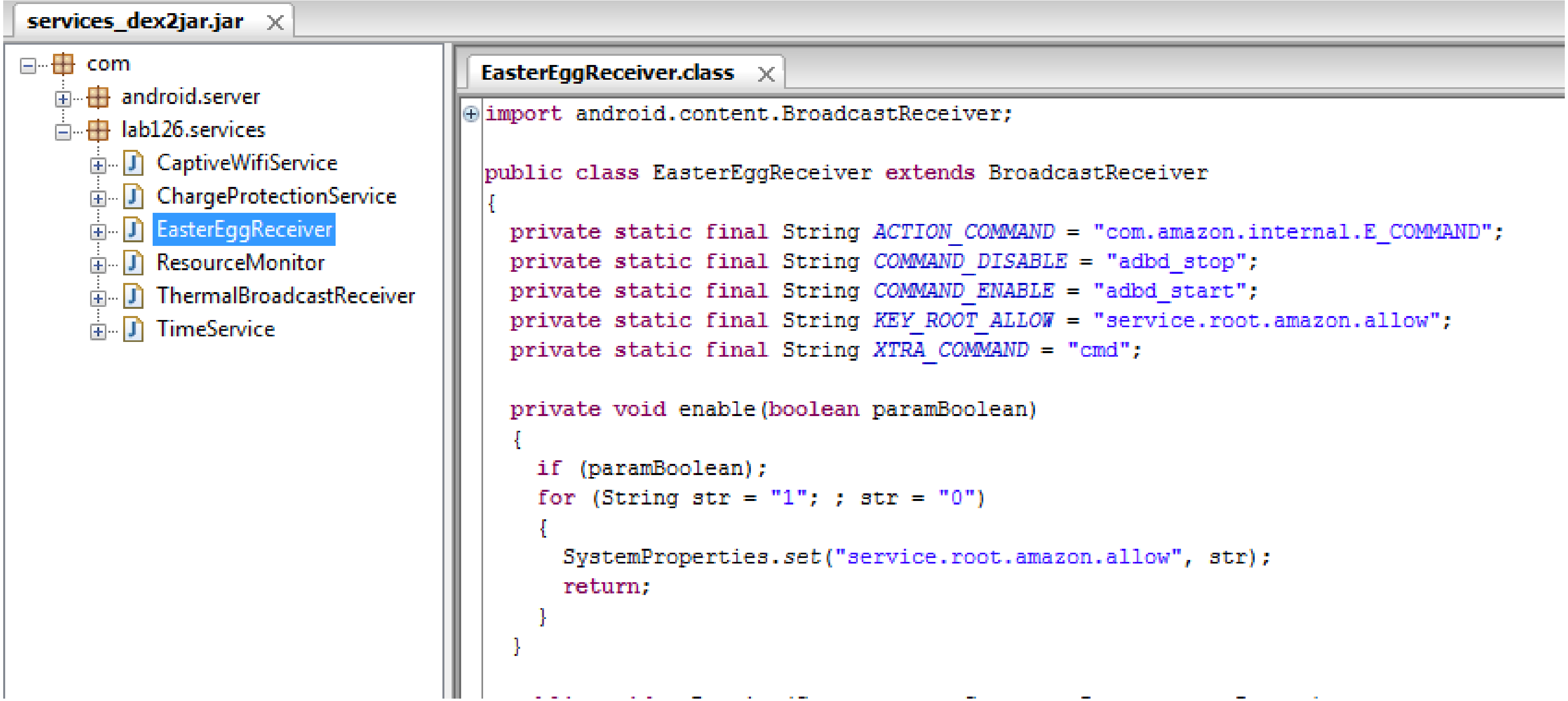
- Mobil session er ofte lang i forhold til fx. session i en browser

- Pas på med at bruge UUID eller lignende som session token

7

Security Decisions via Untrusted Inputs

Intents



```
import android.content.BroadcastReceiver;

public class EasterEggReceiver extends BroadcastReceiver
{
  private static final String ACTION_COMMAND = "com.amazon.internal.E_COMMAND";
  private static final String COMMAND_DISABLE = "adbd_stop";
  private static final String COMMAND_ENABLE = "adbd_start";
  private static final String KEY_ROOT_ALLOW = "service.root.amazon.allow";
  private static final String XTRA_COMMAND = "cmd";

  private void enable(boolean paramBoolean)
  {
    if (paramBoolean);
    for (String str = "1"; ; str = "0")
    {
      SystemProperties.set("service.root.amazon.allow", str);
      return;
    }
  }
```

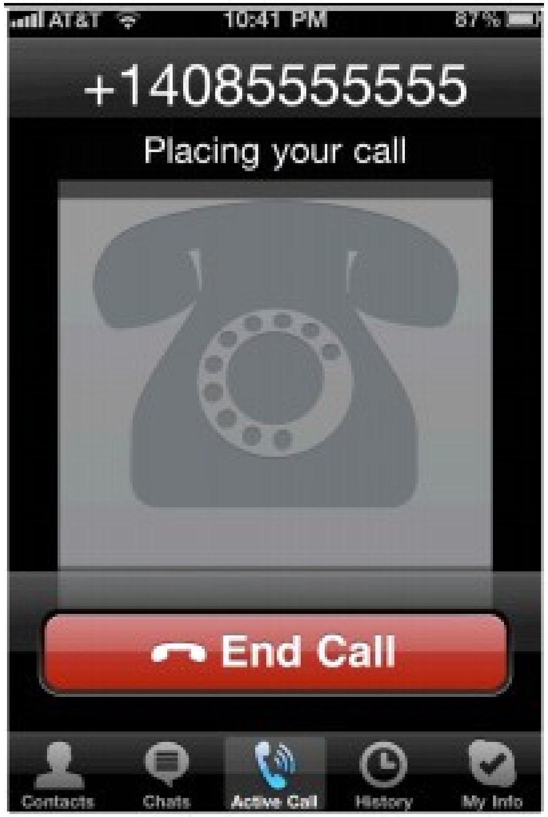
Intents - modtag

```
<receiver android:name=“my.special.receiver”
    android:exported=true
android:permission=“my.own.permission”>
  ...
</receiver>
```

Intents - broadcast

```
Intent i = new Intent();
i.setAction(“my.special.action”);
sendBroadcast(i, “my.special.permission”);
```

URL Schemes

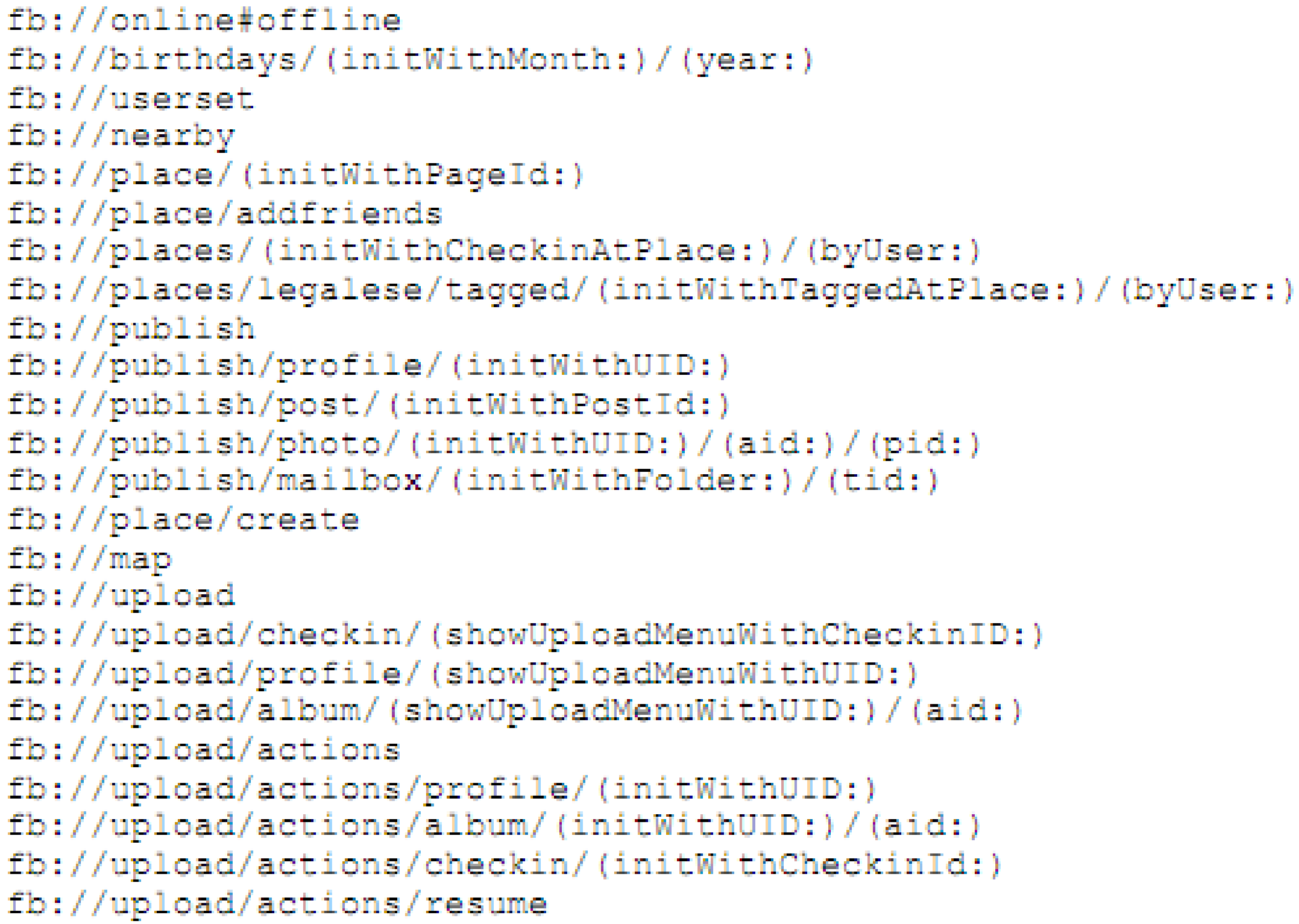


+14085555555

Placing your call

```
<iframe src=”skype://14085555555?call"></iframe>
```

```
strings Facebook.app/Facebook | grep 'fb:' | more
```



```
fb://online#offline
fb://birthdays/(initWithMonth:)/(year:)
fb://userset
fb://nearby
fb://place/(initWithPageId:)
fb://place/addfriends
fb://places/(initWithCheckinAtPlace:)/(byUser:)
fb://places/legalese/tagged/(initWithTaggedAtPlace:)/(byUser:)
fb://publish
fb://publish/profile/(initWithUID:)
fb://publish/post/(initWithPostId:)
fb://publish/photo/(initWithUID:)/(aid:)/(pid:)
fb://publish/mailbox/(initWithFolder:)/(tid:)
fb://place/create
fb://map
fb://upload
fb://upload/checkin/(showUploadMenuWithCheckinID:)
fb://upload/profile/(showUploadMenuWithUID:)
fb://upload/album/(showUploadMenuWithUID:)/(aid:)
fb://upload/actions
fb://upload/actions/profile/(initWithUID:)
fb://upload/actions/album/(initWithUID:)/(aid:)
fb://upload/actions/checkin/(initWithCheckinId:)
fb://upload/actions/resume
```

```
-(BOOL)application:(UIApplication *)application
     handleOpenURL:(NSURL *)url
{
   //1. Parse URL <-- Careful - do thorough input validation
   //2. Ask for authorization
   //3. Perform transaction
}
```

Security Decisions via Untrusted Inputs

- Input validering
- Undersøg rettigheder
- Input validering
- Input validering
- Input validering
- Prompt evt. brugeren for bekræftigelse
- ....og input validering

8 Side Channel Data Leakage

Følsom data logges eller caches de forkerte steder

Screen shot ved backgrounding

Side Channel Data Leakage

- Debug din app og undersøg hvilket filer bliver oprettet.
- Tjek logfiler
- Log aldrig username og password

9 Broken Cryptography

Lav ikke din egen kryptografi

Encoding != encryption

Obfuskering != encryption

Serialization != encryption

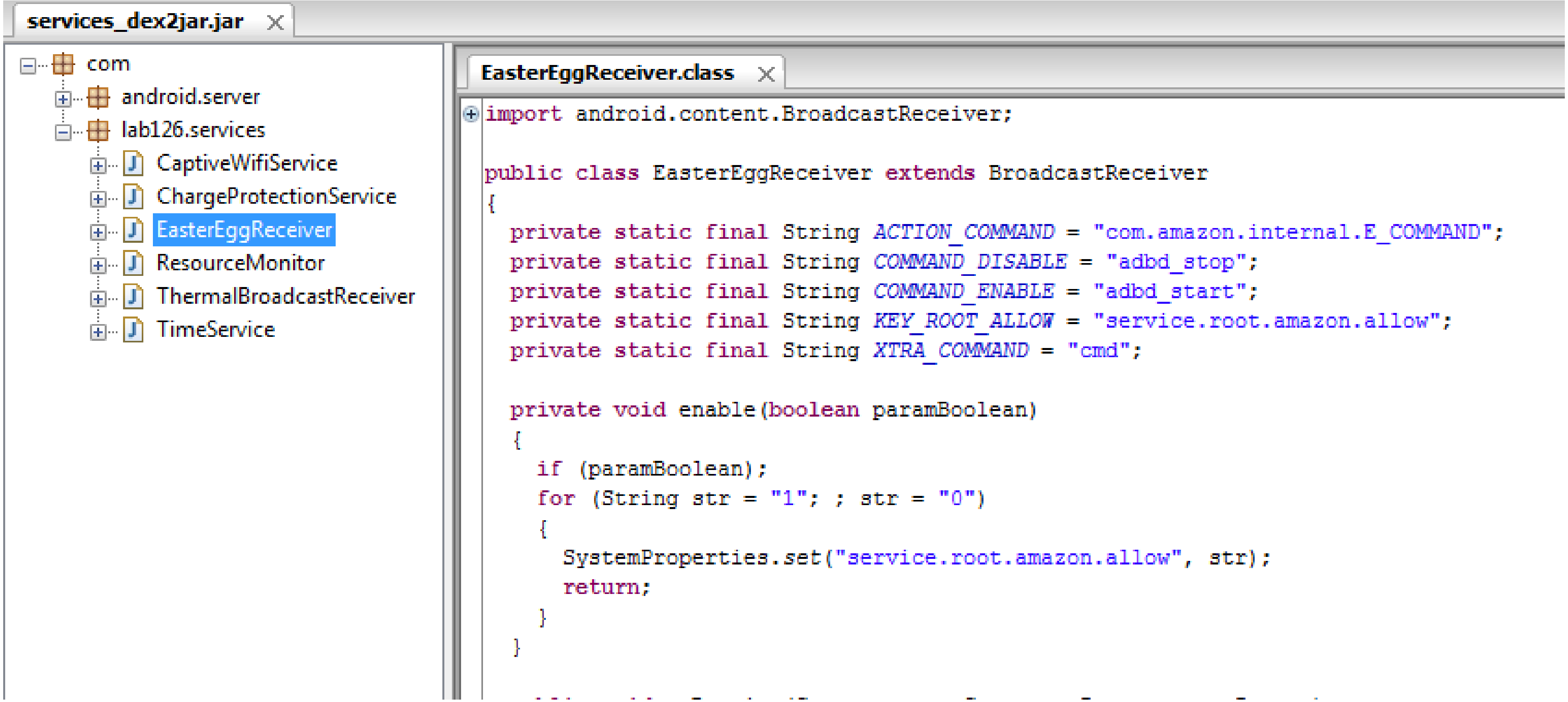
10

Sensitive Information Disclosure

Alt kan reverse engineeres

I app'en, undlad at placere

- Nøgler
- Passwords
- Følsom forretningslogik



```
import android.content.BroadcastReceiver;

public class EasterEggReceiver extends BroadcastReceiver
{
  private static final String ACTION_COMMAND = "com.amazon.internal.E_COMMAND";
  private static final String COMMAND_DISABLE = "adbd_stop";
  private static final String COMMAND_ENABLE = "adbd_start";
  private static final String KEY_ROOT_ALLOW = "service.root.amazon.allow";
  private static final String XTRA_COMMAND = "cmd";

  private void enable(boolean paramBoolean)
  {
    if (paramBoolean);
    for (String str = "1"; ; str = "0")
    {
      SystemProperties.set("service.root.amazon.allow", str);
      return;
    }
  }
```

```
if (rememberMe) {
  saveCredentials(userName, password);
}

//our secret backdoor account
if (userName.equals("all_powerful") &&
password.equals("iamsosmart")) {
  launchAdminHome(v);
}
```

```
public static final double
SECRET_SAUCE_FORMULA = (1.2344 * 4.35 - 4 +
1.442) * 2.221;
```

....med Dex2Jar og JD-GUI kommer man langt.

Obfuskering løser ikke problemet

....det løfter blot sværhedsgraden

“Men hvorfor obfuskere iOS, det er jo c-kode?”

NEJ!

Objective-C har mange spændende ting stående i den kompilerede kode

otool, class-dump, ...

Obfuskering

Man kan lave obfuskeringen. Men overvej hellere: hvorfor har jeg dette stående i koden?

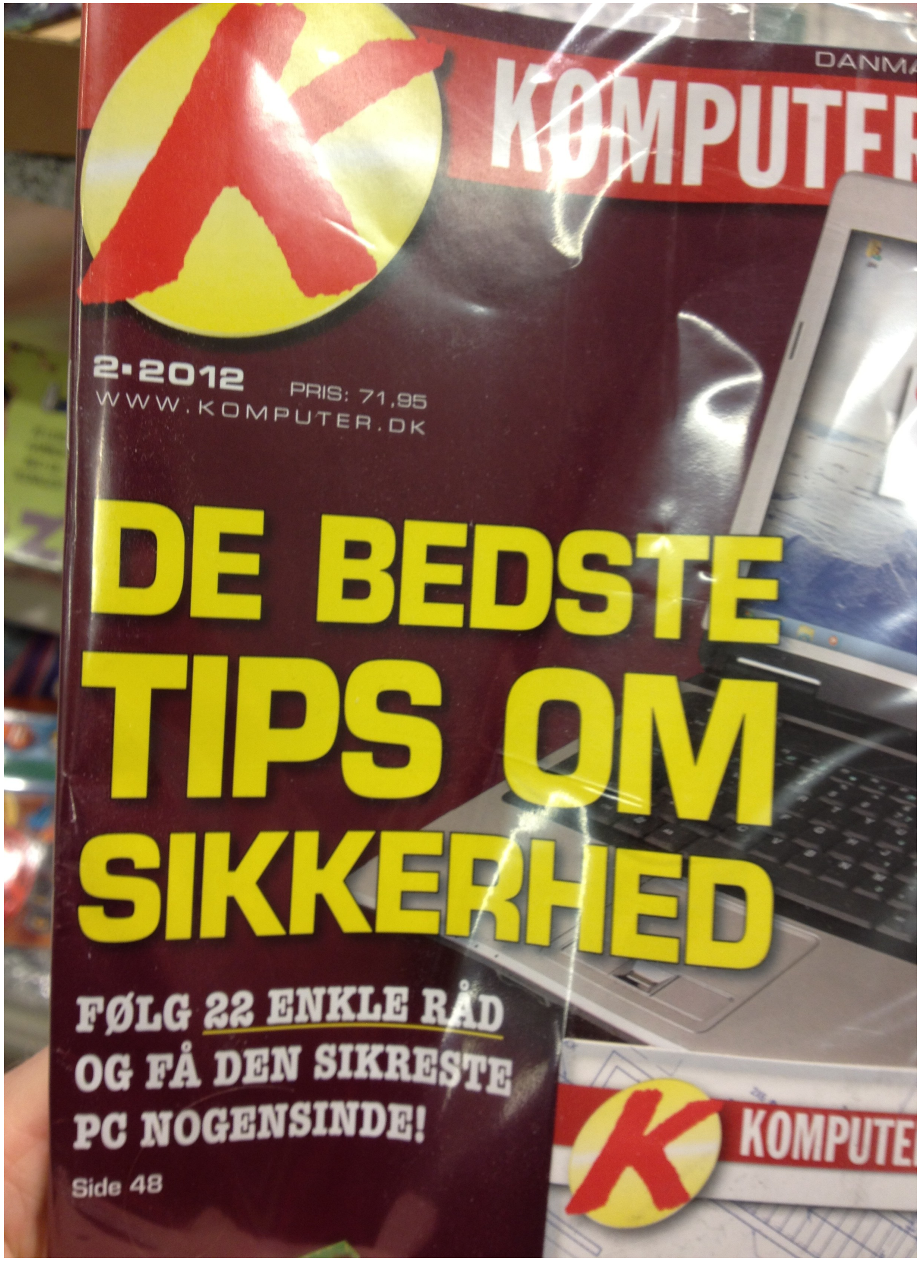
OWASP – Top 10 mobile risks
(release candidate v. 1.0)

1. Insecure Data Storage
2. Weak Server Side Controls
3. Insufficient Transport Layer Protection
4. Client Side Injection
5. Poor Authorization and Authentication
6. Improper Session Handling
7. Security Decisions Via Untrusted Inputs
8. Side Channel Data Leakage
9. Broken Cryptography
10. Sensitive Information Disclosure

Hack yourself

- Debug din app og undersøg hvilket filer bliver oprettet.
- Log intet – eller overvej hvergang du logger.
- Tjek logfiler.
- Opsæt proxy og kig på trafikken mellem app og backend.
- Skriv forskellige ting ind i input felter. Go crazy!

COPENHAGEN
INTERNATIONAL
SOFTWARE DEVELOPMENT
CONFERENCE 2012
goto;
conference
Conference: May 21-23 // Training: May 24-25



DANMA

KOMPUTER

2•2012

PRIS: 71,95

WWW.KOMPUTER.DK

DE BEDSTE TIPS OM SIKKERHED

FØLG 22 ENKLE RÅD OG FÅ DEN SIKRESTE PC NOGENSINDE!

Side 48

KOMPUTEI

Tak for jeres tid

Referencer

http://www.qadit.com/blog/?p=2182

http://www.f-secure.com/weblog/archives/00002280.html

http://www.machackpc.com/iphone-malware-%E2%80%93-iphoneibotnet-a/

http://www.slideshare.net/JackMannino/owasp-top-10-mobile-risks

https://www.cs.berkeley.edu/~emc/slides/SevenWaysToHangYourselfWithGoogleAndroid.pdf

http://gizmodo.com/5881778/googles-finally-cracking-down-on-android-malware

http://intrepidusgroup.com/insight/2011/08/dropbox-for-android-vulnerability-breakdown/

http://www.nypost.com/p/news/business/citibank_admits_security_flaw_in_fDLT7l6VFdqKLLaTx75cYM

https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks

http://www.slideshare.net/iamleeg/security-and-encryption-on-ios

https://grepular.com/Dropbox_Mobile_Less_Secure_Than_Dropbox_Desktop

http://www.uni-ulm.de/in/mi/mitarbeiter/koenings/catching-authtokens.html

http://threatpost.com/en_us/blogs/apple-releases-ios-5-removes-diginotar-certs-iphones-ipads-101211

http://blog.thoughtcrime.org/authenticity-is-broken-in-ssl-but-your-app-ha

http://intrepidusgroup.com/insight/2012/01/android-backdoor-fail-the-kindle-fire-easter-egg/

https://media.blackhat.com/bh-eu-11/Nitesh_Dhanjani/BlackHat_EU_2011_Dhanjani_Attacks_Against_Apples_iOS-WP.pdf

http://blog.wingsofhermes.org/?p=58