# SECURITY 2013

## 21. ročník konference o bezpečnosti v ICT

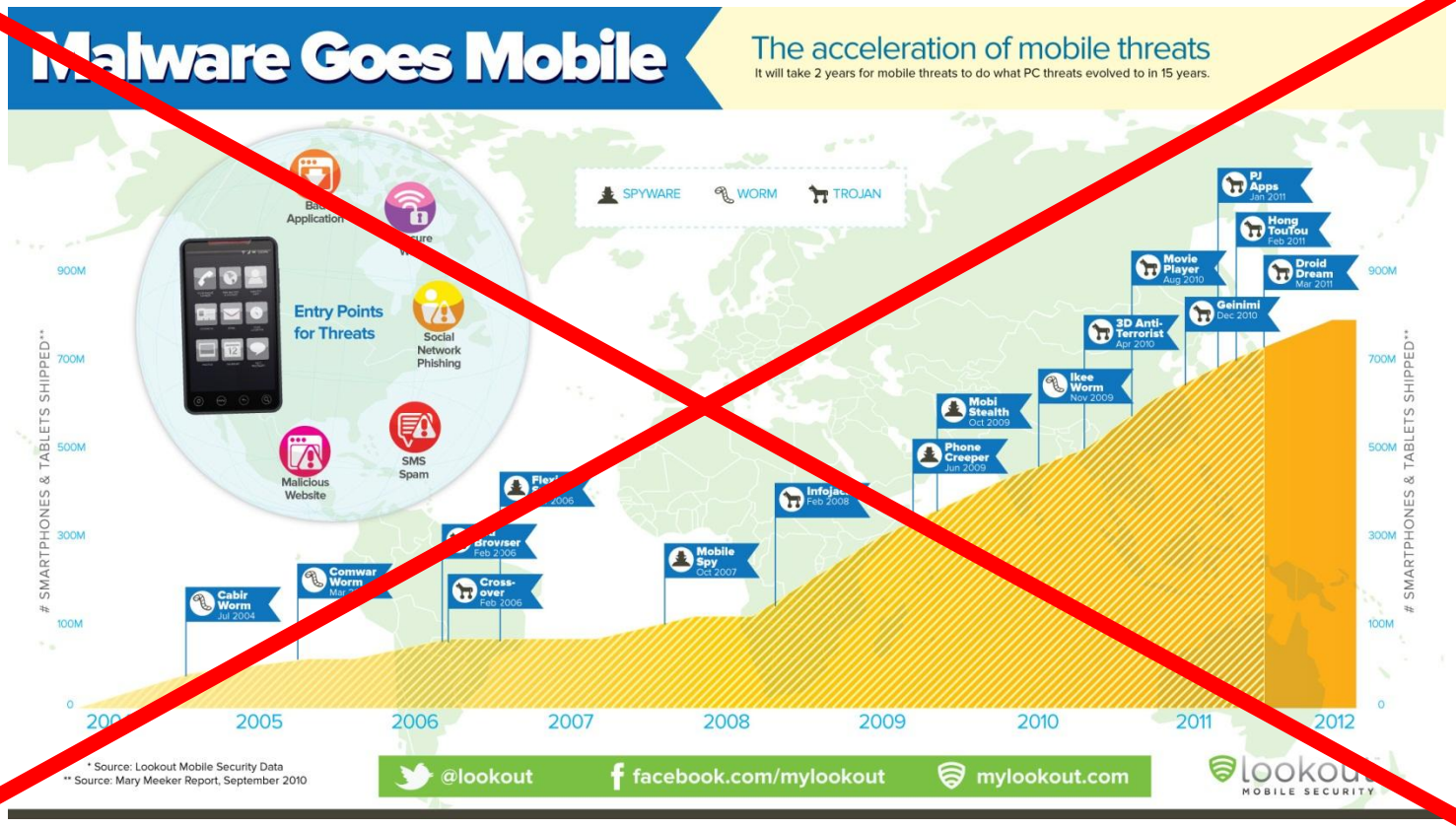
# Bezpečné nastavení a používání mobilních zařízení

Lukáš Bláha

AEC, spol. s r.o.

# Bezpečnost mobilních platforem?

Malware, zero days, smishing, …



# Fyzické útoky – Screen Lock

- Passcode
  - bruteforce útok vs. realita?
- PIN
  - bruteforce útok cca 20 minut
  - smudge útok
- Gesto
  - smudge útok
- Rozpoznání obličeje
  - podvržení fotky (Android 4.0 ICS fail)
- Hlas
  - možnost podvrhnout
- Kombinace
  - uživatelsky nepřívětivé = reálně nepoužitelné
- Použití akcelerometru/gyroskopu pro hádání přístupového hesla/gesta
  - Sedící uživatel – uhádnutí PINu 43%, gesta 73%
  - Jdoucí uživatel – uhádnutí PINu 20%, gesta 40%

Adam J. Aviv, Benjamin Sapp, Matt Blaze and Jonathan M. Smith - Practicality of Accelerometer Side Channels on Smartphones [2012]
Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith - Smudge Attacks on Smartphone Touch Screens [2010]

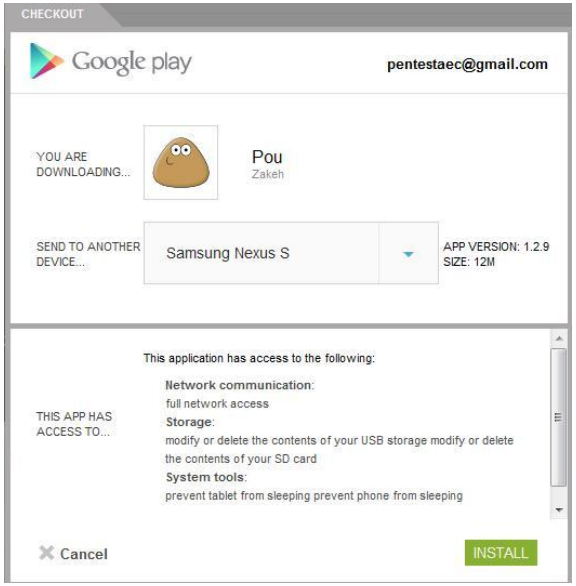
# Fyzické útoky – Android ADB

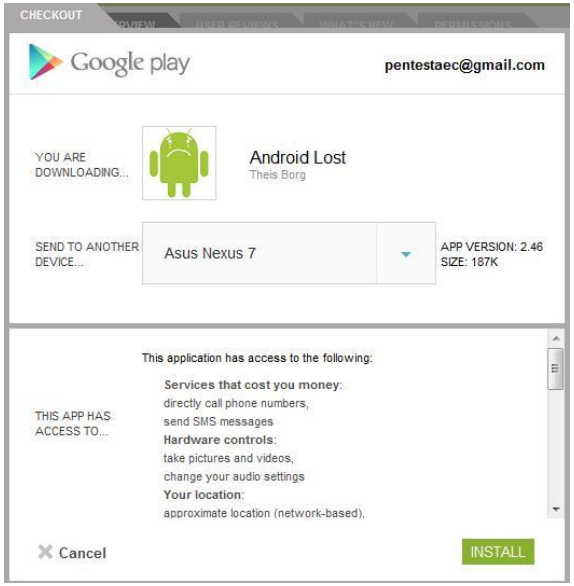
- Juice Jacking
- Připojení zařízení na veřejné nabíječky
- Záložní baterie
- „Chvilkové zapůjčení zařízení“
- Základní problém – povolené ADB (USB Debugging, nezbytné pro development)

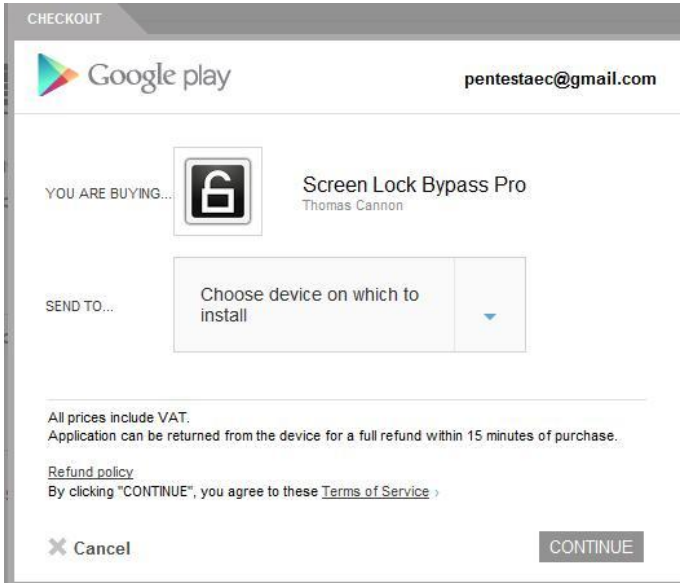
- Přístup k SD kartě, fotkám, Google účtu!, atd.
- Možnost rootu zařízení => kompletní přístup k systému!

# Android „z druhé strany“

- Google remote kill
  - Vzdálené smazání „malware“ z vašeho zařízení ☺
- Možnost  vzdálené instalace aplikací
  - Pro uživatele může být užitečné, co když se to ale dostane do nesprávných rukou?



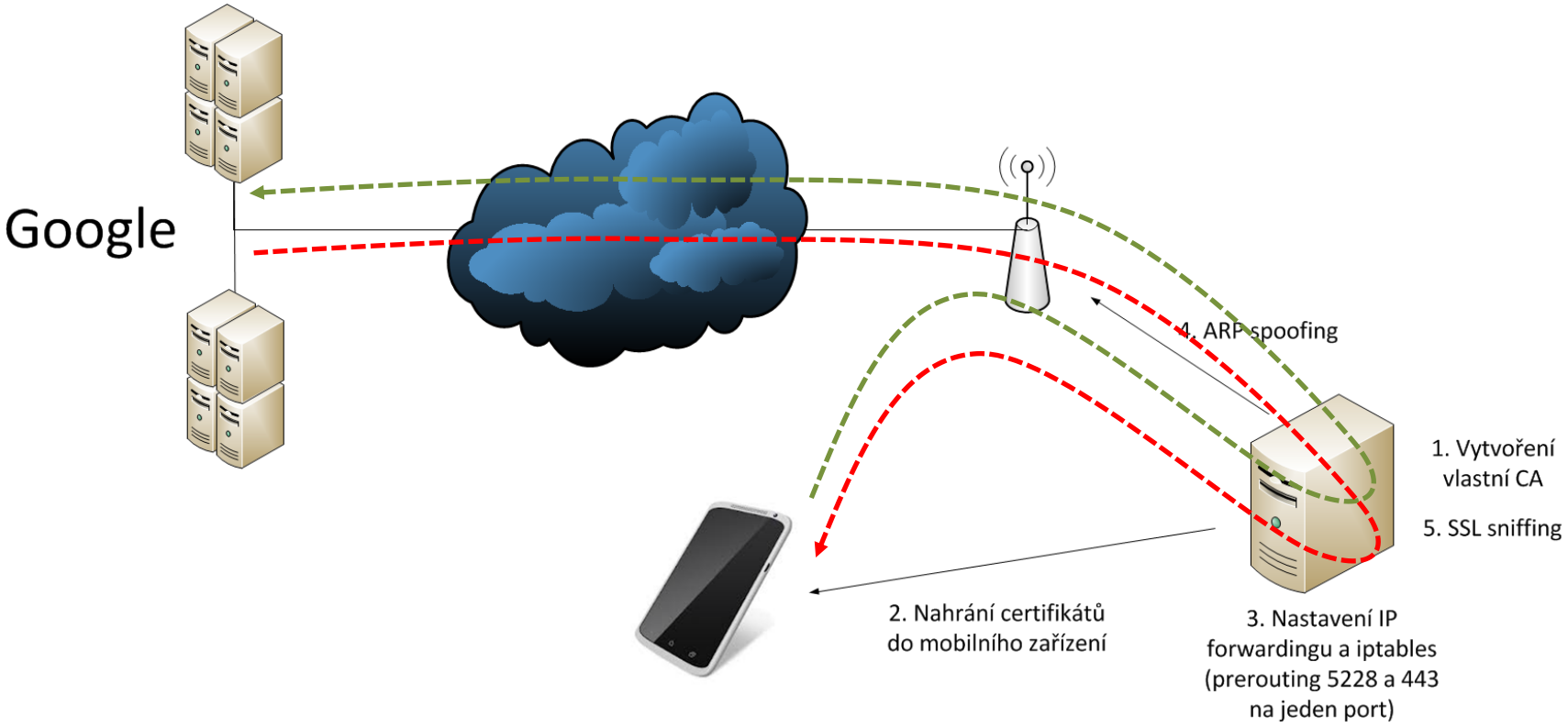
# Android „z druhé strany“

- Jak to funguje?
- GTalkService (TCP/SSL, porty 5228 a 443)
  - periodický hartbeat
  - REMOVE_ASSET
  - INSTALL_ASSET
    - tickle_id
    - assetid
    - asset_name
    - asset_type
    - asset_package
    - asset_blob_url
    - asset_signature ←
    - asset_size

```
|[02e614] com.android.vending.AssetDownloader.verifyApk:(Landroid/content/Context;Landroid/net/Uri;
|0000: const/4 v7, #int 0 // #0
|0001: const-string v8, "IOException in finally block." // string@0482
|0003: const/4 v5, #int 0 // #0
|0004: const-string v6, "#" // string@0030
|0006: invoke-virtual {v11, v6}, Ljava/lang/String;.split:(Ljava/lang/String;)[Ljava/lang/String; /
|0009: move-result-object v4
|000a: const/4 v6, #int 0 // #0
|000b: aget-object v0, v4, v6
|000d: const/4 v6, #int 1 // #1
|000e: aget-object v6, v4, v6
|0010: invoke-static {v6}, Ljava/lang/Long;.parseLong:(Ljava/lang/String;)J // method@1286
|0013: move-result-wide v1
|0014: invoke-virtual {v9}, Landroid/content/Context;.getContentResolver:()Landroid/content/Content
|0017: move-result-object v6
|0018: invoke-virtual {v6, v10}, Landroid/content/ContentResolver;.openInputStream:(Landroid/net/Ur
|001b: move-result-object v5
|001c: if-nez v5, 0031 // +0015
|001e: const-string v6, "Unable to open input stream, nothing available to verify." // string@0c20
|0020: invoke-static {v6}, Lcom/android/vending/util/Log;.w:(Ljava/lang/String;)V // method@108a
|0023: if-eqz v5, 0028 // +0005
|0025: invoke-virtual {v5}, Ljava/io/InputStream;.close:()V // method@124e
|0028: move v6, v7
|0029: return v6
|002a: move-exception v3
|002b: const-string v6, "IOException in finally block." // string@0482
|002d: invoke-static {v8}, Lcom/android/vending/util/Log;.w:(Ljava/lang/String;)V // method@108a
|0030: goto 0028 // -0008
|0031: invoke-static {v5, v0, v1, v2}, Lcom/android/vending/util/Sha1Util;.verify:(Ljava/io/InputSt
|0034: move-result v6
|0035: if-eqz v5, 0029 // -000c
|0037: invoke-virtual {v5}, Ljava/io/InputStream;.close:()V // method@124e
```

Jon Oberheide – Android Hax (SummerCon 2010)

# Android „z druhé strany“



# Android „z druhé strany“

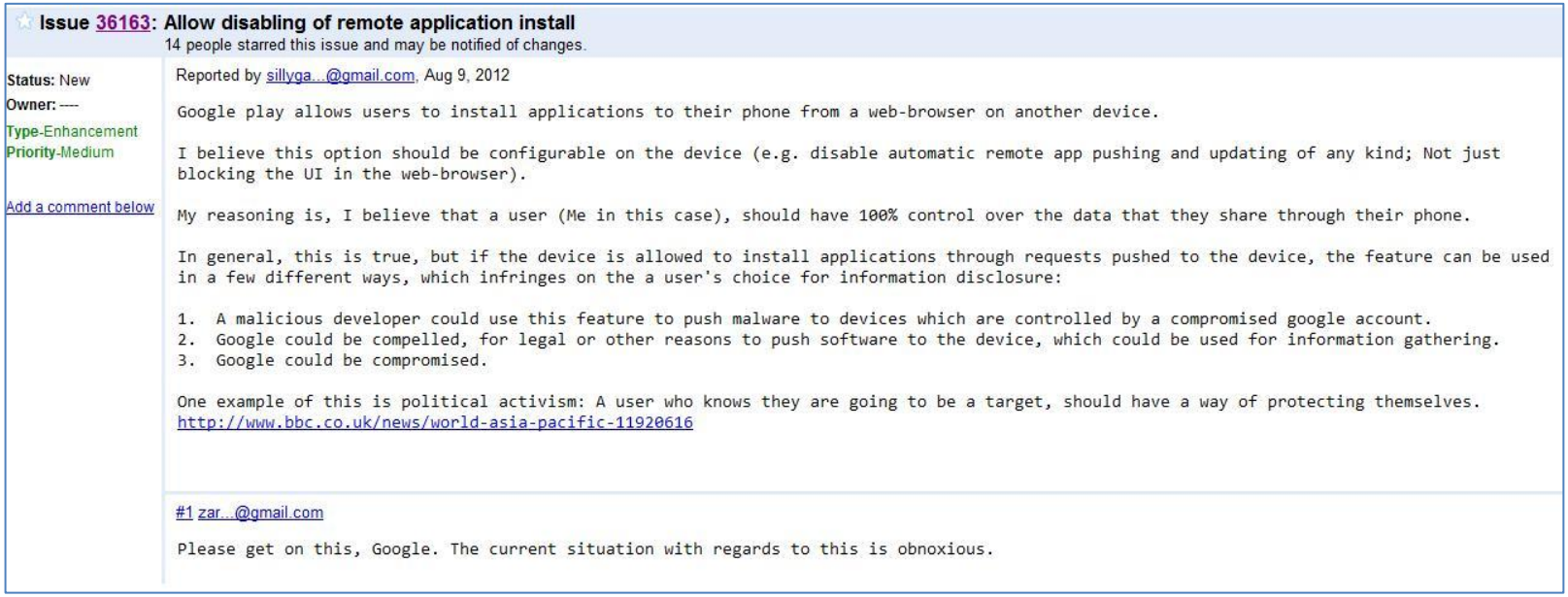
- 1360582258 DEBUG sslsniff : Read from Server (mtalk.google.com) :
- ×BB0F84F1
- google.com*SERVER_NOTIFICATION2do_not_collapse:ń
- NOTIFICATION_PAYLOADŘCAEY5vOgyMwnIhoKFGNvbS5tZXRhbW9raS5BcXVhcG9wEAEYAyoKRnJ1a XQgUG9wITIUcGVudGVzdGFlY0BnbWFpbC5jb206Iwi1CRIedjI6Y29tLm1ldG…OtbWwtAEqHRIbbkpPe FNtU3B3ZFVlVDd1alNPbXFvVFFGeDVBMgEz@J#0:1360582425130818%08605c67f9fd7ecd

- 1360582308 DEBUG sslsniff : Read from Client (*.google.com) :
- POST /market/api/ApiRequest HTTP/1.1
- Content-Type: application/x-www-form-urlencoded; charset=UTF-8
- User-Agent: Android-Market/2
- X-Public-Android-Id: b8e432fb7c270da8
- Content-Length: 2603
- Host: android.clients.google.com
- Connection: Keep-Alive

- 1360582308 DEBUG sslsniff : Read from Client (*.google.com) :
- version=2&request=CoIDCqACRFFBQUFNRUFBQUNIbTZJMFBCYWZEZlVzY0ItYnZmWWJYMUQwb1V YYXJVUjMwMUZHTUg5em03cm5seUZ...1YmU6MTo0MjE2IAIonJi4yMwnOhpjb20uZ29vZ2xlLmFuZH JvaWQueW91dHViZUD4IBQTGh52Mjpjb20uZ29vZ2xlLmVhcnRoOjE6MTIzNTIxMDAgAiicmLjIzCc6EG NvbS5nb29nbGUuZWFydGhA5PTxBRQTGh52Mjpjb20ubWV0YW1va2kuQXF1YXBvcDoxOjEyMD

# Android „z druhé strany“

- Jak se proti tomu bránit?
  - Google:



**Issue 36163: Allow disabling of remote application install**

14 people starred this issue and may be notified of changes.

**Status:** New
**Owner:** ----
Type-Enhancement
Priority-Medium

Add a comment below

Reported by sillyga...@gmail.com, Aug 9, 2012

Google play allows users to install applications to their phone from a web-browser on another device.

I believe this option should be configurable on the device (e.g. disable automatic remote app pushing and updating of any kind; Not just blocking the UI in the web-browser).

My reasoning is, I believe that a user (Me in this case), should have 100% control over the data that they share through their phone.

In general, this is true, but if the device is allowed to install applications through requests pushed to the device, the feature can be used in a few different ways, which infringes on the a user's choice for information disclosure:

1. A malicious developer could use this feature to push malware to devices which are controlled by a compromised google account.
2. Google could be compelled, for legal or other reasons to push software to the device, which could be used for information gathering.
3. Google could be compromised.

One example of this is political activism: A user who knows they are going to be a target, should have a way of protecting themselves.
http://www.bbc.co.uk/news/world-asia-pacific-11920616

#1 zar...@gmail.com

Please get on this, Google. The current situation with regards to this is obnoxious.

  - Technologicky: pouze root zařízení a instalace aplikace, blokující tyto požadavky – neexistuje ☺

# Fyzické útoky - iOS

- Keychains
- SQLite databáze pro ukládání citlivých dat (přihlašovací údaje, RSA klíče, …)
  - K nalezení ve /var/Keychains/keychain-2.db

- Keychain data jsou šifrována
  - HW šifrovacím klíčem - nemůže být přesunuto na jiné zařízení
  - Uživatelským PINem/passcodem
- Idea – vývojáři mohou použít keychains pro bezpečné uložení citlivých dat
  - Problém při jailbreaku => Keychain Dumper, Keychain Viewer
- Řešení
  - Pokud uživatel nastaví passcode, je získání dat složité, ne však nemožné
  - Co když ho uživatel nenastaví?
  - Nepoužívat pro ukládání citlivých informací při vývoji aplikací
  - Vlastní řešení  kryptografických modulů?

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

# Děkuji za pozornost.

Lukáš Bláha

AEC, spol. s r.o.

lukas.blaha@aec.cz