GOPAS
POCITACOVA.SKOLA.CZ

Kali Pwn Pad ~ vyzbrojen tabletem je nebezpečím pro společnost

Kamil Vávra

vavkamil@gmail.com

HACKERFest 2014

Kdo jsem ?

- Kamil Vávra
  - 23 let
  - Brno
  - Správce počítačové sítě
- Perl, Linux, Android
- Offensive & Defensive Security
- Programming & Penetration testing
- Kali Linux, ethical hacking & web security

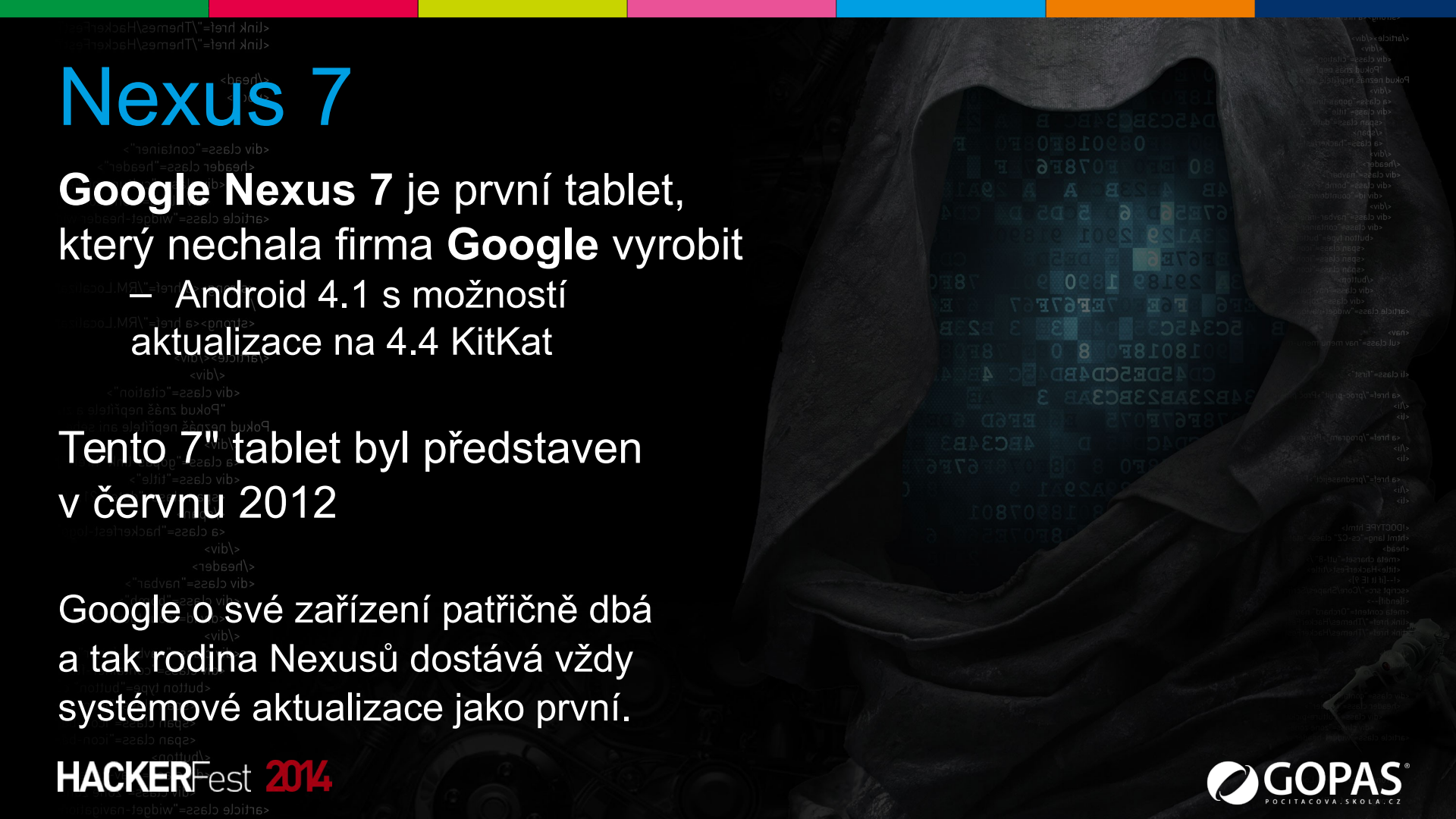
Nexus 7

Google Nexus 7 je první tablet, který nechala firma **Google** vyrobit

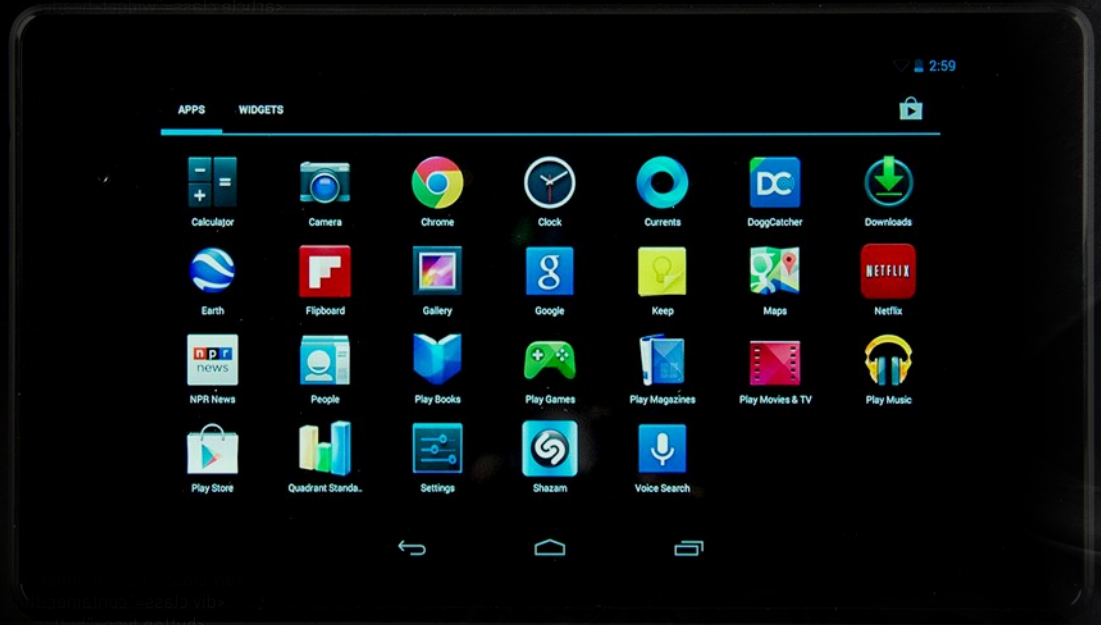
- Android 4.1 s možností aktualizace na 4.4 KitKat

Tento 7" tablet byl představen v červnu 2012

Google o své zařízení patřičně dbá a tak rodina Nexusů dostává vždy systémové aktualizace jako první.



Nexus 7


2:59
APPS
WIDGETS
Calculator
Camera
Chrome
Clock
Currents
DoggCatcher
Downloads
Earth
Flipboard
Gallery
Google
Keep
Maps
Netflix
NPR News
People
Play Books
Play Games
Play Magazines
Play Movies & TV
Play Music
Play Store
Quadrant Standa..
Settings
Shazam
Voice Search

Nexus 7

HACKERFest 2014

GOPAS
POCITACOVA.SKOLA.CZ


Nexus 7
1. DEMO

Nexus 7

MITMf aplikace

Framework for
Man-In-The-Middle attacks

Framework představen před 3 měsíci
https://github.com/byt3bl33d3r/MITMf

Nexus 7

MITMf a nejpodstatnější změny

- Integrated SSLstrip+ (https://github.com/LeonardoNve/sslstrip2) by Leonardo Nve to partially bypass HSTS as demonstrated at BlackHat Asia 2014

- Spoof plugin může nyní exploitovat „ShellShock“ bug během DHCP spoofingu!

Nexus 7

O čem budu mluvit

- Historie Androidu
  - Bezpečnostní aktualizace
  - Statistiky
- Android malware
  - První incidenty
- Exploitace Android zařízení
  - Demo jednotlivých útoků

O čem budu mluvit

- Pwn Pad
  - Modifikace zařízení
  - Integrace Kali Linuxu
  - Hacking z Android tabletu
- Net Hunter
  - Kali Linux pro Nexus
  - Hacking ze smartphone
  - Google Nexus 5

Android & něco málo z historie

- **Říjen 2003**
  - V Kalifornii byla založena společnost Android Inc.
- **Srpen 2005:**
  - Google Inc. odkoupil v té době nepříliš známou „startup“ firmu Android Inc. a udělal z ní svoji dceřinou společnost.

Android & něco málo z historie

- **Září 2007:**
  - Tým Googlu vyvinul platformu založenou na Linuxovém jádře a získal několik patentů v oblasti mobilních technologií.
- **Říjen 2008:**
  - Ve Spojených státech amerických byl uveden první komerční telefon vyrobený firmou HTC s operačním systémem Android.

Android & něco málo z historie

- **Leden 2009:**
  - První telefon s Androidem byl uveden na trh pro Českou republiku.
- **26. Říjen 2009:**
  - Byla uvolněna aktualizace **Android 2.0/2.1 (Eclair)** s podporou Bluetooth 2.1.

Android & něco málo z historie

- **6. Prosinec 2010:**
  - **Android 2.3/2.4 (Gingerbread) ~** Podpora pro NFC, který dnes podporují některé mobilní telefony a tablety. Dále byla zavedena technologie NX bit pro CPU sloužící k oddělení paměti pro instrukce procesoru (strojového kódu) a pamětí pro data.

Android & něco málo z historie

- **22. Únor 2011:**
  - **Android 3.0/3.1/3.2 (Honeycomb) ~** Optimalizace pro velké obrazovky tabletů, USB Host. Možnost plného šifrování souborového systému s 128bit AES klíčem odvozeným z hesla uživatele.

Android & něco málo z historie

- **19. Říjen 2011:**
  - **Android 4.0/4.0.4 (Ice Cream Sandwich)**

    ~ Address space layout randomization

    - metoda počítačové bezpečnosti,

    která umisťuje strojový kód programu,

    knihovny a data v operační paměti

    do náhodně zvolené adresy.

    Cílem je znemožnit některé typy útoků a exploitů.

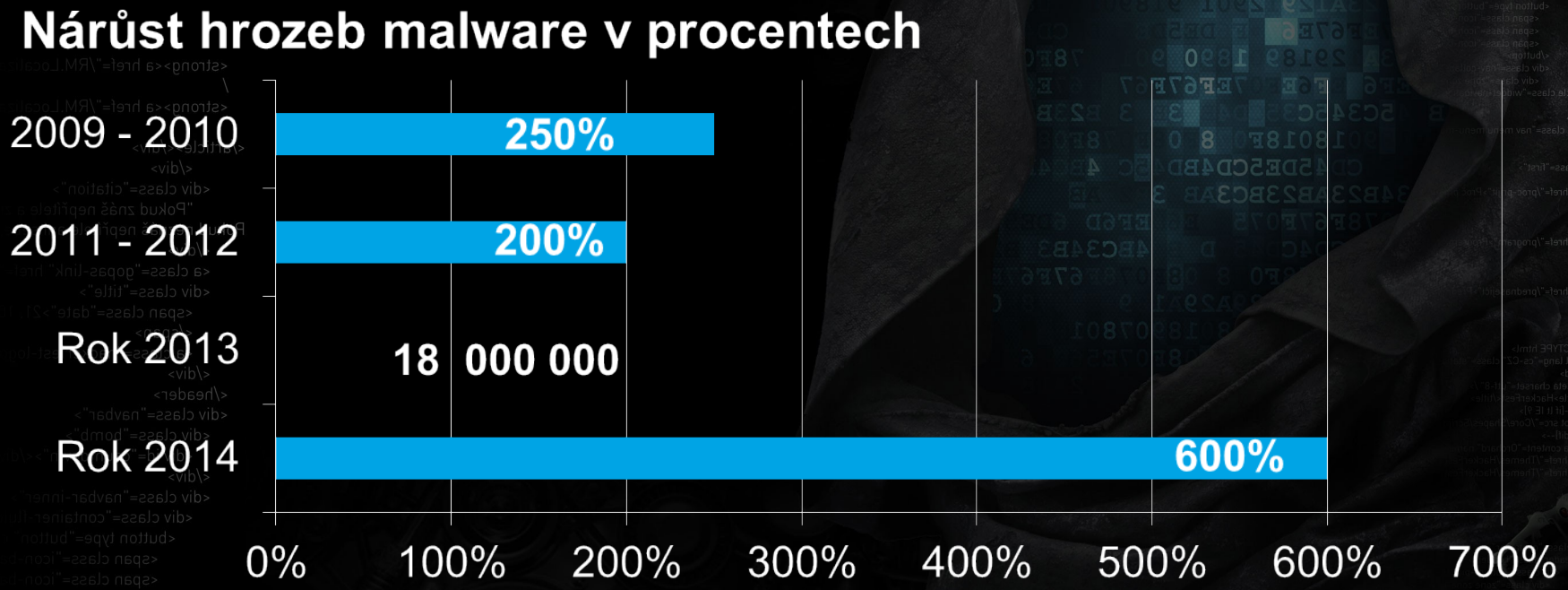
Android & něco málo z historie

- **9. Červenec 2012:**
- **4.1/4.2/4.3 (Jelly Bean) ~**
  - Tato aktualizace zablokovala u všech aplikací rozesílání SMS bez interakce uživatele. Dále je zabudována základní anti-malware ochrana, znemožňující například stahování a instalaci aplikací na pozadí.

Android & něco málo z historie

- V roce 2012 společnost Juniper analyzovala 1 850 000 aplikací pro android z 500 různých marketů. Z toho **267 259** obsahovalo malware.
- V květnu tohoto roku Google oznámil 900 milionů aktivovaných Android zařízení a 48 miliard stažených aplikací z Google Play.

Statistika


Nárůst hrozeb malware v procentech
2009 - 2010
250%
2011 - 2012
200%
Rok 2013
18 000 000
Rok 2014
600%
0%
100%
200%
300%
400%
500%
600%
700%

Android & historie malware

- **9. Srpen 2010:**
  - **SMS.AndroidOS.FakePlayer.a**
  - První SMS Android Malware.
    Aplikace slouží jako Media Player.
    Jakmile je nainstalována na telefonu,
    trojan začne rozesílat SMS
    na premium čísla.

Android & historie malware

- **17. Srpen 2010:**
  - **AndroidOS_Droisnake.A**
  - Jedná se o první GPS Spy malware. Aplikace se tváří jako klasická hra Snake známá z nokie, "hra" slouží jako zástěrka pro špionážní aplikaci, která běží na pozadí a odesílá GPS souřadnice na server.

Android & historie malware

- **14. Září 2010:**
  - **SMS.AndroidOS.FakePlayer.b**
  - První porno malware pro android! Tento malware je varianta SMS.AndroidOS.FakePlayer.A. Aplikace nazvaná pornoplayer.apk s pornografickou ikonou slibuje přísun erotických obrázků zdarma. Po spuštění aplikace bohužel uživatel žádnou erotiku neuvidí, aplikace pouze odešle 4 premium SMS.

Android & historie malware

- **29. Prosinec 2010:**
  - **Android.Geinimi**
  - První příklad botnetu postaveného na Android zařízeních. Škodlivý kód byl vložen do legitimních her a distribuován po čínských a ruských sítích. Jakmile je malware nainstalovaný, začne přijímat příkazy od serveru a útočník je schopný ovládat celý telefon. Konkrétně shromažďuje GPS souřadnice, identifikátor telefonu IMEI a sim karty IMSI.

Android & historie malware

- **1. Březen 2011:**
  - **Android.DroidDream**
  - První příklad nové generace mobilního malware šířeného přes Android Market, dle Symantecu bylo napadeno 50.000 až 200.000 uživatelů. Použitím dvou nástrojů (rageagainstthecage and exploid) se snaží o root telefonu.

Android & historie malware

- **1. Březen 2011:**
  - **Android.BgServ**
  - 6. Března 2011 vydal Google nástroj Android Market Security tool k odstranění malware DroidDream. Tento trojan je převlečený právě za tento security tool a napadá dalších minimálně 5000 uživatelů. Jedná se o první vážnou demonstraci toho, jak je Android Market nezabezpečený.

Android & historie malware

- **9. Květen 2011:**
  - **Android.Adsms**
  - Nový druh malware zaměřený na uživatele China Mobile. Malware se šíří pomocí odkazu zaslaného prostřednictvím SMS. Uvedená zpráva se tváří jako oznámení operátora ke stažení bezpečnostního patche z uvedeného odkazu. Po stažení rozesílá SMS na premium čísla.

Android & historie malware

- **31. Květen 2011**
  - **Android.LightDD**
  - Nová verze trojanu Android.DroidDream, přezdívaná DroidDreamLight, byla nalezena ve 24 aplikacích od 5 různých vývojářů distribuovaných v Android Marketu.
    Infikováno bylo cca **120 000** uživatelů.

Android & Exploitace

- UI Redressing
- WebView addJavascriptInterface
  - Remote Code Execution
- Secure USB Debugging Bypass
  - Android 4.4.2
    - Lock Pattern Bypass
- Hacking Android Smartphone

UI Redressing Attack

Attacks on Android Devices Revisited

HACKERFest 2014

GOPAS
POCITACOVA.SKOLA.CZ

UI Redressing Attack

"Attacks" on mobile phones via:

- trojan horses
- applications with the persmission to do phone calls

UI Redressing Attack

Může aplikace bez oprávnění k provádění telefonních hovorů uskutečnit hovor?

UI Redressing Attack

Slabé místo:

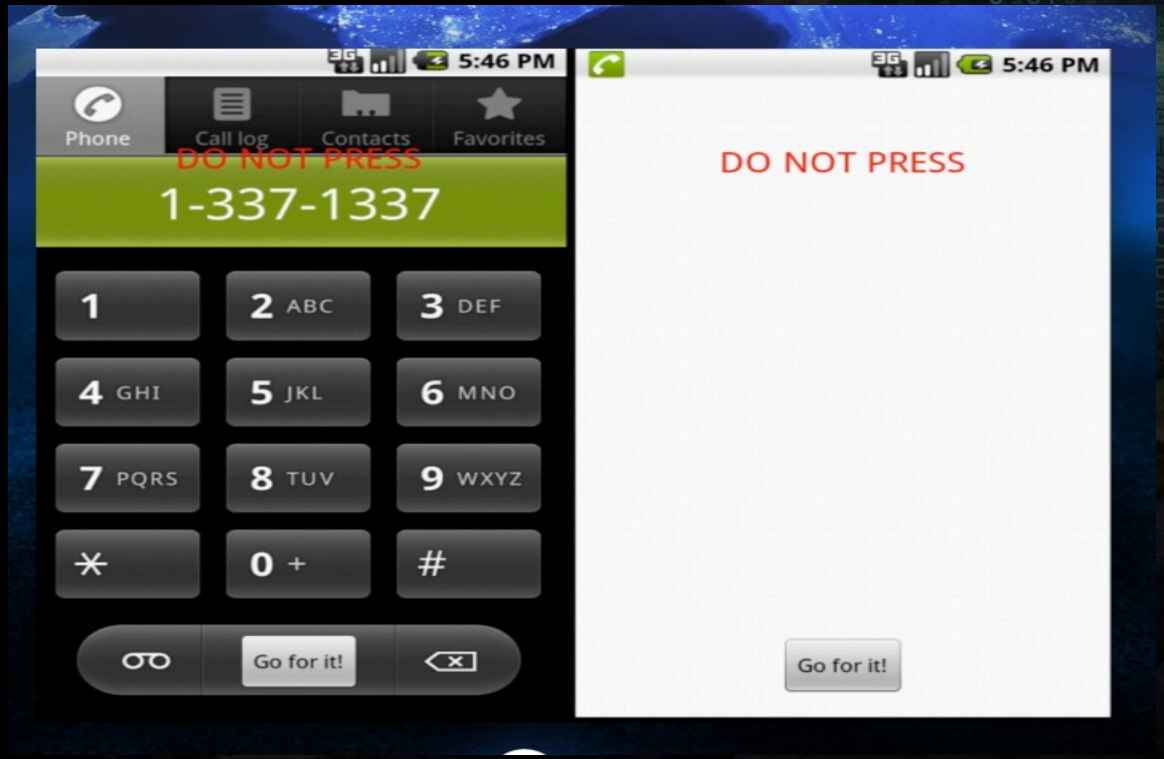
- aplikace může otevřít jinou aplikaci
- kliknutí na notifikace prodje skrz (clickjacking)

Idea: vytvořit notifikaci, která bude vypadat jako normální aplikace

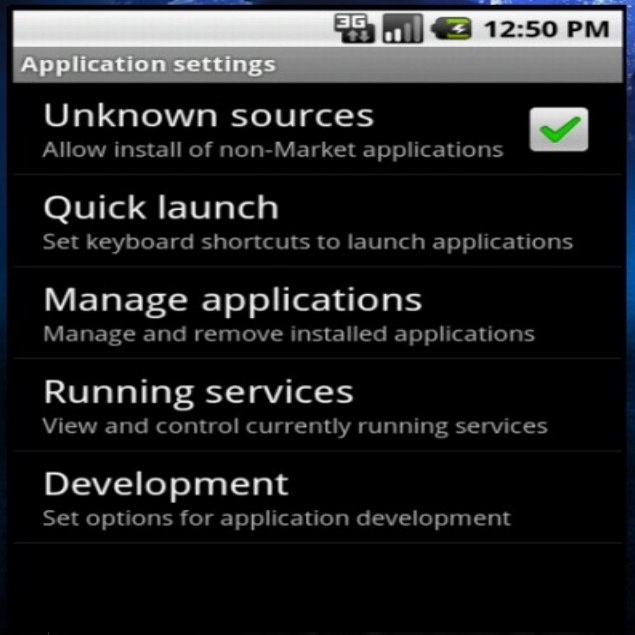
UI Redressing Attack

UI Redressing Attack

UI Redressing Attack



UI Redressing Attack



Application settings

Allow the installation of non-Market applications:
5 touch gestures

WebView exploit

Reakce uživatelů:

- android nejde napadnout návštěvou webové stránky
- není se čeho bát
- stačí mít čistou instalaci Androidu
- instalovat aplikace pouze z Google Play

Building Web Apps in WebView

HACKERFest 2014

GOPAS
POCITACOVA.SKOLA.CZ

Android exploitace

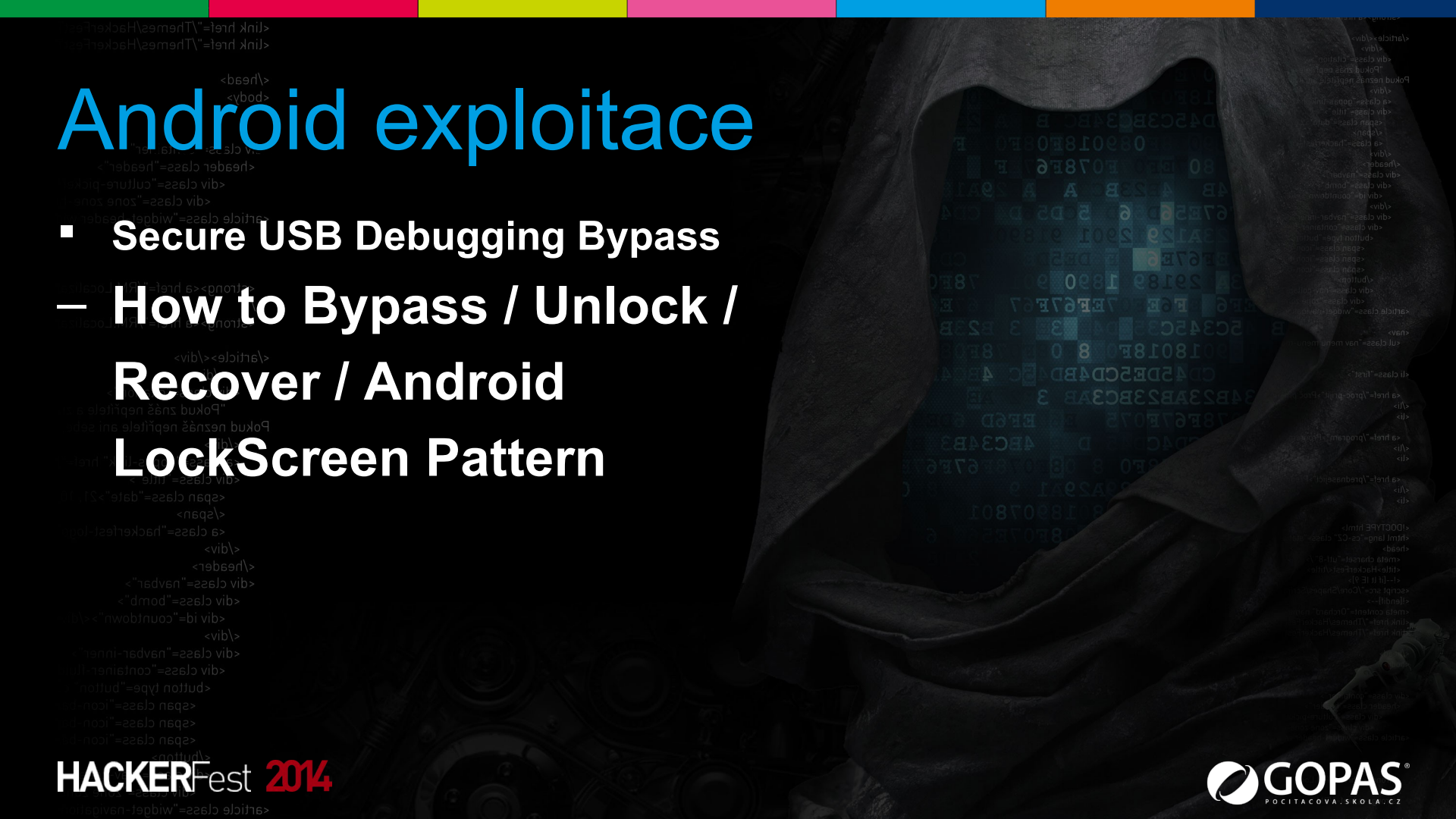
- **Secure USB Debugging Bypass**

Android exploitace

- **Secure USB Debugging Bypass**

Android exploitace

- Secure USB Debugging Bypass
- How to Bypass / Unlock / Recover / Android LockScreen Pattern



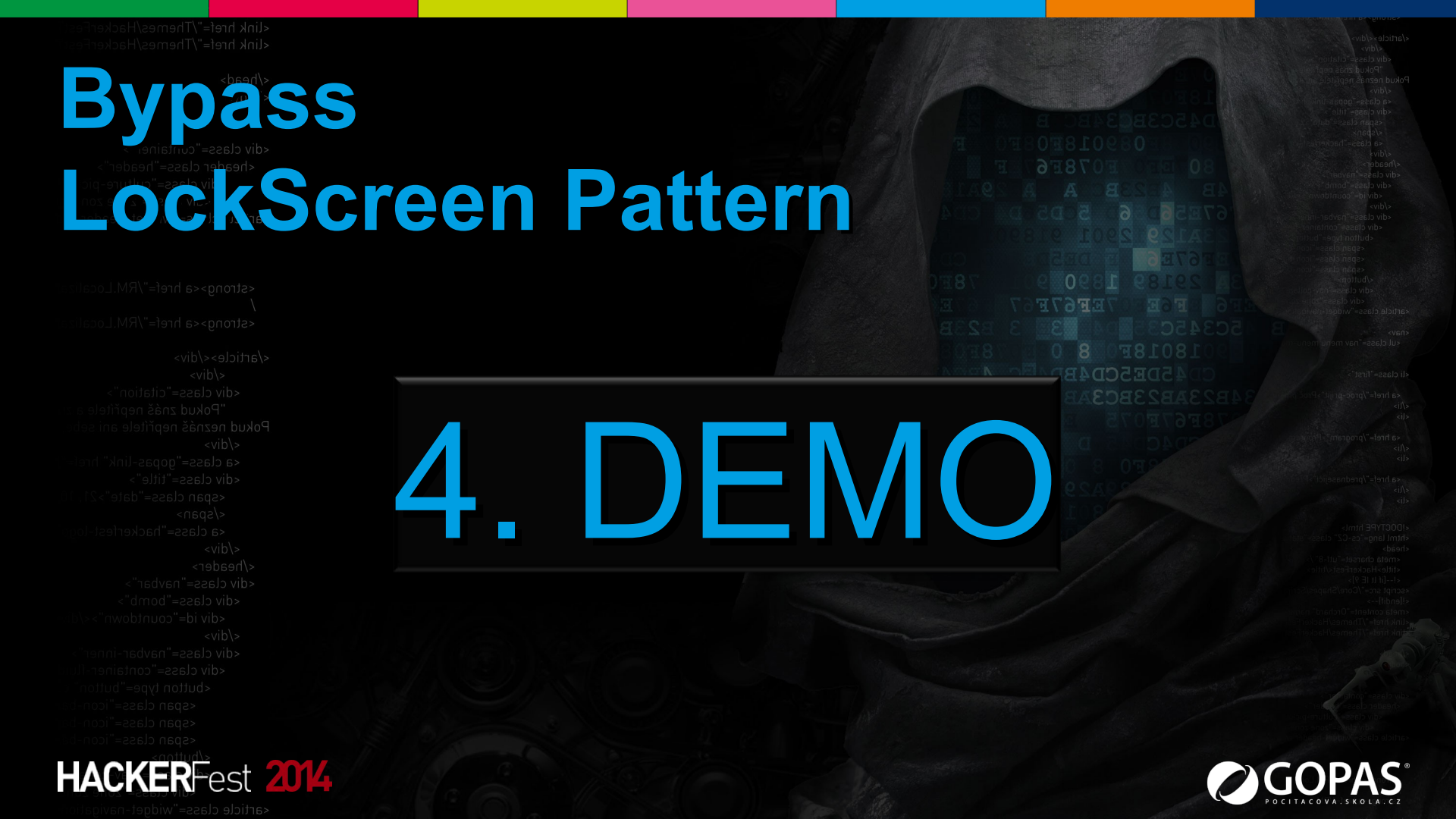
Android exploitace

- adb shell
- cd /data/data/com.android.providers.settings/ databases sqlite3 settings.db
- update system set value=0 where name='lock_pattern_autolock';
- update system set value=0 where name='lockscreen.lockedoutpermanently';
- .quit

Android exploitace

- adb shell rm /data/system/gesture.key
- Reboot when done.
- **Step 3.** When device reboots, you will still see a pattern lock screen. But here's the catch: just try any random pattern and it may unlock then remove the pattern from settings.

Bypass LockScreen Pattern



HACKERFest 2014

GOPAS
POCITACOVA.SKOLA.CZ

Hacking Android Smartphones

- webview_addjavascriptinterface
- Metasploit module

- msf >
  - use exploit/android/browser/webview_addjavascriptinterface

WebView exploit

Reakce uživatelů:

- android nejde napadnout návštěvou webové stránky
- není se čeho bát
- stačí mít čistou instalaci Androidu
- instalovat aplikace pouze z Google Play

webview_addjavascriptinterface

5. DEMO

Hacking Android Smartphones

HACKERFest 2014

GOPAS
POCITACOVA.SKOLA.CZ

Kali Pwn Pad

- Společnost Pwnie Express, zaměřující se na hardwarové bezpečnostní nástroje, představila v Březnu roku 2013, na bezpečnostní konferenci RSA v San Franciscu, svůj nový produkt

Kali Pwn Pad

HACKERFest 2014

GOPAS
POCITACOVA.SKOLA.CZ

Pwn Pad ~ závody ve zbrojení

- „Každý pentester, kterého znám, má smartphone, tablet a notebook, ale nikdo z nich tablet nepoužívá k reálným pentestům“, řekl tehdy v rozhovoru Dave Porcello, Pwnie Express CEO.

Pwn Pad ~ závody ve zbrojení

HACKERFest 2014

GOPAS
POCITACOVA.SKOLA.CZ

Pwn Pad ~ závody ve zbrojení

HACKERFest 2014

GOPAS
POCITACOVA.SKOLA.CZ

Pwn Pad ~ závody ve zbrojení

HACKERFest 2014

GOPAS
POCITACOVA.SKOLA.CZ

Pwn Pad ~ závody ve zbrojení

HACKERFest 2014

GOPAS
POCITACOVA.SKOLA.CZ

Pwn Pad ~ závody ve zbrojení

HACKERFest 2014

GOPAS
POCITACOVA.SKOLA.CZ

Pwn Pad ~ závody ve zbrojení

HACKERFest 2014

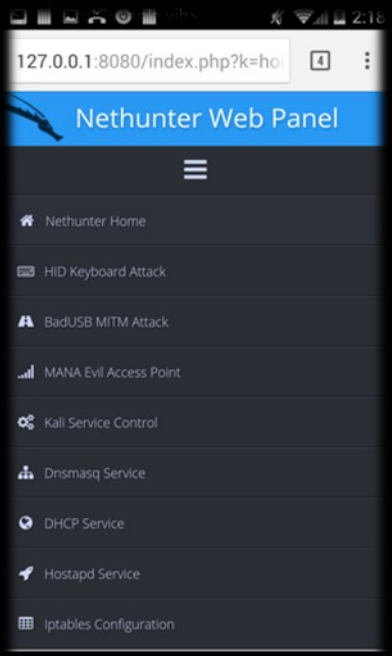
GOPAS
POCITACOVA.SKOLA.CZ

Net Hunter

- Nexus 5 smartphone
- Android & Kali Linux

- **Více info na:**
- http://nethunter.com/

Net Hunter



HACKERFest 2014

GOPAS
POCITACOVA.SKOLA.CZ

Net Hunter

8. DEMO

HACKERFest 2014

GOPAS
POCITACOVA.SKOLA.CZ

Net Hunter

9. DEMO

HACKERFest 2014

GOPAS
POCITACOVA.SKOLA.CZ

Kdo jsem ?

- Kamil Vávra
  - 23 let
  - Brno
  - Správce počítačové sítě
- vavkamil@gmail.com
- twitter.com/vavkamil