Into The Droid

Gaining Access to Android User Data
Introduction

• Why this talk is useful
  • Defend access / gain access
  • Device seizure, loss, border crossing, stop and search, espionage...

• The company
  • viaForensics - Mobile security and digital forensics, strong R&D team, government agencies and corporations

• The speaker
  • Thomas Cannon - Director of Breaking Things
Challenges

- ADB off by default
- Screen lock
- Code signing for updates and boot images
- Encryption
- Variety of device hardware, software and configuration
Bootloader Essentials

- How we use the bootloader
- Accessing bootloader mode
- Bootloader protocols
- Bootloader protection
Defeat The Bootloader

• S-ON vs S-OFF

• @secuflag controlled in radio firmware

• Gold Card - specially formatted MicroSD card can bypass carrier ID check when flashing ROMs

• White Card - special SIM card used as an authentication token to control access to diagnostic mode
Defeat The Bootloader

- Emulate White Card with hardware, combine with Gold Card to enter diagnostics and clear S-ON
Defeat The Bootloader

- White Card not needed for CDMA phones
- Once S-OFF, can RAM load a custom boot image
- This technique wipes most devices! But not all.
- Successfully used this technique to gain access to some locked stock HTC devices such as HTC Desire
- Try it yourself with an XTC Clip
Forensic Boot Image

- Start early in the boot chain before the system loads
- Provide ADB root shell over USB which can be used to image the device
- Do not mount anything, including cache, to prevent any writes to partitions
- Devices with raw NAND flash and wear levelling implemented in software (YAFFS2) can be prevented from overwriting deleted data
Build Boot Image

$ abootimg -x stock-recovery.img
$ abootimg-unpack-initrd
$ cd ramdisk
(edit ramdisk contents)
$ cd ..
$ abootimg-pack-initrd -f
$ abootimg -u stock-recovery.img -r initrd.img
RAM Disk Contents

/dev
/proc
/sbin
  adb
  busybox (+ symlinks)
  nanddump (to dump partitions)
/sys
init
default.prop (enable root shell, ro.secure=0)
init.rc (do not mount partitions, just start adb)
ueventd.rc
Flash and RAM Load

- Samsung
  - Dump partitions with ODIN <= 1.52 or Heimdall. Maybe.
  - Flashing with ODIN or Heimdall
    - heimdall flash --recovery recovery.bin (Epic 4G)
    - heimdall flash --kernel zImage (Galaxy S)
- HTC
  - fastboot boot recovery.img (RAM Loading)
  - fastboot flash recovery recovery.img (flash partition)
- Motorola
  - sbf_flash image name.sbf (make sure it only contains recovery)
JTAG Primer

- How it works
- Flasher Box
  - ORT
  - RiffBox
- Medusa Box
Serial Debug Cable

- Some devices have debug access via serial cables which can be used to gain access to data.

- On Samsung Galaxy SII / Galaxy Note this is activated by grounding ID pin of USB with a 523K ohm resistor.

- TTL serial access provided on D+ and D- pins of USB connector.

- Use a Bus Pirate and MicroUSB breakout board to connect.
Crack PIN or Password

• Salt
  - /data/data/com.android.providers.settings/databases/settings.db
  - SELECT * FROM secure WHERE name = 'lockscreen.password_salt'

• PIN / password
  - /data/system/password.key
  - Salted SHA1 of password concatenated with salted MD5
Crack PIN or Password

- Calculate the value of the salt in lowercase hex with no padding

```
$ python -c "print '%x' % 720624377925219614"
```

a002c0dbeb8351e

- Copy the last 32 bytes of password.key (MD5 hash in hex), add a colon and then add the salt

5D8EC41CB1812AC0BD9CB6C4F2CD0122:a002c0dbeb8351e

- Crack with software such as oclHashcat-lite
HID Brute Force?

Video
HID Brute Force

- AVR ATMEGA32U4 emulates USB keyboard typing PINs
- USB OTG cable for USB host
- Devices usually rate limit attempts and wipe after too many incorrect passcodes
Android Encryption

About phone

Status
Phone number, signal, etc.

Legal information

Model number
Nexus S

Android version
4.0.4

Baseband version
I9020XXKI1

Kernel version
3.0.8-g6666123
android-build@ybs1 #1
Thu Feb 2 16:56:02 PST 2012

Build number
IMM76D

Encrypt phone

You can encrypt your accounts, settings, downloaded apps and their data, media, and other files. Once you encrypt your phone, you must enter a numeric PIN or password to decrypt it each time you power it on: you can’t unencrypt your phone except by performing a factory data reset, erasing all your data.

Encryption takes an hour or more. You must start with a charged battery and keep your phone plugged in until encryption is complete. If you

Encrypting

Wait while your phone is being encrypted. 5% complete.
Android Encryption

- Supported since Android 3.0
- Based on dm-crypt
- AES 128 CBC
- Implementations may vary, e.g. Samsung has their own key management module
Android Encryption

Password/PIN → PBKDF2 x2000

/dev/urandom → Salt (128 bit)

Master Key (128 bit) → Key (128 bit)

Keylen=32 → Key+IV (32 bytes)

Key (128 bit) → AES 128 CBC

Encrypted Master Key (128 bit) → IV (128 bit)
Android Encryption

Master Key (128 bit) → IV (ESSIV:SHA256) → dm-crypt AES 128 CBC → Encrypted userdata partition → userdata partition
Cracking Encryption

• Encrypted Master Key + Salt stored in footer

• Footer stored at end of partition or in a footer file on another partition or as a partition itself

• Image device and locate footer + encrypted userdata partition
Cracking Encryption

• Parse footer

• Locate Salt and Encrypted Master Key

• Run a password guess through PBKDF2 with salt, use resulting key and IV to decrypt master key, use resulting master key to decrypt first sector of encrypted image.

• If password is correct, plain text will be revealed
- Cracking PINs takes seconds. Passwords are usually short or follow patterns due to being the same as the lock screen password.
Evil Maid Attack

• Load app onto system partition, wait for user to boot phone, get remote access to decrypted user data

• Rootkits - easy to compile for Android

• Evil USB charger
Reverse Shell

- App with no permissions can create a reverse shell, giving remote access to attacker
Desperate Techniques

- Hard reset - some devices prior to 3.0 did not wipe data properly. Wipe, boot, root and recover

- Chip-off - de-solder NAND chips

- Screen smudges
More Techniques!

• Custom update.zip - can you get one signed?

• Race condition on updates via SD cards - fixed

• Own a CA? Who doesn't these days? MITM connection, push app, update or exploit

• Entry via Google Play, if credentials cached on desktop
Santoku Linux

- Free and open bootable Linux distribution full of tools
- Project is a collaboration with other mobile security pros
- Mobile Forensics
- Mobile App Security Testing
- Mobile Malware Analysis

Check out the Alpha release at https://santoku-linux.com
Thank you!

Thomas Cannon

@thomas_cannon
github.com/thomascannon
tcannon@viaforensics.com