

Carnegie Mellon University

This video and all related information and materials (“materials”) are owned by Carnegie Mellon University. These materials are provided on an “as-is” “as available” basis without any warranties and solely for your personal viewing and use.

You agree that Carnegie Mellon is not liable with respect to any materials received by you as a result of viewing the video, or using referenced websites, and/or for any consequences or the use by you of such materials.

By viewing, downloading, and/or using this video and related materials, you agree that you have read and agree to our terms of use (www.sei.cmu.edu/legal/).

© 2015 Carnegie Mellon University.

Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM-0002554



Enhancing Mobile Device Security

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Jose Andre Morales, Ph.D.



Introduction

Talk about

- How mobile devices are currently protected
- What is not protected → private data! And why
- Options to protect private data with fake data
- Prototype construction and testing
- Defensive and offensive options: leveraging GPS and fake data

Current State of the Art

Mobile devices have:

- Encryption – avoid physical access
- Anti-malware – signature based
- Static analysis tools – post infection
- Dynamic analysis tools – heuristic
- Passwords – typically 4 characters!
- Privacy settings – apps and notifications
- OS level app/process isolation (linux)

Overall not bad **BUT** malware just needs your permission!

- App install all or nothing model eases malware introduction!
 - PII at risk!

A potential solution

How can PII be protected from malicious use and exfiltration by an app?

- Purposely provide fake PII! And other data
- Benefits:
 - App cannot distinguish fake from real
 - App will function as expected
 - User can be notified when fake data is accessed
 - User can run any app they choose while protecting their data
 - Too much fake data read? User can uninstall app
 - Data is kept safe!

Polling Question

Do you want to hear some more benefits of fake data?

Prototype

- Modified Android OS to populate random & relevant fake profiles when a phone is activated
- When an app is being installed we provide a 3rd option, called “fake”
- The app will run but will be given fake data when requested
 - Phone details
 - Photos
 - Contacts
 - Outgoing SMS
 - Geo-location (GPS)
- Providing fake data is preferred to blocking or “null” data since those can cause app to crash and destabilize device
- User notified each time fake data is read and has option to uninstall
- Serves to protect private data while user evaluates apps

Prototype testing

Tested with several apps from Google Play, Amazon, and other 3rd party markets

- Implemented in the Android OS source code, very difficult to subvert and detect
- No messages from apps indicating they suspect fake data
- Apps worked as expected, no crashes, slowdowns, or halts
- Other apps not reading fake data worked as expected
- Vast majority of apps request too many permissions and exfiltrated a lot of faked data
 - Primarily device specific data such as ID, owner email, and GPS coordinates
- Serves its purpose to empower the user to install and use desired apps with questionable permissions while protecting private data

Snapshots

Select Menu

APK4Fun

Download Fun APK for Android

Home » Apps » Productivity »
Super-Bright LED Flashlight »
Download Super-Bright LED Flashlight APK 1.0.6



Free Download Super-Bright LED Flashlight 1.0.6 APK for Android

Free [Productivity](#) App by [Launcher Apps](#)

★★★★☆ Downloads: 32727 Updated:
October 31, 2014




You have requested the file:
Name: com.surpax.ledflashlight.panel-1.0.6-APK4Fun.com.apk
Size: 4.96 MB
Uploaded: 01-11-2014 10:28
Last download: 12-01-2015 18:57

[Like](#) 2 | [Tweet](#) 0 | [PinIt](#) | [Share](#) 2


DOWNLOAD NOW

Advertisement



DOWNLOAD

Download



PLAY NOW

DOWNLOAD

Zippyshare.com News:

...and the first update of 2015 is behind us :-)
 11 Jan 2015 18:02
 After quite a long time we finally managed to put together a meaningful update. **What has been changed?** **Link format** - Link format - Links are now alphanumeric and case...

Maintenance / Technical entry
 21 Dec 2013 15:04
 Hey folks, This is maintenance/technical entry, we will update it when something goes wrong. **Edit 21.12.2013** - Sorry for a little slowdowns on 41/42 and 43/44, we had to swap ...

Quick update
 26 Oct 2013 17:51
 We are still alive! Some of You were concerned by the lack of new messages on our blog so we took the opportunity to give You an update. Everything is going fine. We don't have any particularly exc...

- To upload a file just follow these simple steps:**

 - 1) Select a file to send by clicking the "Browse" button. You can then select photos, audio, video, documents or anything else you want to send. The maximum file size is 200 MB.
 - 2) Click the "Start Upload" button to start uploading the file. You will see the progress of the file transfer. Please don't close your browser window while uploading or it will cancel the upload.
 - 3) After a successful upload you'll receive a unique link to the download site, which you can place anywhere: on your homepage, blog, forum or send it via IM or e-mail to your friends.

Benefits of using Zippyshare:

 - ✔ Zippyshare.com is completely free, reliable and popular way to store files online.
 - ✔ We offer fast download speeds.
 - ✔ The maximum filesize for a single file is 200 MB.
 - ✔ The file can be downloaded at any time and as often as you need it.
 - ✔ File Life: 30 days after no activity.
 - ✔ No ridiculous queues!
 - ✔ No limits!

Report illegal files, please [click here](#) and send full link to us!

7:11 MON, JANUARY 12



EMERGENCY CALLS ONLY



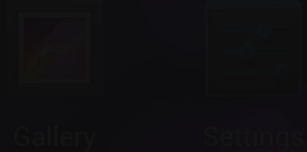
com.surpax.ledflashlight.panel.. 7:11 PM
Download complete.




USB debugging connected
Touch to disable USB debugging.



Connected as a camera
Touch for other USB options.



 Saving screenshot...



Flashlight

Do you want to install this application? It will get access to:

PRIVACY



take pictures and videos

DEVICE ACCESS



full network access

view network connections



control flashlight

prevent phone from sleeping



modify system settings

Cancel

Install

Fake

< Security

DEVICE ADMINISTRATION

Device administrators

View or deactivate device administrators

Unknown sources

Allow installation of apps from unknown sources



Verify apps

Disallow or warn before installation of apps that may cause harm



Fake option

View reports of faked personal and device information. Manage fake option preferences.

CREDENTIAL STORAGE

Trusted credentials

Display trusted CA certificates

Install from storage

Install certificates from storage

Clear credentials

Remove all certificates

6:50

< Fake option

REPORT PREFERENCES

Seafront Kite Poet	<input checked="" type="checkbox"/>
OpenWnn	<input type="checkbox"/>
com.toccatatechnologies.general.ZombieShoot02a	<input checked="" type="checkbox"/>
com.egproject.stoneofsouls	<input checked="" type="checkbox"/>
com.outfit7.talkinggingerfree	<input checked="" type="checkbox"/>
com.surpax.ledflashlight.panel	<input checked="" type="checkbox"/>
com.outfit7.talkingbenpro	<input checked="" type="checkbox"/>

6:49

< Fake option

REPORT PREFERENCES

Seafront Kite Poet	158
com.outfit7.talkinggingerfree	17
com.surpax.ledflashlight.panel	51

com.surpax.ledflashlight.panel
Access Detail


operatornumeric	38 17s
deviceid	11 18s
operatoralpha	21 18s
operatorisocountry	9 18s

Uninstall

OK

REPORT PREFERENCES

Seafront Kite Poet 158

 **Flashlight**

Do you want to uninstall this app?

Cancel OK

Defensive options

Leverage GPS and fake data

- Based on device's current location (GPS) enforce fake profile policy
 - Specify fake data as input to potentially all apps
 - Provide crafted fake data
 - Gives the illusion the device is somewhere else
 - The data is “boring” and unusable
 - System specs are not compatible: fake Android OS version
 - Result is app becomes disinterested, device and its data not a target anymore
 - Useful when device is out of home base
 - Another state, region, country
 - Civilian workforce abroad!

Polling Question

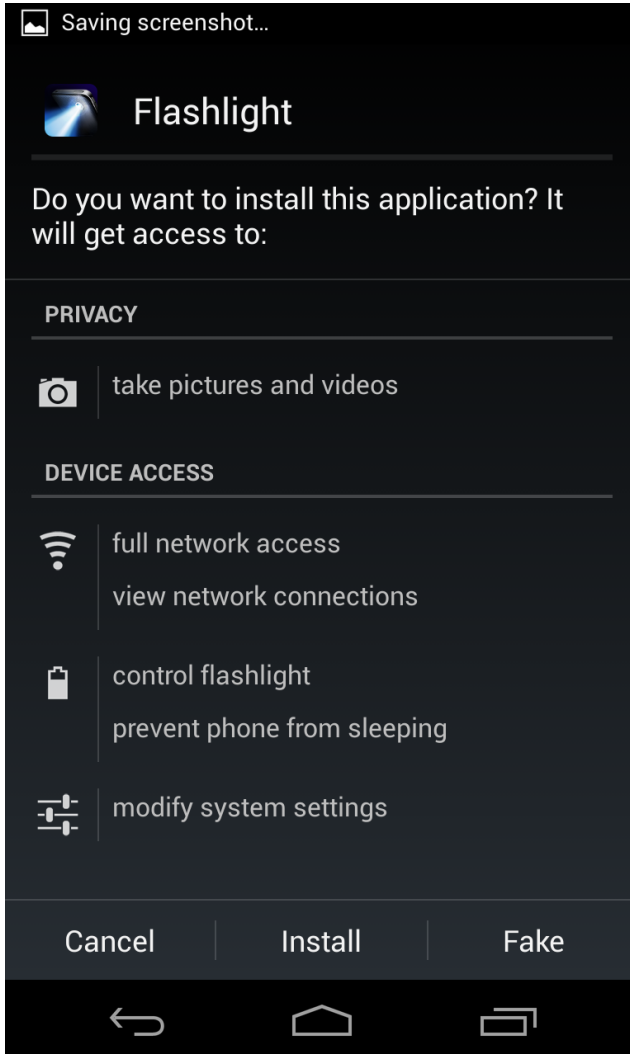
Would you like an example of “out of home base”?

Offensive Options

Purposely mislead the enemy with specific fake data

- Faking data can misinform the enemy to think what we want them to think!
- Used as a tactical device in an operation with preinstalled app:
- App designed to transmit via wifi crafted fake data based on GPS location
 - Fake GPS to predetermined location(s)
 - Mislead and position enemy to our advantage
 - Move enemy focus to bogus theatre
 - Fake contact details that we control
 - Discover their IPs
 - Cyber offensive capabilities
 - Compromise their systems
 - Fake photos and outgoing SMS messages
 - Misleading intelligence creates beneficial opportunities
 - Other limitless ideas!

Modern day ghost device army – WWII operation fortitude



Current Status

Fake profiles

- Fake data prototype up and running
- Not publicly released yet, seeking partners and evaluators

Future work

- Patch updates for fake data to commercial phone versions
- Ghost devices only in a design phase
- iOS
- Seeking stakeholders