



Mobile Security Tools for Rights Defenders and Activists

Derek Halliday
Guardian Project
<https://guardianproject.info>



About The Guardian Project

An Open Source Software project started in 2009 focused on building mobile applications and developer tools for anyone looking to protect their personal data and communications from unjust intrusion and monitoring.

About Me

My many hats include product & project management, usability testing, program deployment and training.

How dependent on your mobile devices are you?



This is a global phenomenon.



A large crowd of people gathered in a city street, with buildings and a monument in the background. The crowd is dense and extends far into the distance. The background shows a cityscape with a prominent white monument and several multi-story buildings. The overall scene suggests a significant public event or protest.

Risk & Threat Model

User Profiling

User Needs

HACKERS CAN TURN YOUR HOME COMPUTER

mobile phone

INTO A BOMB

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

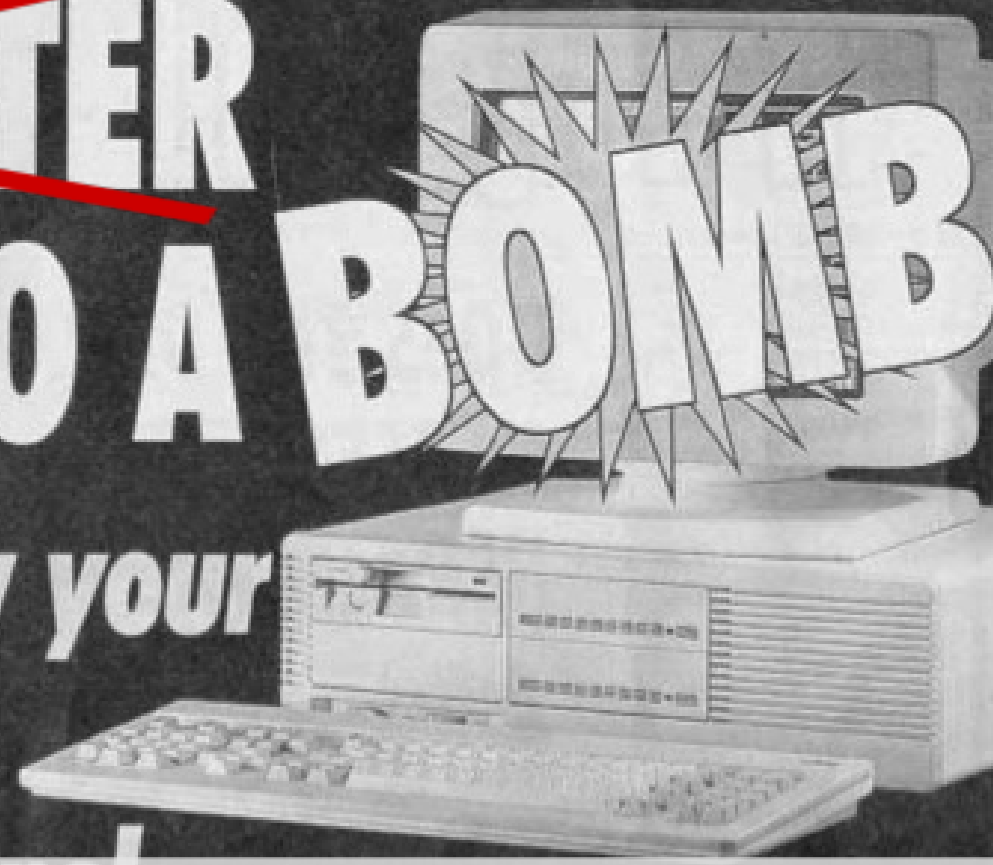
Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBay websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knock out three major online businesses are the least of our worries," Yabenson told Weekly World News.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with

... & blow your family to smithereens!



"Mobile Security" is beginning to resemble traditional enterprise security

KABOOM! It might not look like it, but an innocent home computer can be turned into a deadly weapon.

... computers work, have trouble with the things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular

"As shocking as this is, it shouldn't be the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yabenson points out that these dangerous sociopaths have already:
• Vandalized FBI and U. S. Army websites.
• Broken into Chinese military networks.

scariest," Yabenson said. "Soon it will be sold to terrorists, cults and fanatical religious-fringe groups.

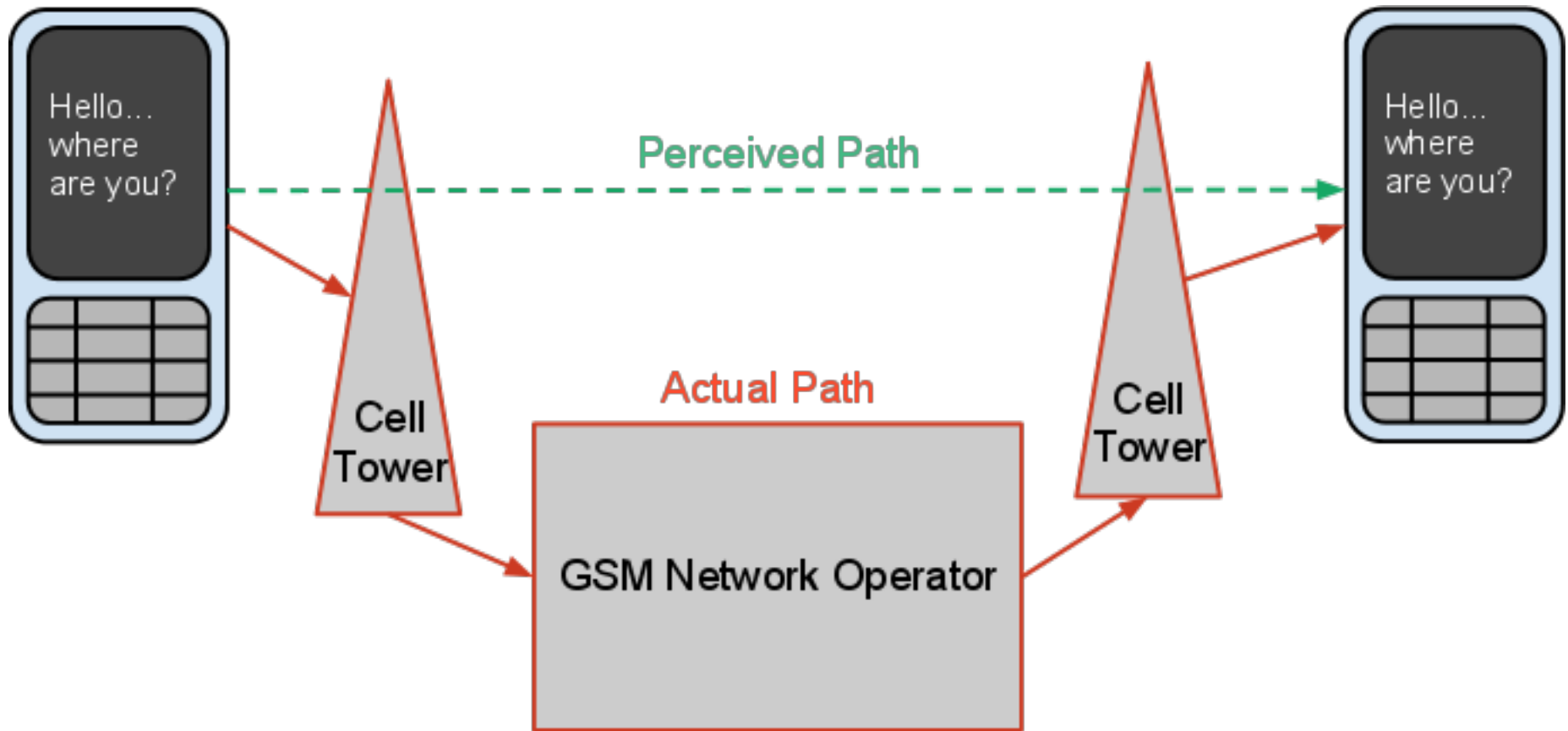
"Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

"And worse, this e-mail bomb program will eventually find its way

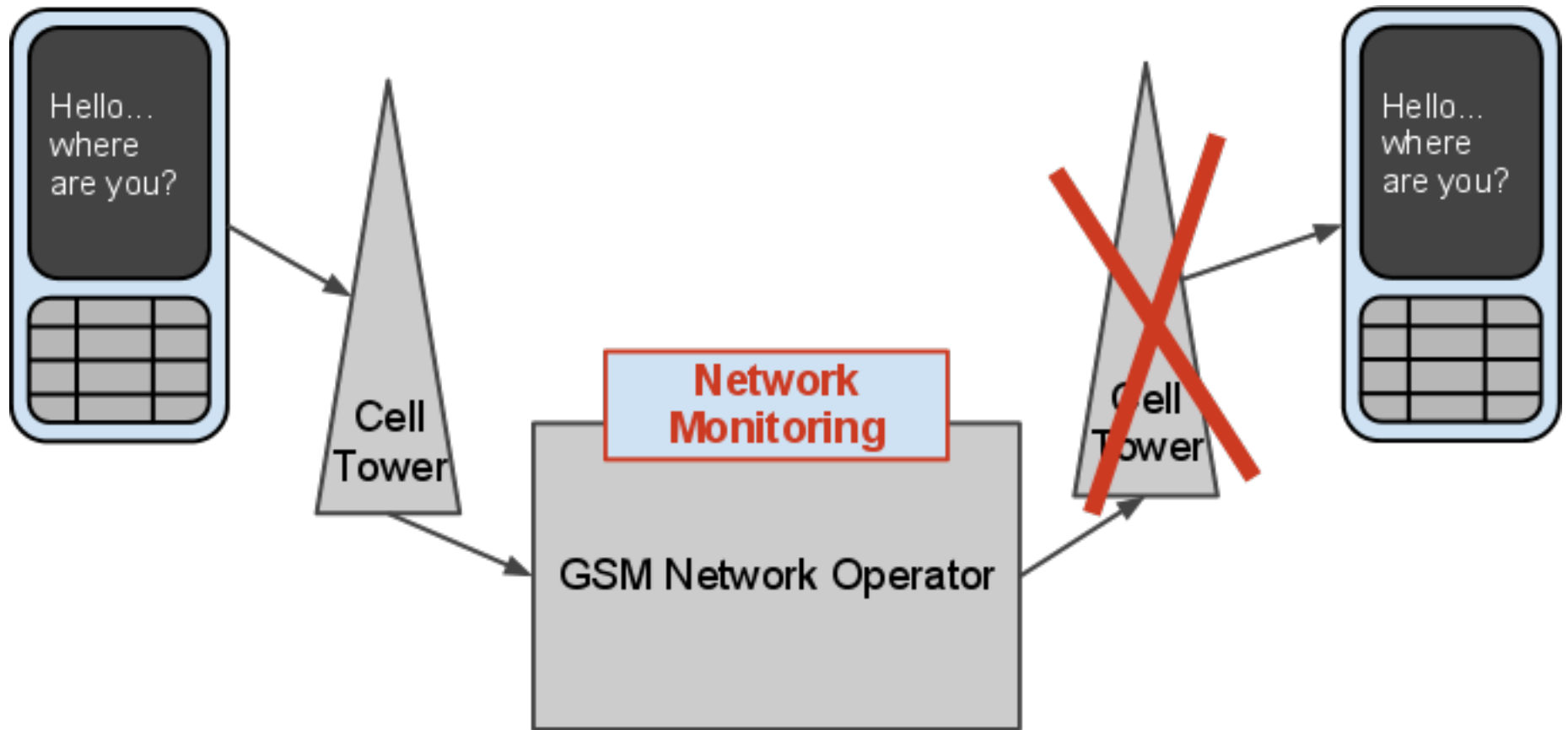
Sidras can wreak death

Activists and rights workers are often at odds with powerful local forces that include governments

Fundamental, high-level risks include wireless networks and their operators

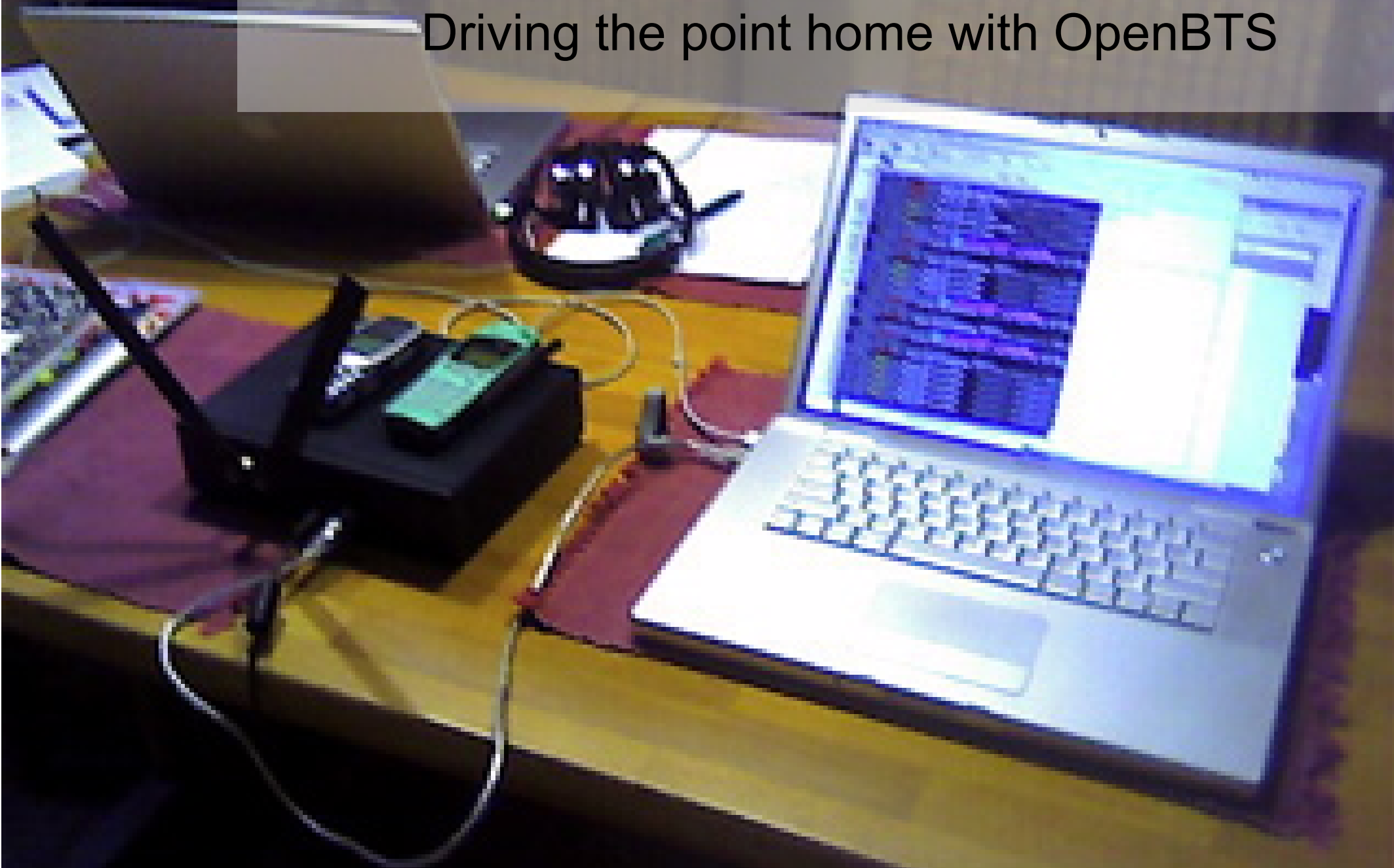


Trivial attacks include SMS filtering, call logging, targeted network shutdown



7/24/08

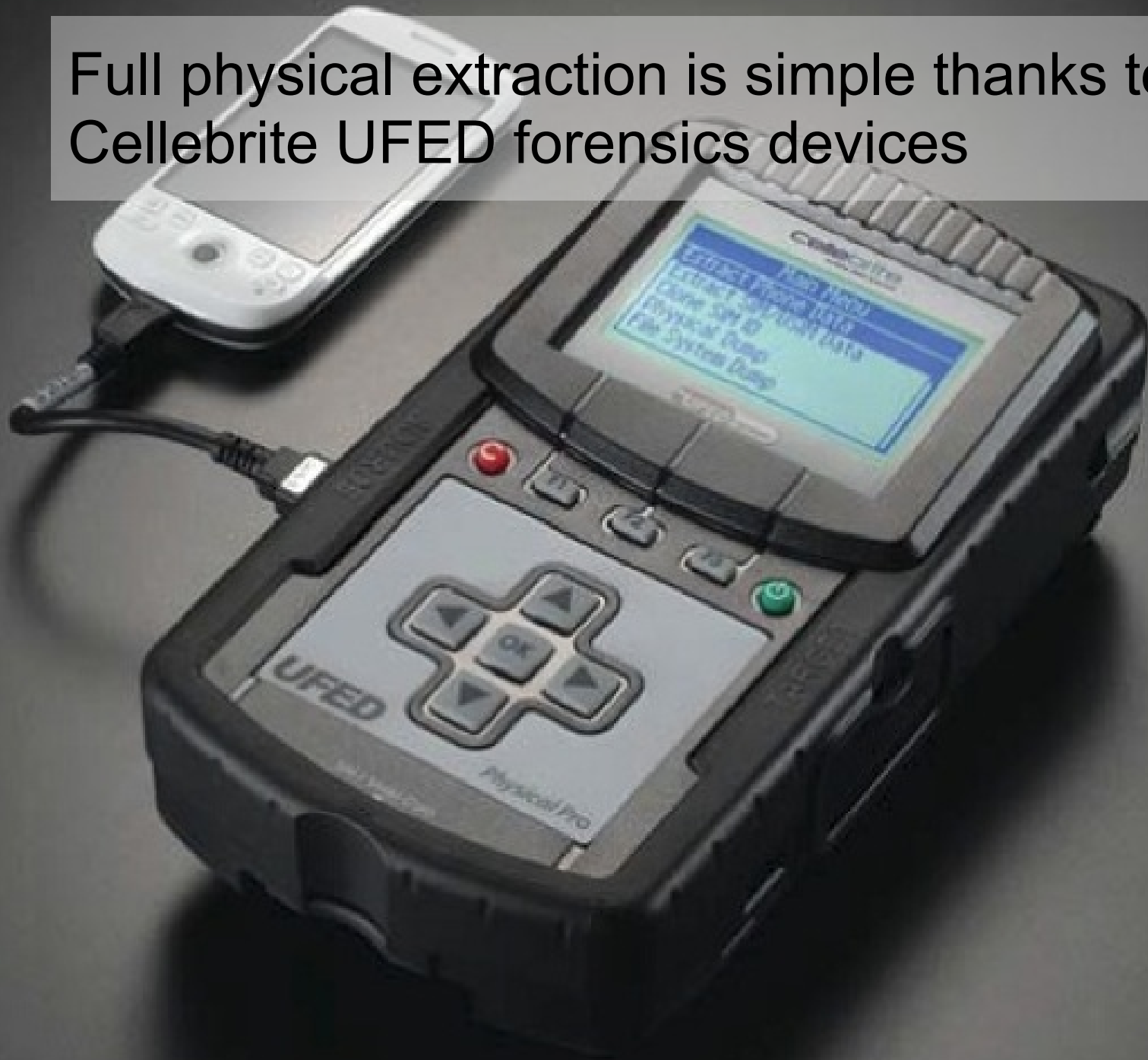
Driving the point home with OpenBTS



Arrest or inspection is often accompanied by search and seizure of mobile devices



Full physical extraction is simple thanks to Cellebrite UFED forensics devices



A large crowd of people gathered in a city street, with buildings and a monument in the background. The crowd is dense and extends far into the distance. The background shows a cityscape with a prominent white monument and several multi-story buildings. The overall scene suggests a significant public event or protest.

Risk & Threat Model

User Profiling

User Needs

Everyday Mobile Internet Freedom

Mobile users in censorship states require a usable method to circumvent content filters, firewalls and monitors. This could be for anything from watching online video to reading blogs or communicating safely with friends. The ability to access whatever content they would like encourages open society and culture.



Activists + Citizen Journalists

Citizen journalists and activists in the street need a way to safely share updates, photos and videos without interception or monitoring by the authorities.



Human Rights Researcher

An undercover human rights researcher traveling through a remote region without mobile data service needs to document local conditions using video, audio and photo capture. Encrypted on-device storage and easy permanent erasure is paramount.



Election monitoring teams need to distribute low cost devices to community organizations to report on issues. Tamper-proof, secure communication via instant messaging or email is required to coordinate volunteers and organizers.



Election Monitoring



Cost and hardware choice are essential

A large crowd of people gathered on a city street, with buildings and a monument in the background. The crowd is dense and extends far into the distance. The background shows a cityscape with a prominent white monument and several multi-story buildings. The text "Risk & Threat Model" is overlaid on the upper part of the image.

Risk & Threat Model

User Profiling

User Needs



Web Browsing



Email



Chat & SMS



Media Capture
& Sharing



Web Browsing



Tor Project



Email



PGP / GPG



Chat & SMS



Pidgin / Adium



Media Capture &
Sharing



WITNESS



We're trying to establish a set of mobile tools targeted at filling the needs of this community

Why should you care?

Brown Veto Allows Warrantless Cellphone Searches

By David Kravets   October 10, 2011 | 11:09 am | Categories: [Surveillance](#), [privacy](#)
 [@dmkravets](#) · 2,008 followers

California Gov. Jerrv Brown is vetoing

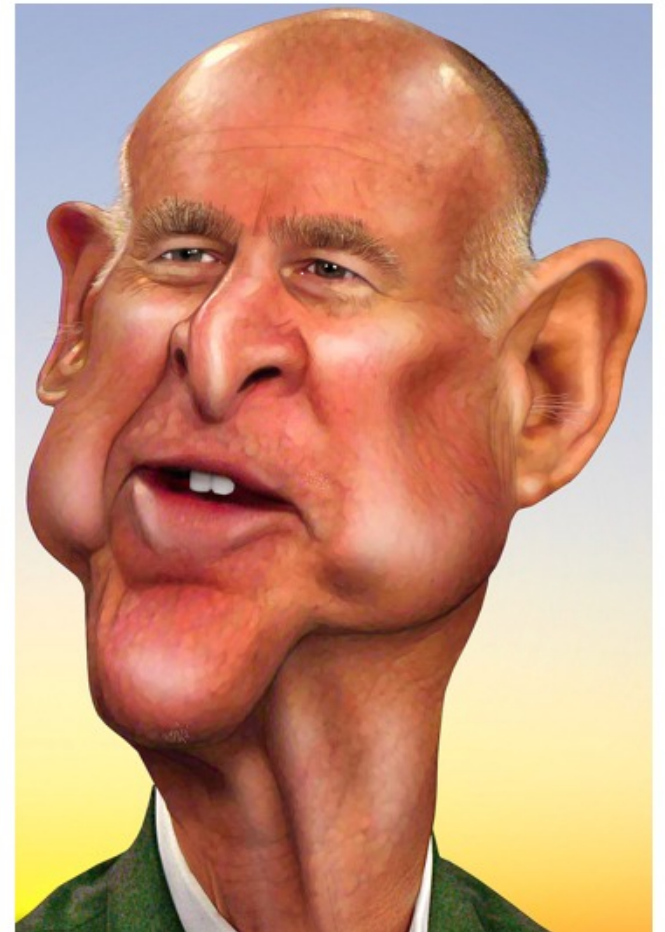
to obtain a court
ile phones of
y arrest.

ced Monday, means
ybody in the Golden
at person's mobile
ital age likely means
-mail, call records,
anking activity,
nd even where the

are given wide
incident to an
se of officer safety.
e [beginning to](#)
ss searches of
e time of an arrest.

dicated
g the rights of
alls from civil

liberties groups and this publication to sign
the bill — saying only that the issue is too
complicated for him to make a decision about.



FCC Questions BART Network Shutdown



BY KENDRA SRIVASTAVA | THU AUG 25, 2011 3:11 PM

An FCC investigator said critics of San Francisco's commuter train cell phone shutdown raise "very valid points," as the commission investigates whether the transit authority violated First Amendment rights.



Why should you care?

The screenshot shows a web browser displaying a CNN Tech article. The browser's address bar shows the URL: www.cnn.com/2011/10/10/tech/mobile/mobile-tools-for-protest/index.html. The page features a red header with the CNN Tech logo and navigation links for various news categories. The main article title is "Mobile tools for protests -- then and now" by Amy Gahran, dated October 10, 2011. A large photograph shows a crowd of people at a protest, with many holding up smartphones to take pictures. A sidebar on the right contains a "TECH: NEWSPULSE" section with several headlines and progress bars. A small advertisement is visible at the bottom right of the page.

www.cnn.com/2011/10/10/tech/mobile/mobile-tools-for-protest/index.html

SET EDITION: U.S. INTERNATIONAL MÉXICO ARABIC

TV: CNNUS CNI CNN en Español

CNN Tech

Home Video ^{BETA} NewsPulse U.S. World Politics Justice Entertainment Tech Health Living Travel Opinion IReport Money

Mobile tools for protests -- then and now

By Amy Gahran, Special to CNN
updated 4:30 PM EST, Mon October 10, 2011 | Filed under: [Mobile](#)

ADVERTISEMENT

TECH: NEWSPULSE

Most popular Tech stories right now

- Netflix whiplash stirs angry mobs -- again
- Computer virus hits U.S. drone fleet
- Cashmore: I'm in love with Siri
- Our future: Empty pockets, except for phones
- Millions without BlackBerry service

Explore the news with NewsPulse »

ADVERTISEMENT

Communicating from and about the Occupy Wall Street protests is primarily a social phenomenon.

STORY HIGHLIGHTS

Editor's note: Amy Gahran writes about mobile tech for CNN.com. She is a San Francisco Bay Area writer and media consultant who writes for [Contagious.com](#), explores how people communicate in

Waiting for i.cdn.turner.com...

The background features a dark gradient with numerous semi-transparent Android robot icons scattered across it. In the top-left corner, there is a circular graphic with a green and blue border, containing a stylized map of the world.

How can developers help?

"Too often, user privacy is an afterthought in the design of computer software and online services. In recent months, social networks have rolled back changes, cell phone manufacturers have altered the way that location tracking data is stored [...] For companies, the costs in lost consumer confidence, fines, and corrective measures can be substantial. Everyday users pay a price as well, and for victims of domestic violence, political protesters, whistleblowers, and others whose safety and livelihood could hinge on their privacy, those costs can be devastating"

- Brian Robick
ACLU, Director of Technology ACLU-WA

Design Goals

- Hide the user and their networks
- Simplify security through good UI+UX
- Consider physical and network threats
- Know the user & localize everything
- Work everyday and in crisis
- Free as in beer & free as in speech
- Support widest range of hardware





What about the apps?



The Android port of Tor, Orbot provides censorship circumvention and anonymity to mobile data traffic.



Basics:

- Designed for simplicity
- "Just works" across 2G, 3G, WiFi

Advanced:

- Transparent proxying w/ root
- Supports Tor Bridges and hidden services

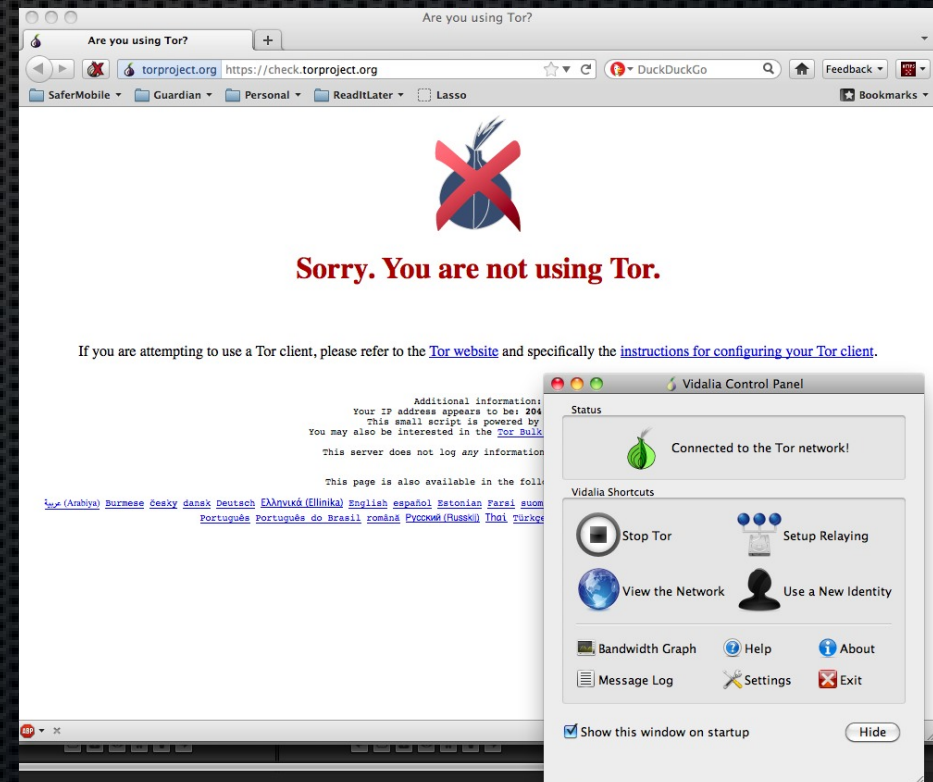


The good:

- Streamlined UI & usability compared to desktop versions of Tor
- Transparent app proxying is simple yet powerful

The bad:

- Root permissions required for custom iptables rules

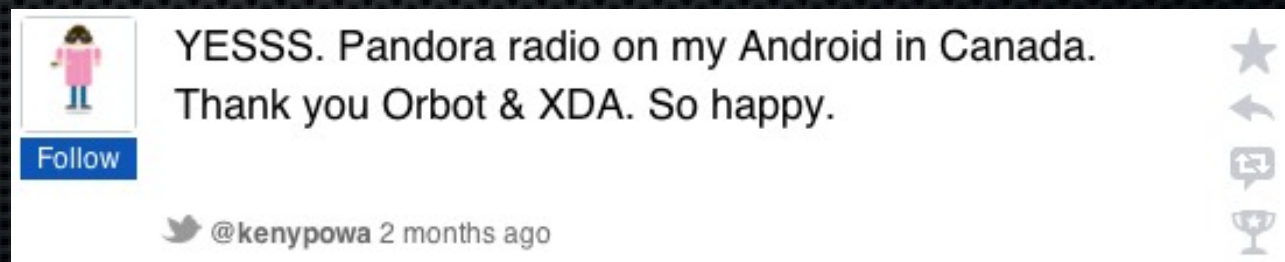




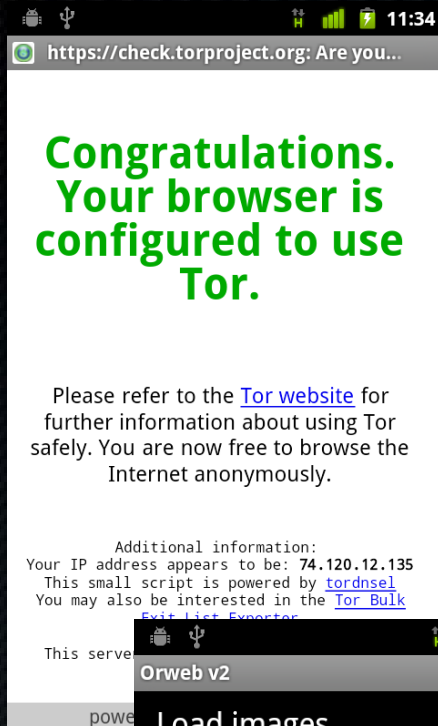
Some usage statistics - are we reaching the right users?

81,972 total installs (users)
19,587 active installs (devices)

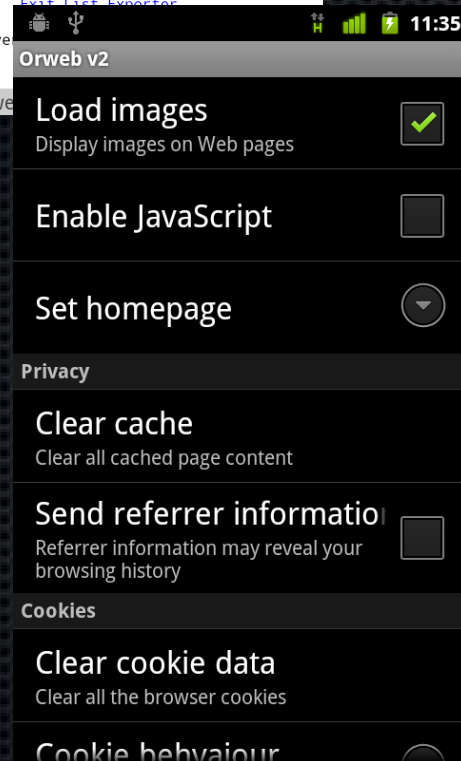
1 United States 37.6% (7,364) 2 Saudi Arabia 9.8% (1,918) 3 Germany 7.6% (1,492) 4 United Kingdom 5.0% (979) 5 France 3.4% (667) 6 Canada 2.5% (488) 7 Italy 2.3% (450) 8 Australia 2.2% (428) 9 Netherlands 1.7% (342) 10 United Arab Emirates 1.5% (303)



A screenshot of a Twitter post. On the left is a profile picture of a person with dark hair wearing a pink shirt and blue pants, with a blue 'Follow' button below it. The text of the tweet reads: 'YESSS. Pandora radio on my Android in Canada. Thank you Orbot & XDA. So happy.' Below the text is the Twitter bird icon, the handle '@kenypowa', and the text '2 months ago'. On the right side of the tweet, there are five icons: a star, a left-pointing arrow, a speech bubble with a plus sign, and a trophy.



A privacy enhanced web browser that supports proxies.



Basics:

- "Torified" web browsing allows circumvention of web filters and firewalls
- Root privileges not needed
- Simple privacy-oriented settings:
 - cookie white-listing
 - user agent manipulation, etc.



A secure, no logging instant messaging app for Android

Key Features:

- XMPP and OTR for cross-compatibility
- Usable with GTalk, Jabber or any self-hosted, secured server
 - Facebook chat (OMG!!)
- Auto-encrypts chats when avail.

Advanced Features:

- Barcode-scanner key verification
- Orbot (Tor) for anonymity



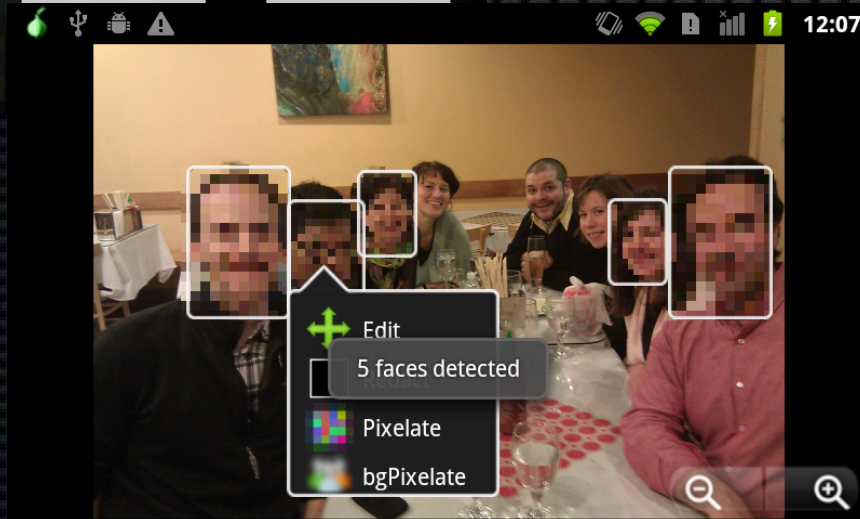
A secure camera application developed to improve visual privacy. Partnership with WITNESS.org

Features:

- Automatic face detection
 - Multiple redaction options
 - Metadata scrubbing
 - Straightforward sharing
- (android.media.FaceDetector)

Upcoming:

- Advanced metadata tools
- Video!





Time for a Demo?



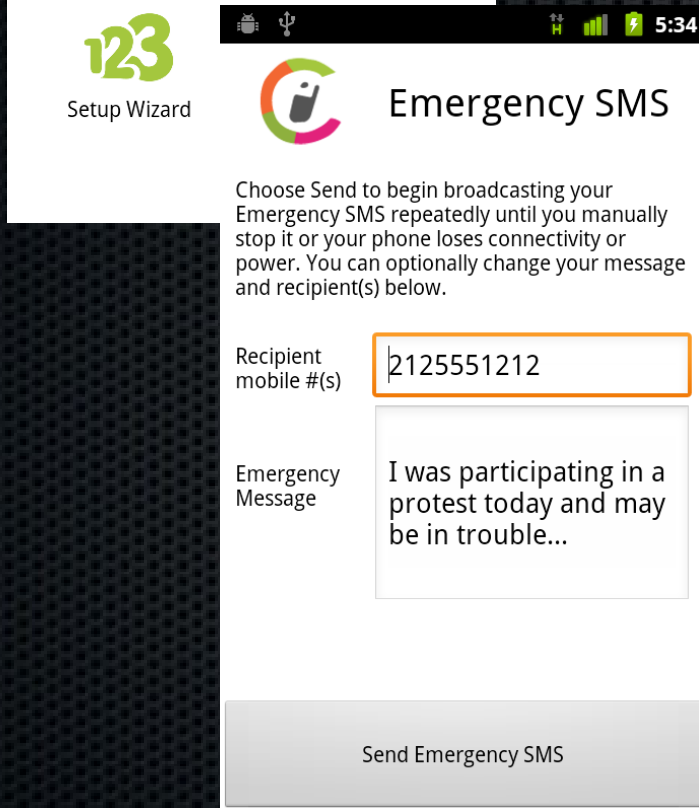
5:28



Set of tools specifically designed for those at risk of device confiscation or arrest. Currently in beta test (not yet in Market).

Basics:

- One-click emergency SMS alert
- Configurable device wipe
- Cross-platform support:
 - Android
 - Symbian / J2ME
 - BlackBerry



Other Apps - TextSecure



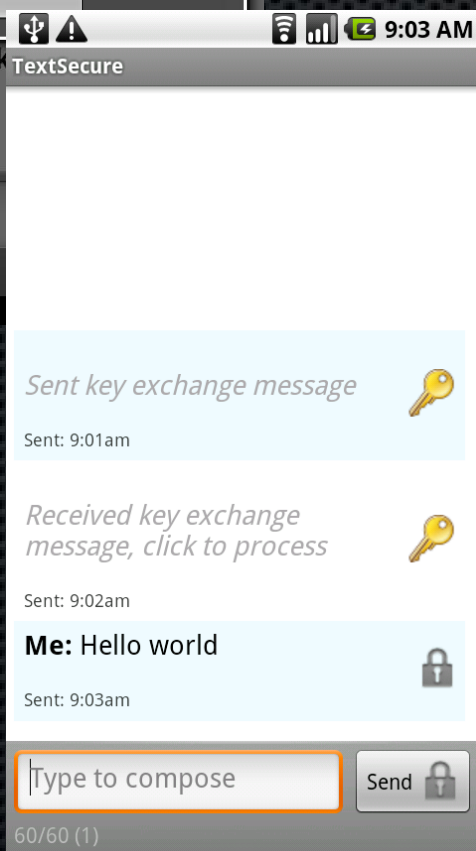
Security-enhanced text messaging application that serves as a full replacement for stock messaging application.

Pros:

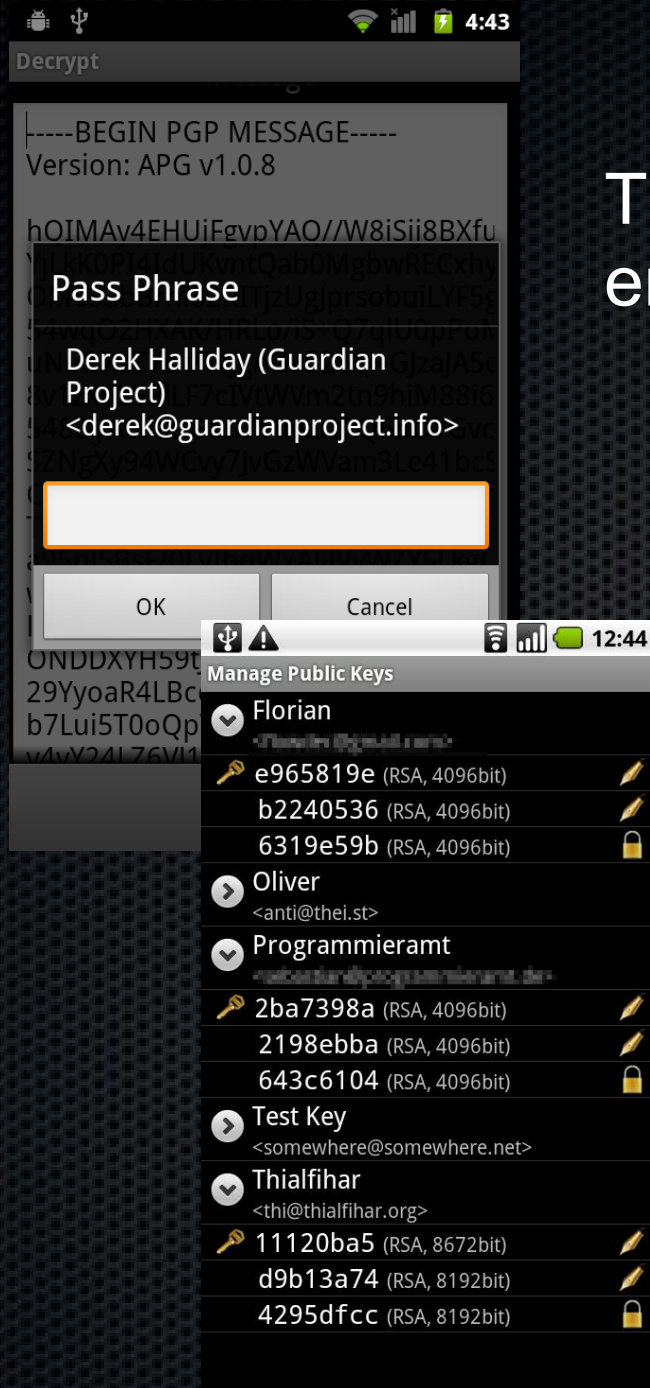
- Also based on OTR standard
- Simple / automated key exchange and verification

Cons:

- Closed source
- Vulnerable to SMS filtering attacks



Other Apps - K9 & APG



Together provide open source PGP / GPG email for mobile devices.

Pros:

- Open Source mobile PGP email (!!)

Cons:

- Some usability issues persist
- Wise to use with a separate 'mobile' keypair currently



- ORLib: a drop-in library for any Android app that wants to connect to Tor; adds SOCKS and HTTP proxying capabilities using the same standard Socket and HTTPClient libraries of Android



- SQLCipher

- An encrypted layer on top of the sqlite mobile database
- Ported from existing open-source project on iOS and WinMo, with modified "android.database" package API
- Originally developed by Zetetic (<http://zetetic.net/>)



Notecipher - a simple passphrase protected notepad app illustrating best practices for implementing SQLCipher. (in Market)



• SQLCipher - an illustrative terminal listing

```
~ sjlombardo$ hexdump -C sqlite.db
00000000 53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 |SQLite format 3.|
...
000003c0 65 74 32 74 32 03 43 52 45 41 54 45 20 54 41 42 |et2t2.CREATE TAB|
000003d0 4c 45 20 74 32 28 61 2c 62 29 24 01 06 17 11 11 |LE t2(a,b)$....|
...
000007e0 20 74 68 65 20 73 68 6f 77 15 01 03 01 2f 01 6f | the show.../.o|
000007f0 6e 65 20 66 6f 72 20 74 68 65 20 6d 6f 6e 65 79 |ne for the money|
```

versus

```
~ $ hexdump -C sqlcipher.db
00000000 84 d1 36 18 eb b5 82 90 c4 70 0d ee 43 cb 61 87 |.?6?...?p.?C?a.|
00000010 91 42 3c cd 55 24 ab c6 c4 1d c6 67 b4 e3 96 bb |.B<?U$????.?g???.?|
...
00000be0 dc 77 5c 6c de c6 d3 be 43 49 48 3e f3 02 94 a9 |?w\|??*CIH>?..?|
00000bf0 8e 99 ee 28 23 43 ab a4 97 cd 63 42 8a 8e 7c c6 |..?(#C???.?cB..|?|
```



- SQLCipher - what's required to implement?

1. Add a single sqlcipher.jar and a few .so's to the application libs directory
2. Update the import path from android.database.sqlite.* to info.guardianproject.database.sqlite.* in any source files that reference it. The original android.database.Cursor can still be used unchanged.
3. Init the database in onCreate() and pass a variable argument to the open database method with a password*:

```
SQLiteDatabase.loadLibs(this); //first init the db libraries with the context  
SQLiteOpenHelper.getWritableDatabase("thisismysecret");
```

Check out NoteCipher source for a working example:

<https://github.com/guardianproject/notepadbot>



Portable Shared Security Tokens (PSST)

- We've found that identity management is a big sticking point for many of our end-users
- What about identity tokens that can easily and securely sync between computing contexts?

Open Source Telephone Net (OSTN)

- CSipSimple is a great Open Source SIP client for Android that supports ZRTP
- Presents issues for novice (or advanced!) users on configuration
- International context of our target users poses a latency issue that, for now, is solved with "use Skype"



Thank You!

We're under active development and seeking developers, designers, users, and partners for our work.

Visit: <https://guardianproject.info>

Follow: @guardianproject

IRC: guardianproject on freenode or oftc

Code, Issues & Betas: <https://github.com/guardianproject>