Mobile Device Security

Zachary Weinberg
zackw@cmu.edu
Carnegie Mellon University

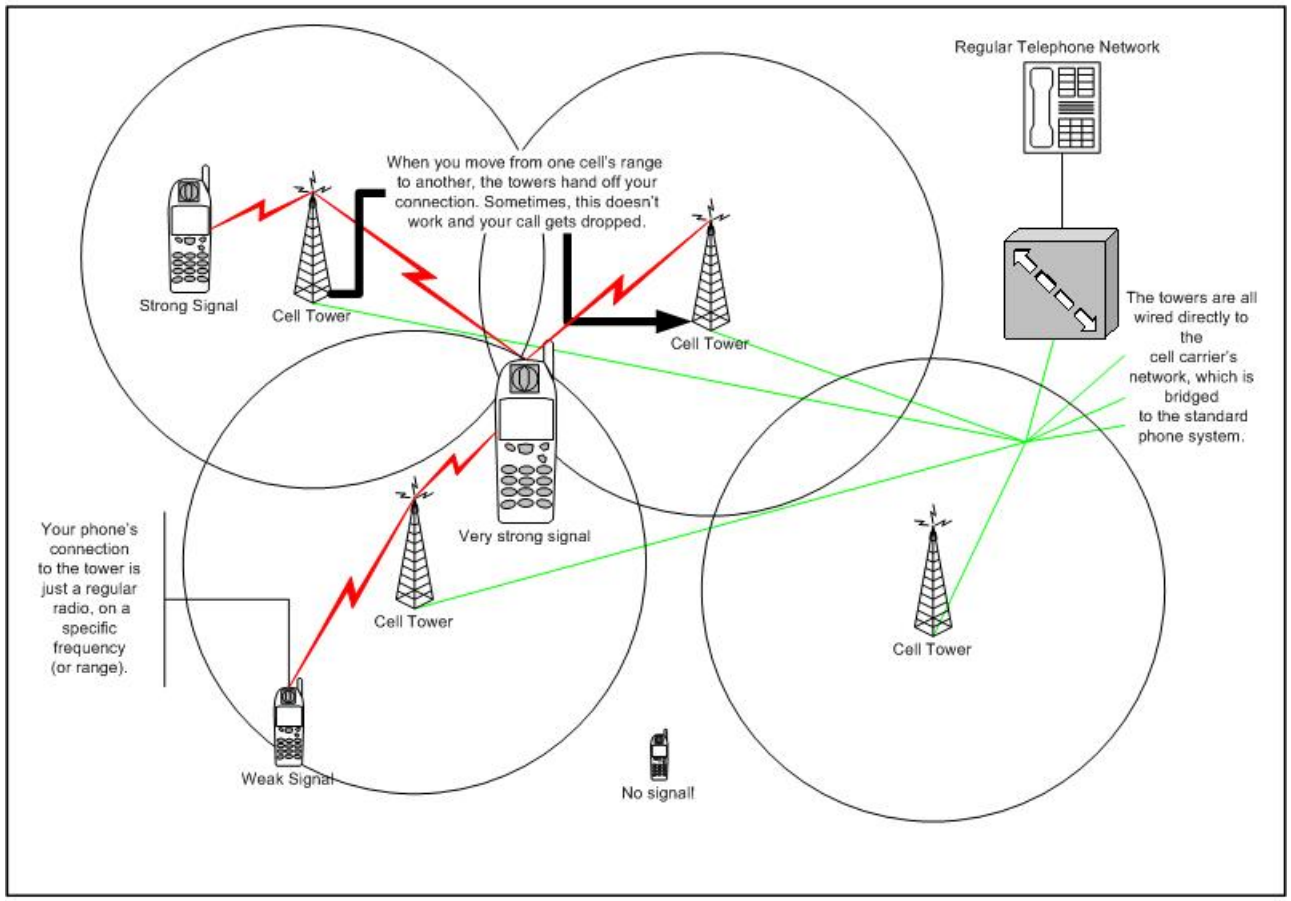
Researchers discussed

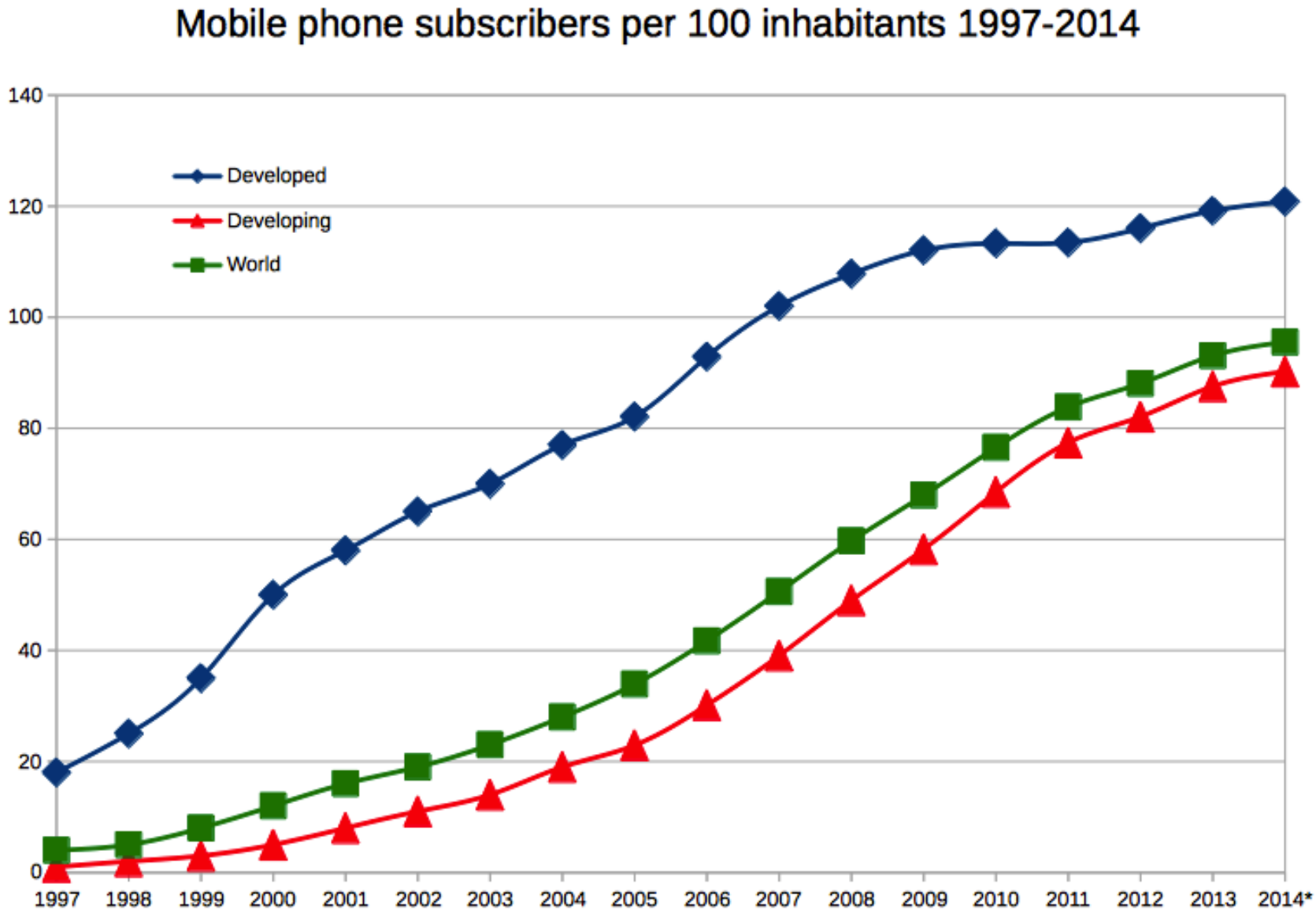
- Ravishankar Borgaonkar
- Manuel Egele
- Adrienne Porter Felt
- Nico Golde
- Karsten Nohl
- Wu Zhou
- the grugq

Cellular Telephony: Timeline

- Pagers: 1950
- Car phones: 1956
- Satellite phones: 1979
- Handheld, cellular phones: 1982
- SMS messaging: 1992
- First PDA/phone: 1993
- GPS and maps: 1999
- Cameras: 2000
- “3G” data service: 2001
- Integrated email: 2002
- Complete web browser: 2002
- iPhone: 2007
- Android: 2008
- “4G” data: 2010 (still rolling out)

What we mean by “cellular”





Source: ITU via Wikipedia

What your phone knows about you

- Phone number
- Call log
- Text messages
- Email
- Contacts
- Calendar
- Web browsing history
- Physical location
- Physical activity logs
- WiFi networks you use
- Photographs you took
- Account credentials
- Second authenticators
- Payment credentials

How to steal all this delicious data?

- Just ask for it
- Steal the phone physically
- Install malware
  - Subvert existing app
  - Subvert popular library
- Be a malicious website
  - Deliver malicious ads
- Be the network

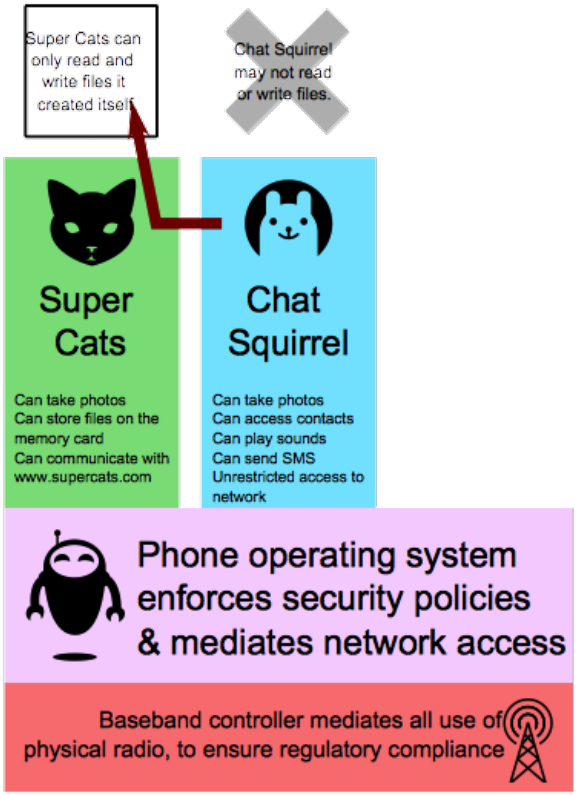
Malware is harder on mobile…

- The OS restricts each application to a limited set of privileges
- The baseband controller enforces FCC regulations
- The cell tower enforces phone company policy

Cell network tracks physical location of phone, maps phone numbers to devices, enforces usage and billing policies

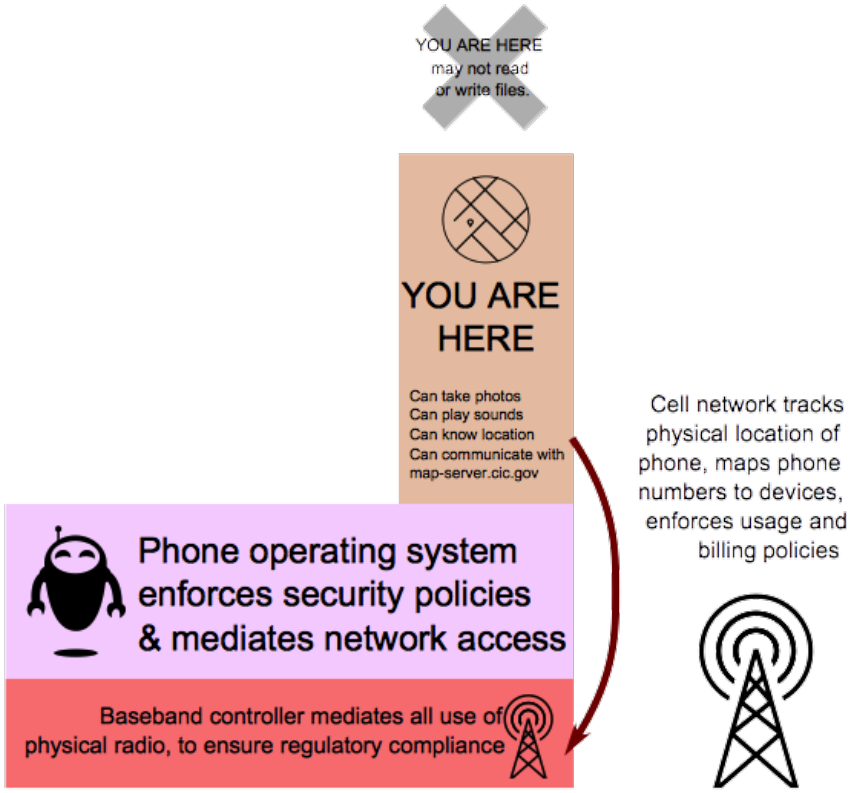
Confused deputies

- Chat Squirrel can't read or write files …
  - Maybe it can trick another application that can?



Layer bypass

- YOU ARE HERE can't talk directly to the network
  - maybe it can bypass the OS, which enforces that policy?



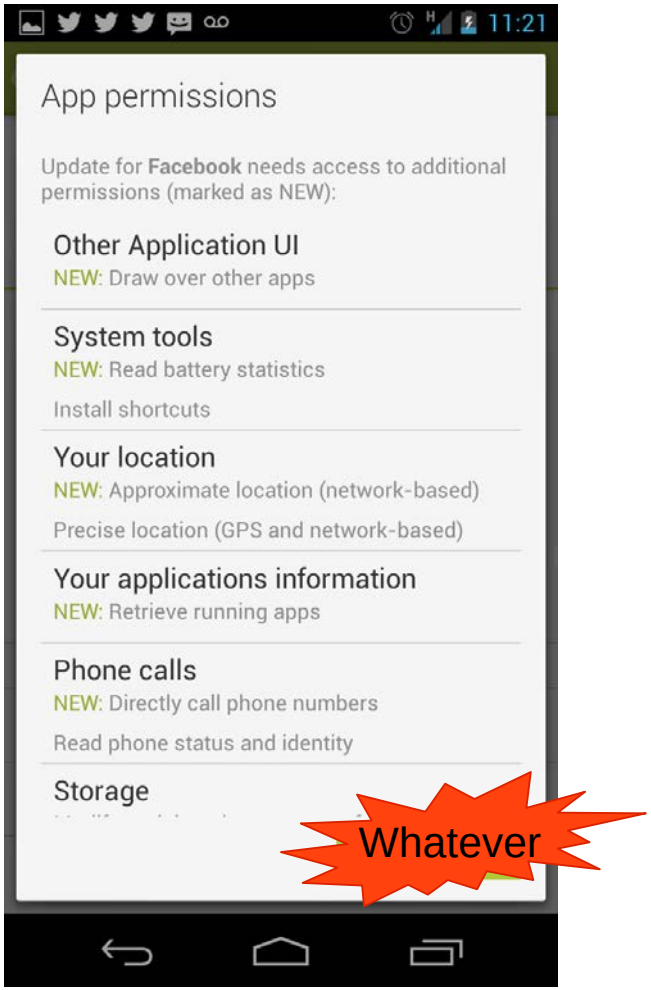
All application attacks apply

- Buffer overflow
- Use after free
- TOCTOU race
- Misuse of cryptography
- Unauthenticated TLS

- Many apps talk to websites
  - XSS?
  - CSRF?
  - SQL injection?
  - Buggy auth protocol?

Privilege creep

- You can just *ask* for lots of privileges and you'll probably get them
- Applications keep adding functionality, and new privileges



Facebook for Android update dialog

Privilege creep: flashlight apps

Flashlight Apps	 Super-Bright LED Flashlight	 Brightest Flashlight Free	 Tiny Flashlight + LED	 Flashlight	 Flashlight	 Brightest LED Flashlight	 Color Flashlight	 High-Powered Flashlight	 Flashlight HD LED	 Flashlight: LED Torch Light
Permissions										
retrieve running apps	✓					✓		✓		
modify or delete the contents of your USB storage	✓	✓				✓		✓		
test access to protected storage	✓	✓				✓		✓		
take pictures and videos	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
view Wi-Fi connections	✓	✓				✓		✓	✓	
read phone status and identity	✓	✓			✓	✓		✓		
receive data from Internet	✓					✓		✓		
control flashlight	✓	✓	✓			✓	✓	✓	✓	
change system display settings	✓					✓		✓		
modify system settings	✓					✓		✓		
prevent device from sleeping	✓							✓		
view network connections	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
full network access	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
approximate location (network-based)	✓	✓						✓		
precise location (GPS and network-based)	✓	✓						✓		
disable or modify status bar	✓	✓								
read Home settings and shortcuts	✓	✓		✓						✓
install shortcuts	✓	✓		✓						✓
uninstall shortcuts	✓	✓		✓						✓
control vibration	✓		✓							
prevent device from sleeping		✓	✓	✓		✓			✓	✓
write Home settings and shortcuts				✓						✓
disable your screen lock				✓						✓
read Google service configuration					✓				✓	

http://www.snoopwall.com/threat-reports-10-01-2014/

Ad libraries are, as usual, evil

- 1,407 iOS applications analyzed
  - (825 from App Store, 582 from Cydia)
- Pervasive ad and app-telemetry libraries
  - 772 apps (55%) contain at least one such library
- Send UDID and AppID on start, with each ad-request
  - Ad company can build detailed usage profiles
- Application has privileges it doesn't need itself

https://iseclab.org/papers/egele-ndss11.pdf

Repackaging (with malware)

- Take a legitimate application
- Combine it with off-the-shelf malware
- Re-upload to app store under new name
- You get the purchase price, the ad revenue, *and* the botnet!

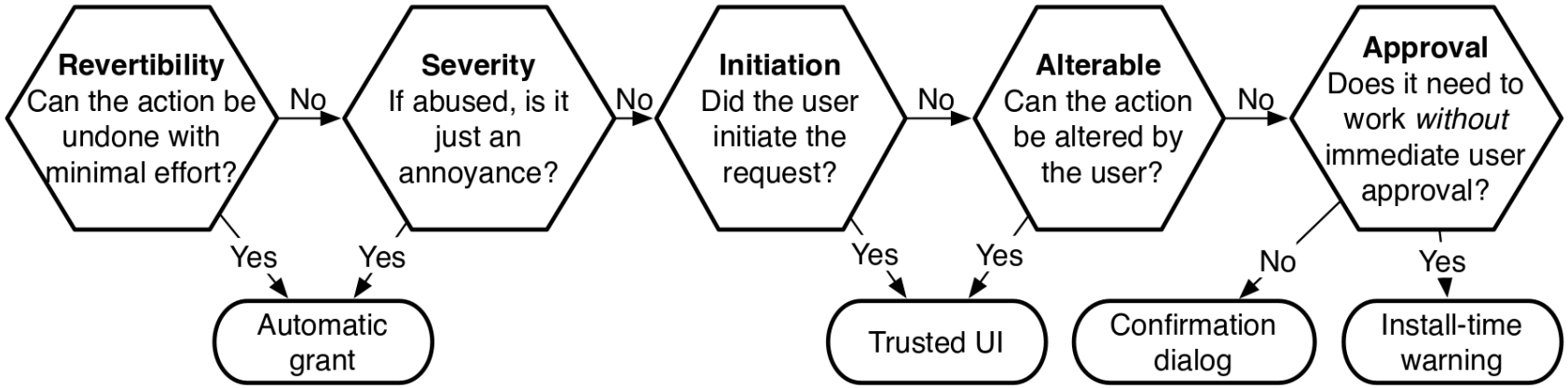
- 1083 of 1260 malware samples were this

http://www.ieee-security.org/TC/SP2012/papers/4681a095.pdf

Possible solution to privilege creep

Cosmetic changes can always be undone

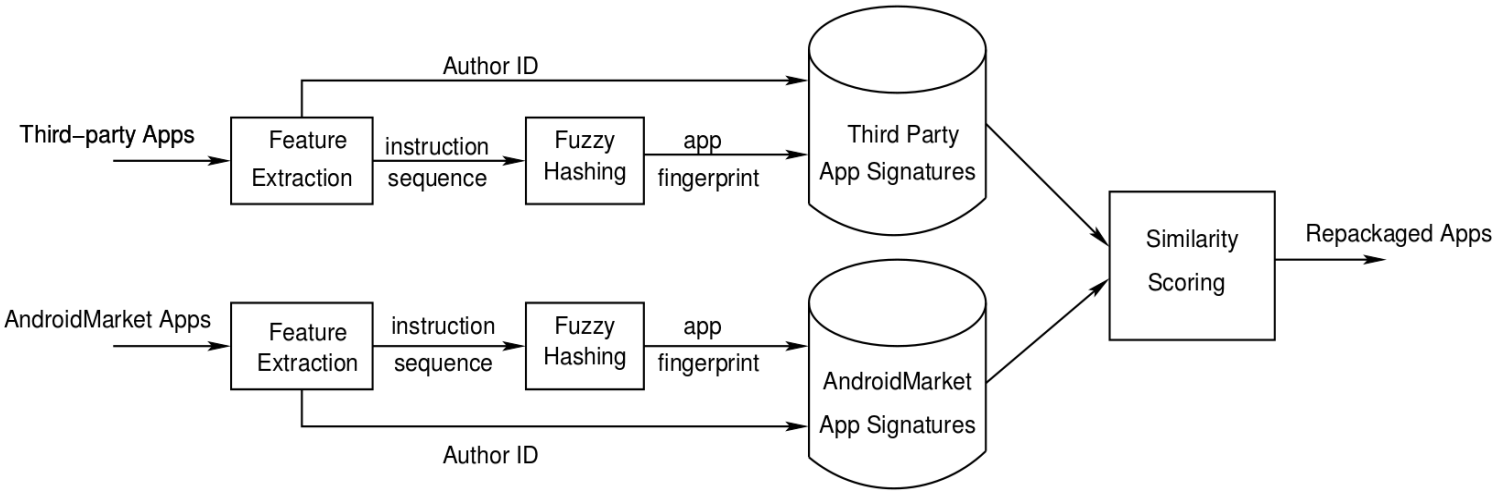
Access to files, camera, etc. infers permission from user action



https://www.usenix.org/system/files/conference/hotsec12/hotsec12-final19.pdf

Possible solution to repackaging

- Market operator can weed them out
  - Market operator has to care
  - What if market operator is the malware source?
- The original app probably wasn't obfuscated

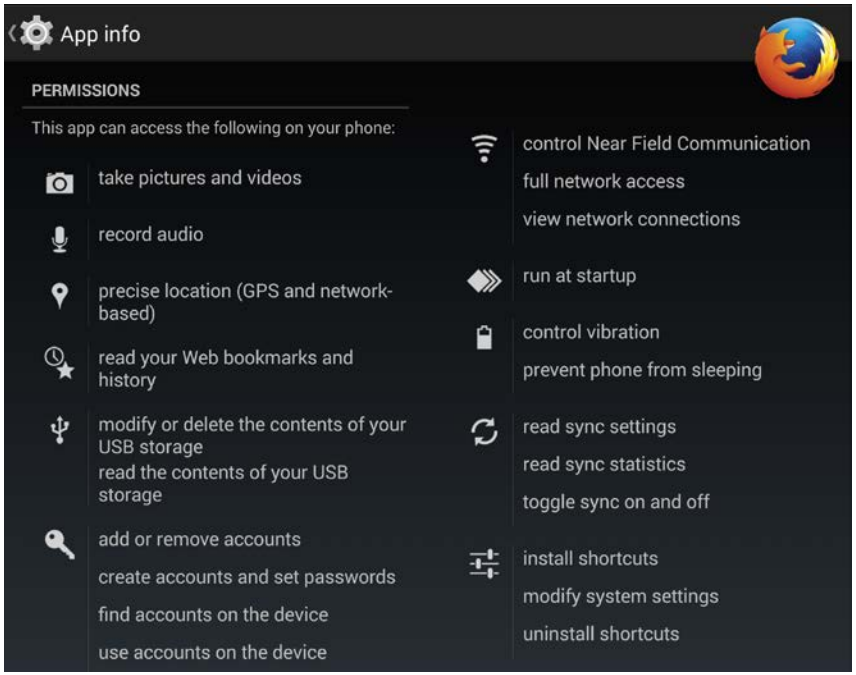


https://discovery.csc.ncsu.edu/pubs/CODASPY12.pdf

Possible solution to evil advertising

Malicious websites

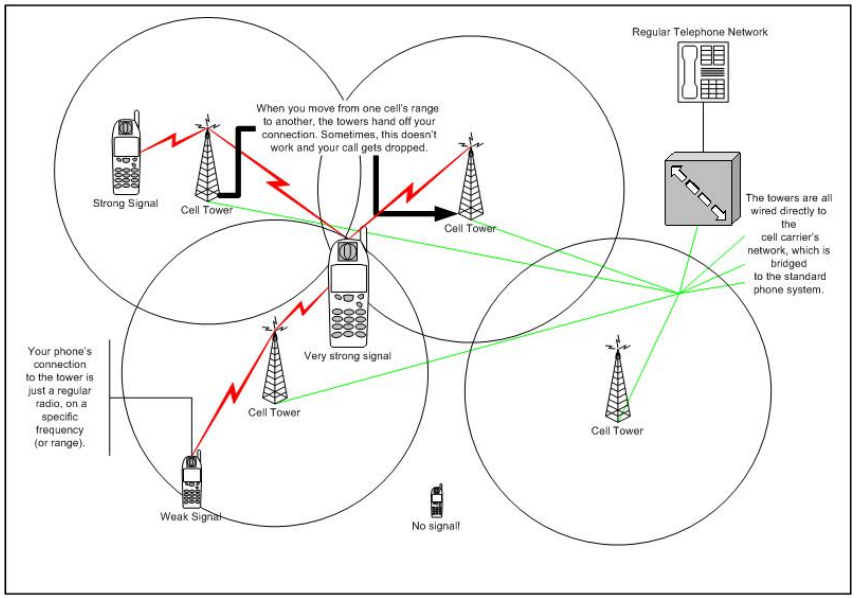
- Everything you heard in the past two lectures applies
- Browsers require a frightening number of privileges
- Mobile-variant websites get less security attention from their developers
- Apps often embed websites



Permissions list for Firefox for Android as found on my phone

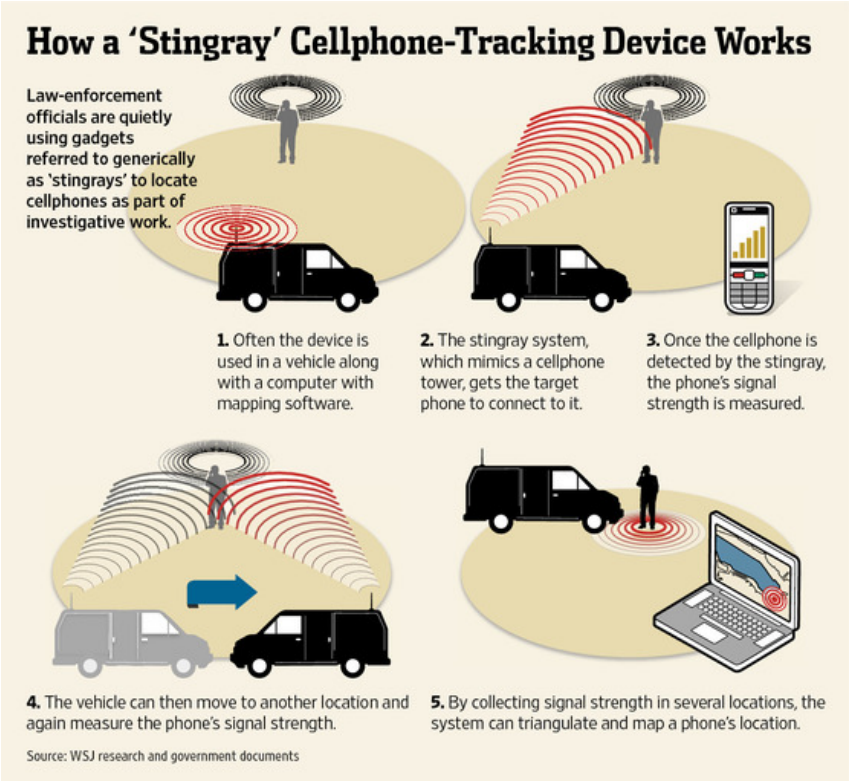
Being the network

- Cell phones implicitly trust the cell towers
- The towers know where each phone is
  - to within a city block
- Channel security is vintage 1990s proprietary, i.e. junk
- No end-to-end encryption in general



IMSI catchers

- Fake cell tower
  - Nearby; strongest signal
  - Logs devices that connect to it
  - with physical locations
- Can log all traffic
  - call/data encryption ends at the tower
- Can buy a “femtocell” for $250, r00t it, and turn it into one of these
- May be able to 0wn such devices remotely



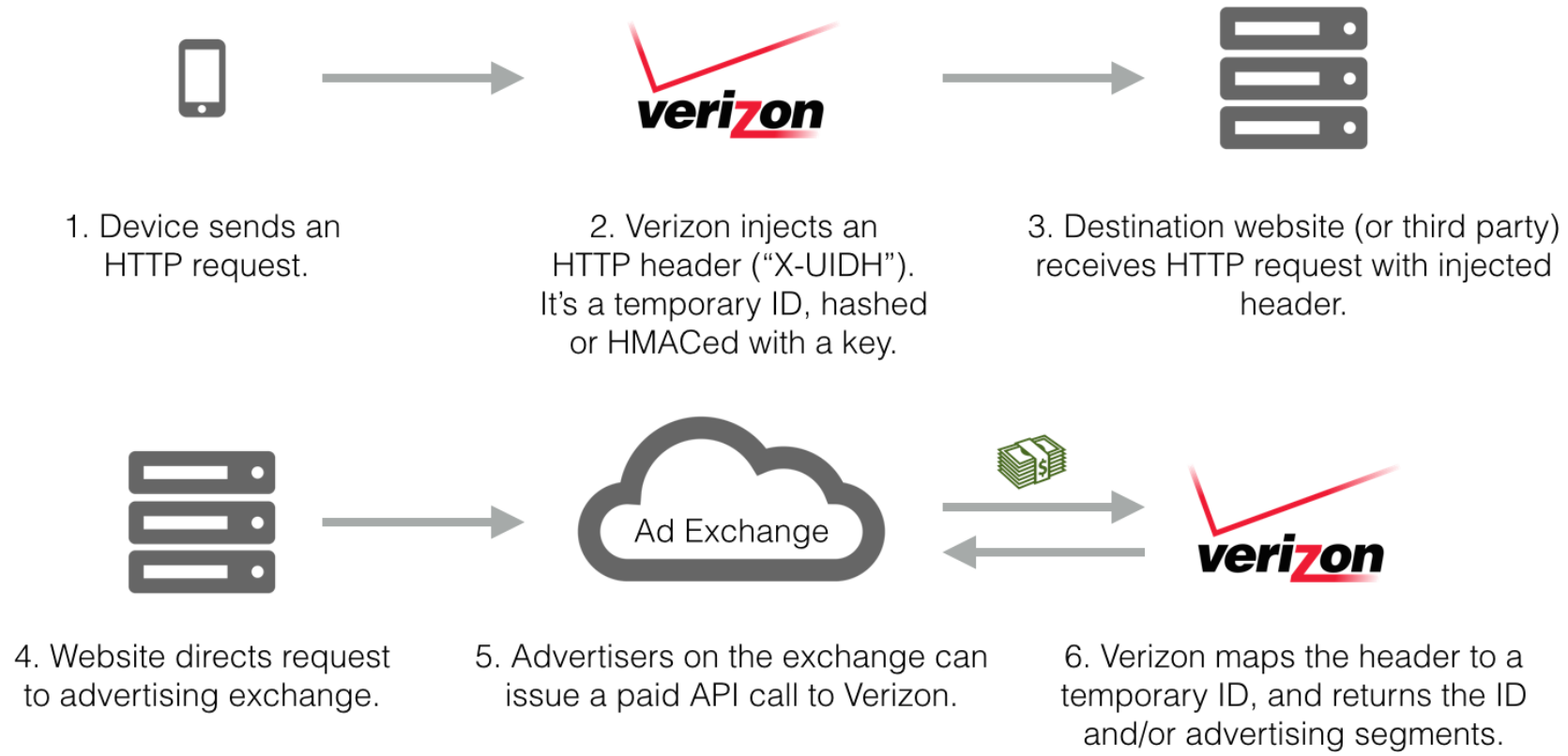
Channel security or lack thereof

- An object lesson in Kerckhoffs' Principle
- 2G: A5 ciphers, developed 1987, kept secret
  - Reverse engineered in 1999
  - A5/2 completely broken within a month
  - A5/1 partially broken 2006, completely 2010
- 3G: KASUMI cipher, developed 1999, semi-publicly
  - Weaknesses found 2001, 2006, 2010, 2013…
  - Some practical attacks, but not (yet!) as used in 3G
- Compare AES: developed 1999-2001, *publicly*
  - Still no practical attacks

Protocol downgrade

- 3G and up have OK channel security, *but*…
- Phones automatically fall back to 2G if no 3G service
- Jam the 3G signal from the real tower, crack the weak 2G encryption

Data tampering by legitimate carrier



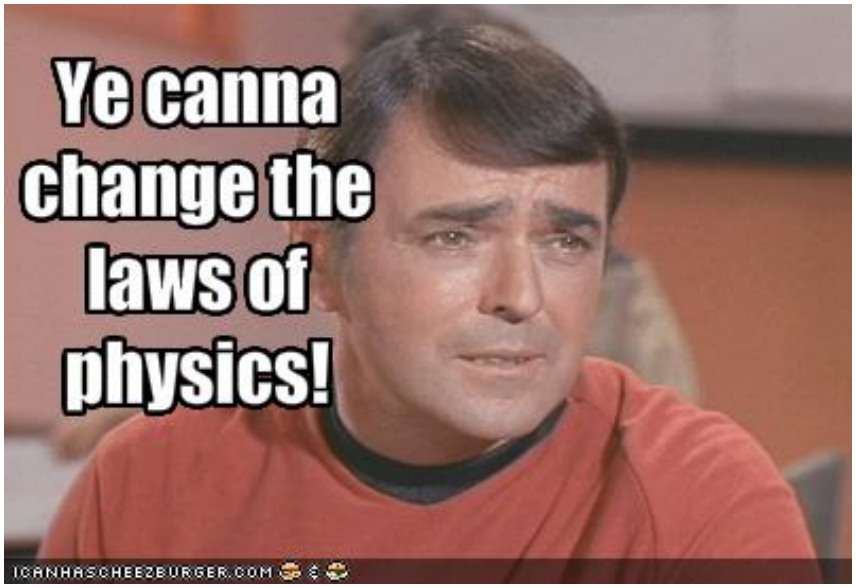
End-to-end crypto (e.g. HTTPS) makes this go away

http://webpolicy.org/2014/10/24/how-verizons-advertising-header-works/

Solution for tampering/eavesdropping

- End-to-end secure channel
- Data: HTTPS, VPNs
  - Built into iOS and Android
- Calls, text messages: need 3rd party app
  - WhisperSystems, Silent Circle, etc
  - Both ends have to have the software

Solution for location tracking



- Cell towers can't help but know where the phones are
- Carriers do not *need* to record location history, maybe they shouldn't
- Courts should treat location tracking as an invasive search (needs a warrant)


Questions?

Further reading

https://source.android.com/devices/tech/security/
https://www.eecs.berkeley.edu/~daw/papers/anduser-soups12.pdf
https://www.usenix.org/system/files/conference/hotsec12/hotsec12-final19.pdf
http://www.ieee-security.org/TC/SP2012/papers/4681a095.pdf
https://iseclab.org/papers/egele-ndss11.pdf
https://discovery.csc.ncsu.edu/pubs/CODASPY12.pdf
http://warrantless.org/2014/09/pd-hack/
https://media.blackhat.com/bh-us-11/Borgaonkar/BH_US_11_RaviNicoKredon_Femtocells-WP.pdf
https://www.isti.tu-berlin.de/fileadmin/fg214/ravi/Darshak-bh14.pdf
http://openbsc.osmocom.org/trac/raw-attachment/wiki/OsmoDevCon2012/Introduction-to-femtocells.pdf
https://srlabs.de/blog/wp-content/uploads/2010/07/Attacking.Phone_.Privacy_Karsten.Nohl_1.pdf
http://blog.cryptographyengineering.com/2013/05/a-few-thoughts-on-cellular-encryption.html
http://www.slideshare.net/grugq/mobile-opsec

Image sources

https://commons.wikimedia.org/wiki/File:Mobile_phone_evolution.jpg
https://commons.wikimedia.org/wiki/File:Mobile_phone_subscribers_1997-2014_ITU.svg
http://www.visiognomy.com/diagrams/archives/2005/02/16/cell-phone-towers/
http://thenounproject.com/term/cat/7776/
http://thenounproject.com/term/squirrel/26718/
http://thenounproject.com/term/map/23349/
http://thenounproject.com/term/robot/28643/
http://thenounproject.com/term/antenna/5467/
http://thenextweb.com/facebook/2013/04/13/facebooks-android-app-can-now-retrieve-data-about-what-apps-you-use/
http://www.gbeye.com/doctor-who/dr-who-daleks-exterminate-maxi-poster
http://warrantless.org/wp-content/uploads/2014/09/stingray_wsj.jpg
http://www.gerry.co.za/lessons/pics/402_lawsofphysics.jpg
http://webpolicy.org/2014/10/24/how-verizons-advertising-header-works/

END