Byrne Seminar

Internet of Things Things

kulikows@cs.rutgers.edu

mcgrew@cs.rutgers.edu

Week 1: Definitions, mapping out the course

Week 2: Composition of an IOT Thing. Programming it.

The IOT before the "I": Apollo AGC (1961-71)

Week 3: Introduction to our processor: The Arduino

Distribution of hardware **WHICH I WANT BACK**

Week 4: Security of IOT things. Fiddling with devices

Week 5: Getting used to the Arduino and building devices

Week 6: Show-offs; turn in your code

Uses of IOTs: medicine, "smart cities", political oppression **PIZZA**

Week 7: Research description: you pick an IOT, and research it for presentation to the class, political oppression, privacy issues, battery life, project showoffs

Week 8: Security of IOT things #2: security, and liability

Week 9: Presentations of research projects part 1 **PIZZA**

Week 10: Presentations of research projects part 2

Presentations (and excuses ☺)

Security. Again

OIT Help Desk Today at 8:16 PM

To: info_allcampuses@rams.rutgers.edu

WARNING: critical vulnerability discovered in Wi-Fi

OH

A serious vulnerability has been identified in the wireless encryption standards used for Wi-Fi networks. Attackers can use this so-called KRACK vulnerability to access information that was previously assumed to be safely encrypted, including credit card numbers, passwords, photos, and protected health information. Any device that supports Wi-Fi is potentially affected.

What to do to protect your information:

To prevent an attack, users should update devices as soon as patches or updates become available. Devices affected by the vulnerability include phones, tablets, computers, connected home devices, and wireless access points and routers. Check with device vendors or carriers for the availability of updates. A number of companies have made patches/updates available. Read the following for information on how major companies are addressing this issue:
https://www.pcmag.com/news/356809/krack-wi-fi-bug-what-apple-google-more-are-doing-to-fix-i

Key points to remember:

- All devices supporting Wi-Fi are potentially affected.
- Install updates/patches as soon as they're available.
- Do not use unpatched devices on Wi-Fi to transmit sensitive or private information.
- All data transmitted can be decrypted.

If you need help:

If you have any questions or concerns, please contact your departmental IT support or the Help Desk:

Camden | 856-225-6274 | http://computing.camden.rutgers.edu

Security. Again

KIM ZETTER SECURITY 07.31.10 07:57 PM

HACKER SPOOFS CELL PHONE TOWER TO INTERCEPT CALLS

Security.

LAS VEGAS – A security researcher created a cell phone base station that tricks cell phones into routing their outbound calls through his device, allowing someone to intercept even encrypted calls in the clear.

The device tricks the phones into disabling encryption and records call details and content before they're routed on their proper way through voice-over-IP.

The low-cost, home-brewed device, developed by researcher Chris Paget, mimics more expensive devices already used by intelligence and law enforcement agencies - called IMSI catchers - that can capture phone ID data and content. The devices essentially spoof a legitimate GSM tower and entice cell phones to send them data by emitting a signal that's stronger than legitimate towers in the area.

"If you have the ability to deliver a reasonably strong signal, then those around are owned," Paget said.

Paget's system costs only about $1,500, as opposed to several hundreds of thousands for professional products. Most of the price is for the laptop he used to operate the system.

Security.

LAS VEGAS – A security researcher created a cell phone base station that tricks cell phones into routing their outbound calls through his device, allowing someone to intercept even encrypted calls in the clear.

The device tricks the phones into disabling encryption and records call details and content before they're routed on their proper way through voice-over-IP.

The low-cost, home-brewed device, developed by researcher Chris Paget, mimics more expensive devices already used by intelligence and law enforcement agencies - called IMSI catchers - that can capture phone ID data and content. The devices essentially spoof a legitimate GSM tower and entice cell phones to send them data by emitting a signal that's stronger than legitimate towers in the area.

"If you have the ability to deliver a reasonably strong signal, then those around are owned," Paget said.

Paget's system costs only about $1,500, as opposed to several hundreds of thousands for professional products. Most of the price is for the laptop he used to operate the system.

Privacy

Invade privacy – from the vendor

- AT&T "Family Map"
- Sprint "Family Locator"
- Verison "Family Locator"
- android "remotely locate device"
- iphone "find my iphone"

Privacy

- apple/android "Connect" – collect posts from 'friends', including with GPS coordinates

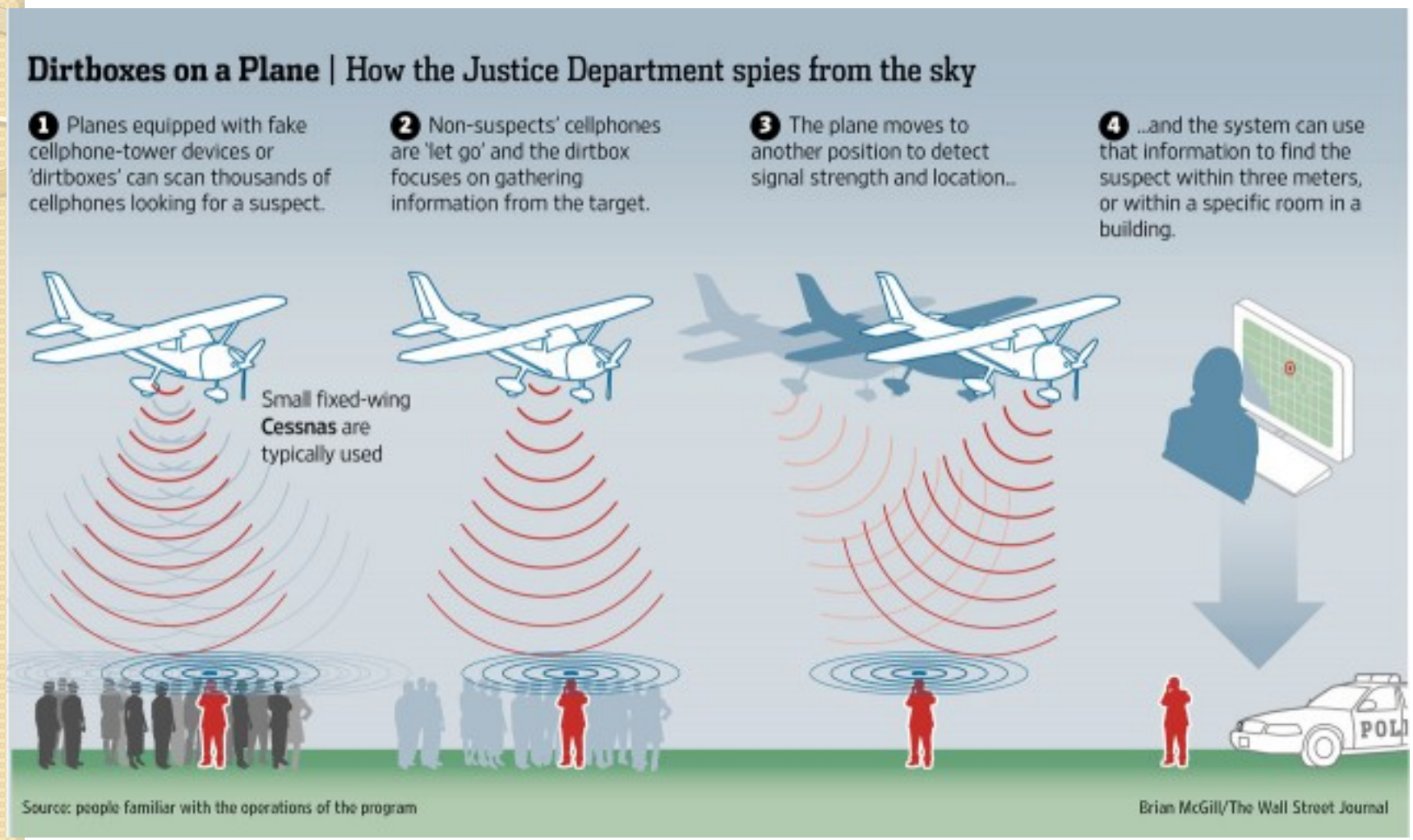
- "Find my Friends"

- Phone Tracker

- mSpy

- Spyzie

Privacy: Stingray


Dirtboxes on a Plane | How the Justice Department spies from the sky
1 Planes equipped with fake cellphone-tower devices or 'dirtboxes' can scan thousands of cellphones looking for a suspect.
2 Non-suspects' cellphones are 'let go' and the dirtbox focuses on gathering information from the target.
3 The plane moves to another position to detect signal strength and location..
4 ...and the system can use that information to find the suspect within three meters, or within a specific room in a building.
Small fixed-wing Cessnas are typically used
Source: people familiar with the operations of the program
Brian McGill/The Wall Street Journal

“So what? I’ve got nothing to hide…”

future tense ASU | NEW AMERICA | SLATE

Learn more about Future Tense »

future tense THE CITIZEN'S GUIDE TO THE FUTURE | SEPT. 27 2013 11:19 AM

How NSA Spies Abused Their Powers to Snoop on Girlfriends, Lovers, and First Dates

By Ryan Gallagher

Open “www.slate.com/articles/technology/future_tense/2012/03/future_tense_emerging_technologies_society_and_policy

#POLITICS SEPTEMBER 27, 2013 / 3:34 PM / 4 YEARS AGO

NSA staff used spy tools on spouses, ex-lovers: watchdog

Alina Selyukh

4 MIN READ

WASHINGTON (Reuters) - At least a dozen U.S. National Security Agency employees have been caught using secret government surveillance tools to spy on the emails or phone calls of their current or former spouses and lovers in the past decade, according to the intelligence agency's internal watchdog.

How about…

The more they know…

- medical records being used to decide employment
- employment decision based on diet (your refrigerator),
  or DNA ('heritage tests')
- jury profiling by medical records and movements
- deciding access to political mechanisms based on what you believe (e.g IRS)
- Deciding your employment based on who your 'friends' are.

Deciding access to government services based on medical issues (

IOT's: more data into "the mix"

We have to think about privacy when we bulid and deploy these devices, or unscrupulous people will misuse it.

J Med Ethics. 1995 Oct; 21(5): 281–287. PMCID: PMC1376776

Smokers' rights to health care.

R Persaud

Bethlem and Maudsley Hospitals Trust, London.

Abstract

The question whether rights to health care should be altered by smoking behaviour involves wideranging implications for all who indulge in hazardous behaviours, and involves complex economic utilitarian arguments. This paper examines current debate in the UK and suggest the major significance of the controversy has been ignored. That this discussion exists at all implies increasing division over the scope and purpose of a nationalised health service, bestowing health rights on all. When individuals bear the cost of their own health care, they appear to take responsibility for health implications of personal behaviour, but when the state bears the cost, moral obligations of the community and its doctors to care for those who do not value health are called into question. The debate has far-reaching implications as ethical problems of smokers' rights to health care are common to situations where health as a value comes into conflict with other values, such as pleasure or wealth.

Full text

Full text is available as a scanned copy of the original print version. Get a printable copy (PDF file) of the **complete article** (1.2M), or click on a page image below to browse page by page. Links to PubMed are also available for **Selected References**.


281


282


283


284

And now for something completely different: battery life

- Why use battery-powered devices?
- When should we use battery-powered devices?
- When should we NOT use battery-powered devices?

If we decide to use battery power, how can we maximize battery life?

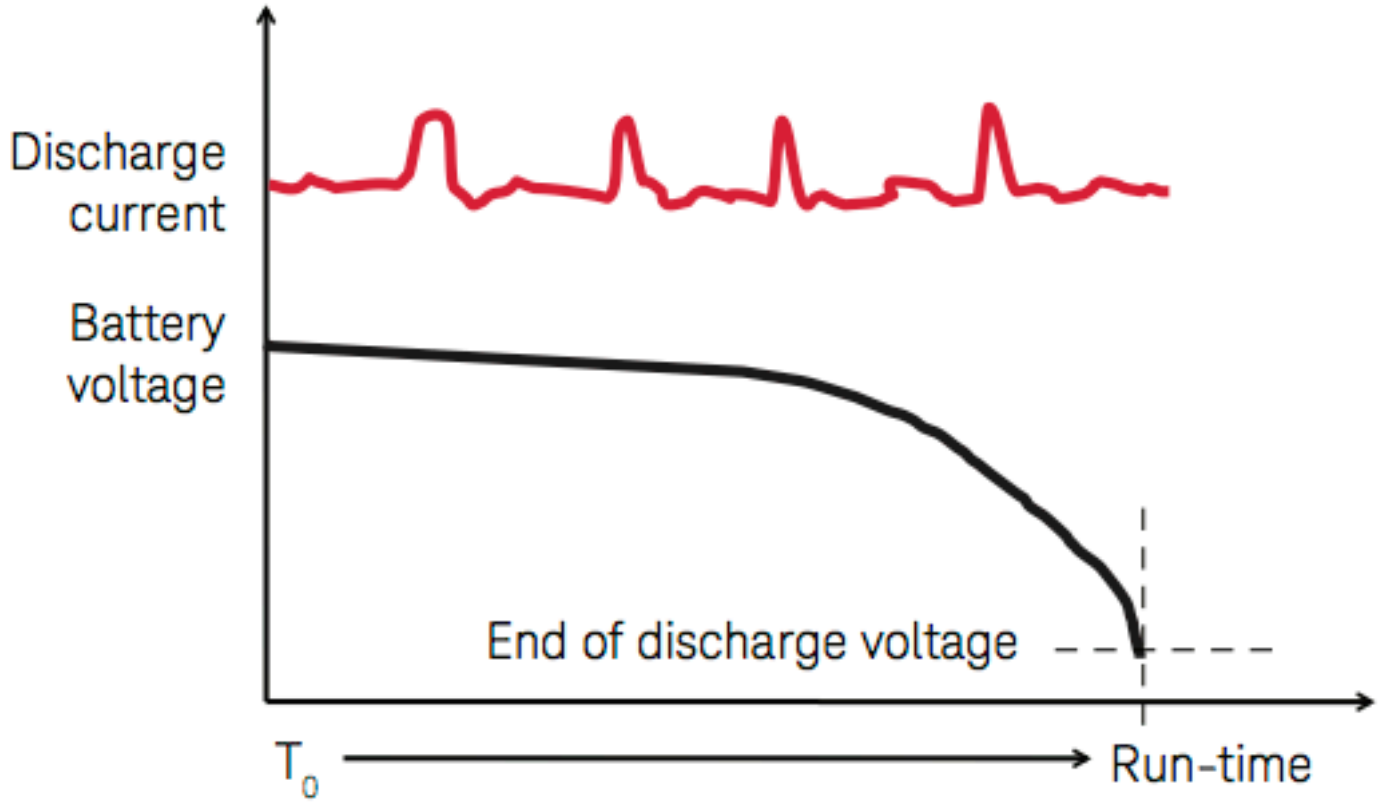


Figure 1. Battery run-down test results

Battery enhancements

- shut off subsystems we don't always need (like radio) - but now our devices cannot be interrogated (or sensors) - but now they're not continuous, and might lose calibration
- enhance support infrastructure to provide power (e.g. poe) for recharging
- Have close base stations so not as much power needed to get data out)
- make sure the device can monitor the voltage from the battery to warn of imminent failure
- minimize sensors to just what is needed
- miminize computing to just what is needed