Internet of Vulnerable Things:

Bluetooth Smart & Wi-Fi Privacy of Wearables & Devices

Michael Hirsch
https://scivision.co
mhirsch@bu.edu

(updated July 22 2015 with HP IoT Security Report info)
6 July 2015

Introduction (1)

- Proliferation of wireless devices
  - wearables
  - devices
  - sensors
- Each one increases attack surface
  - BYOD
- High value targets
  - VIP, corporate BYOD, stalking
  - wearables and devices → tracking beacons

Introduction (2)

7.5 million yearly stalking victims (USA); 15% of women / 6% of men stalking victims in lifetime (CDC 2011)

- Prepaid/burner: also vulnerable to tracking

At this time, people at risk whether stalking victims, VIPs, or BYOD on corporate networks should consider:
1) not using Bluetooth Smart / Low Energy devices < BT v4.2
2) Turn off Wifi on their device when not on their Wifi network
3) not using Bluetooth speakers that are auto-discoverable, auto-pairing

Motivation (1)

Why be concerned about proliferation of physically trackable devices?

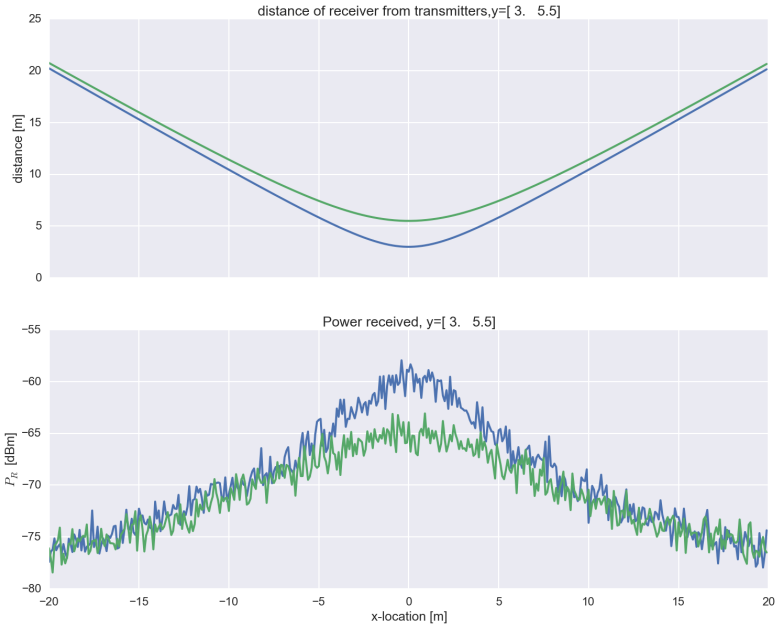
- Spear Phishing
  - “Hi I’m Eve from [your wireless carrier | security camera manufacturer] calling about a software update to your [husband Steve’s | daughter Karen’s] [device | wearable model number]. You’ll see a text message now from us with a link to the ~~update”~~ targeted payload

Motivation (2)

Why be concerned about proliferation of physically trackable devices?

- Harassment / Stalking
  - wait outside workplace
  - obtain Wifi/Bluetooth pings
  - confirms home network for pinpoint location and adverse actions

$20 long range (1km) antenna



Discriminate between multiple devices based on 1/r^2 signal strength differences

Motivation (3)

Why be concerned about proliferation of physically trackable devices?

- Remote Quantification of Attack Vectors
  - Let's see, the target has
    - ~~Smart~~ dumb TV
    - WEP home Wifi
    - Bluetooth Speakers/headphones left on
    - (in)security cameras

Background (1)

Bluetooth Smart:

- 3 advertising channels @ 2402, 2426, 2480 MHz (picked to be between Wifi channels for best interference-free range)
- 37 data chan.
- Hear pairing → trivially crack key→ Force unpairing → pwn connection→ take over / crash device wirelessly / passive eavesdrop

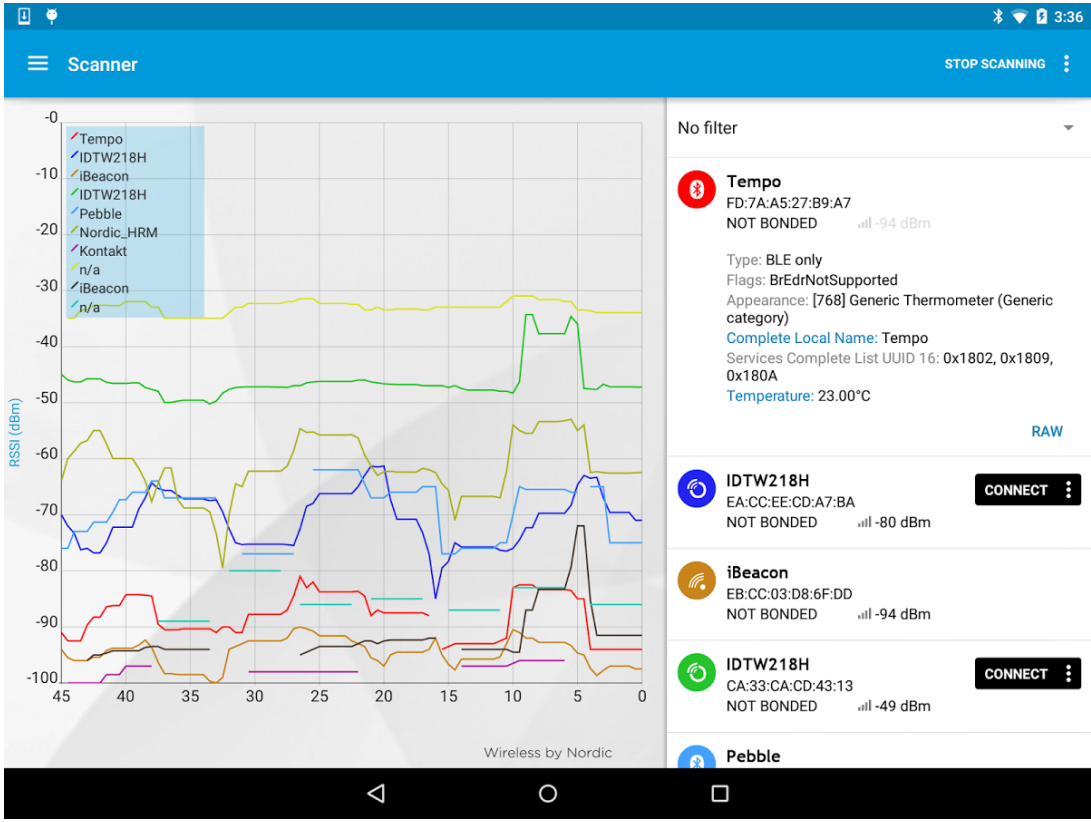
mitigated by ECDH: new in v4.2 Dec 2014

Background (2)

I pickup numerous:

- Auto-discover, Auto-pairing headphones & speakers
- motes
- Bob's iPhone

typically dozens of UUIDs at a time



Nordic Semi Master Control Panel Toolbox (Google Play)

Scenarios (1)

Maximum range ~ 1 km with $20 antenna (more typically 50m..20m for wearable w/o special antennas)

With devices like Ubertooth, possible to monitor already paired devices (as with Wifi) based on periodic updates (100ms to 10sec)

Scenarios (2)

Example #1: Android 5.1 -- wearable can keep screen unlocked when “in range”

If connection can be intercepted and wearable impersonated:

- Alice steps away from desk with wearable, leaves device on desk, Eve impersonates wearable to grab unlocked device
  - Alternative scenario: wearable credentials intercepted due to unencrypted transport
- Will remote-settable corporate device policies allow overriding these wearable-paired issues?

Scenarios (3)

Example #2: any device (iOS, Android, Blackberry, Windows Phone, etc.)

- Eve sits on bench outside Alice's workplace, passively sniffs Alice's MAC/UUID and list of Wi-Fi AP Alice has used in past
- Eve sets up fake WiFi AP SSID, turning Alice's wearable/device into multiple pulse per second tracking beacon!

Mitigation: device rotates MAC/UUID when not connected; preferably periodic MAC/UUID rotation when connected (update AP firmware)

Scenarios (4)

Example #3 (adapted from M. Ryan and HP 2015 IoT Smartwatch report): Bluetooth Smart v4.0 or v4.1 devices & wearables:

Eve passively sniffs Bob's MAC/UUID, learns BTLE simple channel hopping pattern

- Eve jams Bob's BTLE wearable, breaking connection, leading Bob to re-pair,
- Eve sniffs and cracks in 1 second for passive or active wireless access to email, text, phone, calendar, fine location, apps, etc. from up to 1km away

Scenarios (5)

Example #4: all Bluetooth speakers or headsets that are auto-discoverable with HSP (headset) service (most have this)

- Eve walks down street listening for auto-discoverable HSP devices (these are common!)
- Eve notes that many well-to-do neighborhoods have lots of these HSP devices left on 24/7, and that Eve can pair remotely without local confirmation, and listen to everything in the home the microphone can pick up.

Scenarios (6)

Example #5: homes with smart TV, wifi security cam / baby monitor, especially using WEP, WPA1, or WPS.

- Cheap security cameras often have unencrypted or weakly encrypted password exchange.
- Eve cracks Wifi password (or gains access via connection cracked using previously mentioned technique)
- Eve watches/listens to activity in home to target for theft or other adverse action
- HP 2014 IoT report found that 70% of IoT devices tested made UNencrypted connections!

Victim tried to secure their home with surveillance, but made themselves much less secure!

Qualitative Problems

- RF energy knows no borders (only 1/r^2 and obstruction losses)
- Weak processors, weak encryption
  - save energy
  - lazy design
- Few OEMs motivated to make slight tweaks to defaults

Cold War era shortwave radio jamming array
Photo credit: Ingmar Runge, Wikimedia (CC BY 3.0)

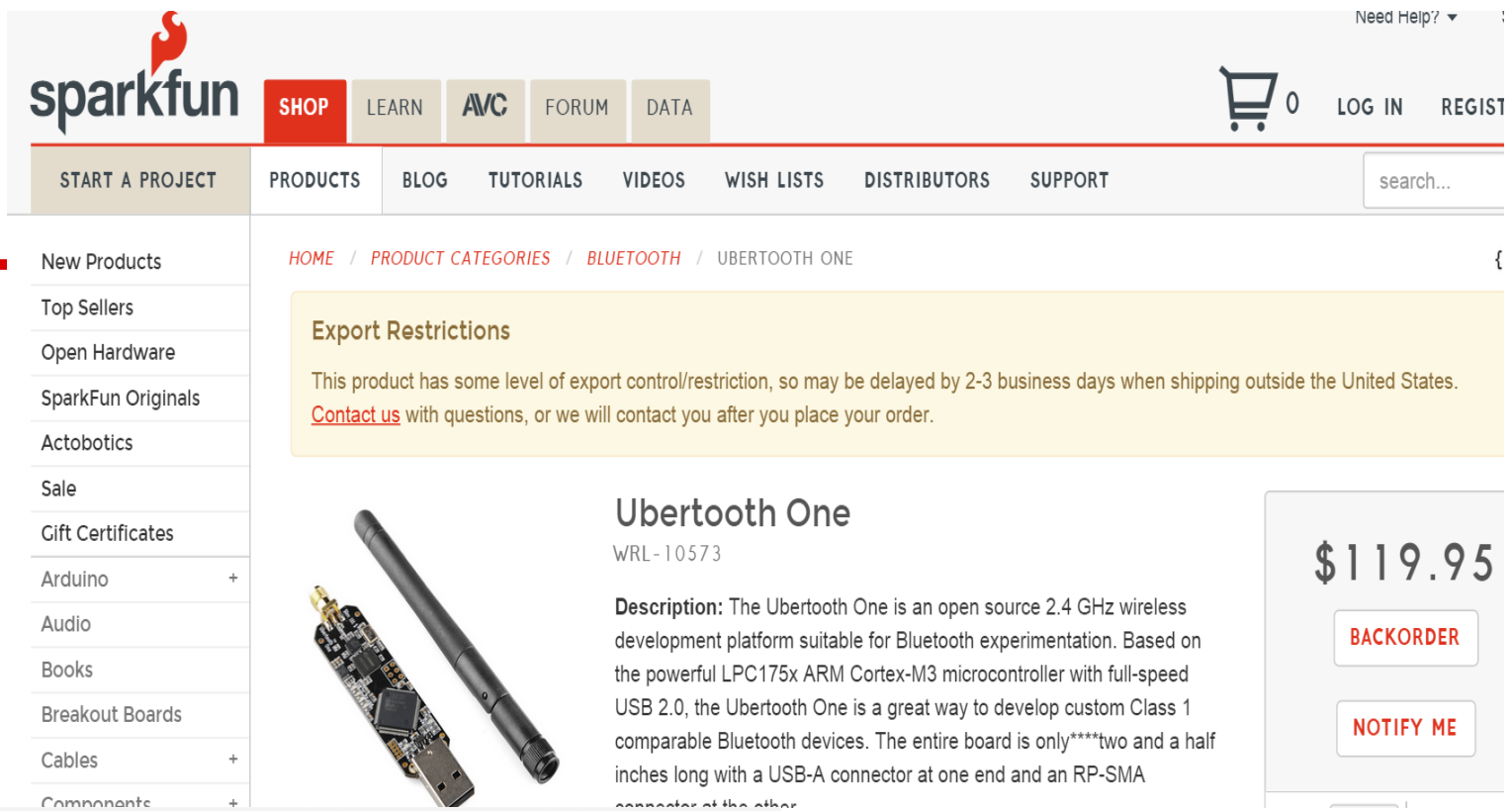
Security doesn't sell!

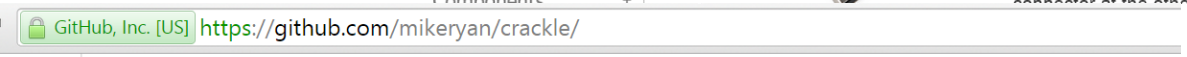
Quantitative Problems

- Devices beacon (multiple times per minute) the Wi-Fi SSIDs they've connected to, including hidden SSID
  - Reveals MAC of device / Wi-Fi enabled wearable
  - mitigated by some recent OS that use random MAC until connected (is your device updated?)
- Bluetooth "smart" channel hopping pattern is trivially predictable--UUID in the clear
  - Follow me!
- Until v4.2 (Dec 2014), Bluetooth effectively paired in the clear

Tools

Before BT v4.2...





crackle cracks BLE Encryption (AKA Bluetooth Smart).

crackle exploits a flaw in the BLE pairing process that allows an attacker to guess or very quickly brute force the TK (Temporary Key). With the TK and other data collected from the pairing process, the STK (Short Term Key) and later the LTK (Long Term Key) can be collected.

With the STK and LTK, all communications between the master and the slave can be decrypted.

crackle was written by Mike Ryan mikeryan@lacklustre.net See web site for more info: http://lacklustre.net/projects/crackle/

Pairing: hear key exchange, code: {000000..999999}, which yields short term & long term keys

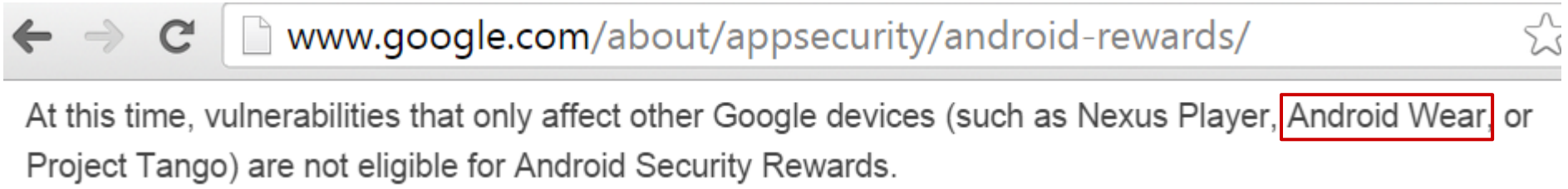
Demos

via Blackhat, Toorcon, Shmoocon, etc.

I am Jack's Heart Monitor

Remote Bluetooth stack crash on Android

"If you're not a cryptographer, don't build a crypto system!" (M. Ryan)



Canonical Issues

- Pwn the weakest device target uses, and escalate from there

- Many more subtle and practical attacks exist, that haven't been discovered/disclosed because existing security is so bad

- Security by proximity is also not secure
- Perfect storm for FreSSH type devices
  - fake air freshener / power strip with evil sniffer inside

Mitigation

- Consider certificate-based authentication
- Distrust PHY
- Remove all unused Wi-Fi from device saved list
  - watch for built-ins like “attwifi” and “tmobile” that device auto-reenables!
- Don’t allow BT v4.0-4.1 wearables on corporate email, devices, and networks
  - How to enforce?
- Ultimately will just have to wait for / live with BT v4.2

Conclusion (1)

- Airgapping, while of limited use, may be one of the only mitigations currently
  - Pair wearable with cheap phone on throwaway account
  - don’t pair with BYOD or corporate device
  - better with BT v4.2+ we hope

- Wearable weaknesses are repeat of same old security problems, made worse by interconnectivity / BYOD / pervasive tech.

Conclusion (2)

At this time, people at risk whether stalking victims, VIPs, or BYOD on corporate networks should consider:
1) not using Bluetooth Smart / Low Energy devices < BT v4.2
2) Turn off Wifi on their device when not on their Wifi network
3) not using Bluetooth speakers / headsets that are auto-discoverable, auto-pairing

References

M. Breiding, et al. "Prevalence and Characteristics of Sexual Violence, Stalking, and Intimate Partner Violence Victimization", National Intimate Partner and Sexual Violence Survey, CDC United States, 2011 http://www.cdc.gov/mmwr/preview/mmwrhtml/ss6308a1.htm

A. Musa, J. Eriksson, "Tracking unmodified smartphones using Wi-Fi monitors", SenSys Nov 2012, Toronto, CA https://www.cme.uic.edu/pub/Bits/Musa/musa-eriksson-sensys12.pdf

D. Namiot, M. Sneps-Sneppe, "Local messages for smartphones", CFIC Coimbra 2013 http://arxiv.org/pdf/1305.4163.pdf

M. Cunche, "Wi-Fi told me everything about you", Confiance Numerique, Mar. 2014 http://confiance-numerique.clermont-universite.fr/Slides/M-Cunche-2014.pdf

Bluetooth v4.2 spec. https://www.bluetooth.org/en-us/specification/adopted-specifications

M. Ryan, "Bluetooth smart: the good the bad the ugly" Blackhat 2013 https://media.blackhat.com/us-13/us-13-Ryan-Bluetooth-Smart-The-Good-The-Bad-The-Ugly-and-The-Fix.pdf

National Security Agency, "Bluetooth Security", https://www.nsa.gov/ia/_files/factsheets/i732-016r-07.pdf

HP Fortify, "Intenet of Things Security Study: Smartwatches", http://go.saas.hp.com/fod/internet-of-things, 22 JUL 2015.

Backup

History

- Bluetooth Smart -- Bluetooth Low Energy (BTLE):
  - a subset of Bluetooth 4.0 ca. 2010
  - Android July 2013
  - iOS 8 September 2014 (CoreMotion)
  - introduced predictive Text
- Modern smartphones can transmit and receive small amounts of data via BTLE

- Estimates of received signal strength (RSSI)