Opt Out or Deauth Trying!

Anti-Tracking Bots Radios and Keystroke Injection

Weston Hecker
Principal Application Security Engineer NCR
Twitter @Westonhecker
A Little About Me.

- About myself: 32 - Work for NCR - Live in North Dakota
- 12 years Pentesting has 13 years of Experience Doing Security Research and Programming.
- Hacking ATMs, POS, Hotel, Cars and Several IOT projects.
- Reverse Engineering Malware – Building Hardware
- Car Hacking Village/Demolabs talk (2FA for 11 dollars) TPMS (Early Warrant detection POC)
Present background: About This Research.

- What lead to this research?
- Chemtrails.
- EOL Windows 7
Present background: About This Research.

- Explain systems that have been used in the past
- Where the instore tracking is going.
- Operating systems spying (Switching to Windows 10)
- Search engines spying (Google, Yahoo) Bing Probably Does to But No One Uses It?
- Billboards spying
- Creepy ADs
- Privacy disappearing
Explanation of Targeted/Personalized Advertising/Uses of targeted advertising.

- What is targeted advertising.
- Personalized advertising
- Behavioral Advertising and cookies.
- Hobbies music automobiles electronics travel ETC
- Collection of non identifiable information. Most of the time no email name or address added information to audience interest cookies
- Jacks up RTB Real time bid information making it useless or undesirable range.
- Programmatic software for advertisement displays.
- Private Market Place. PMP money waisted
Explanation of online tracking.

- Explanation of technology tracking online.
- Expansion of operating systems spying
- How impacts users
- How impacts businesses
- Pages tracked for ad
- Pages other forms of tracking
- GPS Tracking IP address
- Wifi Beacons and cellular towers.
Topics Used for Personalized Ads.

- Arts and Entertainment, Autos and Vehicles, Beauty and Fitness, Books and literature, Business and industrial, Computers and electronics, Finance, Food and drink, Games, Hobbies and Leisure, Home and Garden, Internet and telcom, Jobs education law and government, news online communities, people and society, pets and animals, Real estate, Reference, Science, Shopping, Sports, Travel, World Localities.

What opting out doesn't do

There are some things that opting out doesn't do. Here are some of the most common scenarios and what you can do to address them.
Good Start to Stop Tracking.

• Current ways to stop this !!!!
• Ad Blocking Apps
• AD Blackhole. (Less detectable)
• Track me not.  https://adnauseam.io/
• Trackthis ← Hypervisor!!!
• EFF !!! Privacy Badger
• Paid VPNS *Static VPS*
• All A Good Start.
WHAT DO YOU HAVE AGAINST ADS WESTON.

• I understand the internet costs money to run.
• I gladly pay for email.
• Gladly pay for YouTube RED
• Gladly pay for anything that’s AD Free.
• Even android Stuff You can click don’t track Me and erase locations.
Disable tracking in browsers. Still does nothing
Drive by attacks malicious advertisements.

Attn: NYTimes.com readers: Do not click pop-up box warning about a virus -- it's an unauthorized ad we are working to eliminate.
Explanation of Brick and mortar tracking.

• Since the late 90s stores have used one form or another of tracking.
• Customers are tracked to provide analytics of where they go in the store so that stores can adjust the store layout to sell the most.
• There has been stories that come to light every few years that make references to big brother. But they are soon forgotten.
• The stores remove the system or only had them in a piolet store so they cease expansion into other stores.
• If people stop complaining they will make this a staple mark of there stores.
• There have been improvements to include most cases where customers have to OPT into the store rewards programs.
Frequency ranges and Devices that use them.

- Bluetooth, Cellular beacons, Wifi, Infrared and motion.
- Several years they have gotten negative press by adding instore tracking
- US there has been lots of resistance with most forms of tracking.
- Apple and several other manufactures modify there Bluetooth beacons to protect users.
- UK and other areas of the world there has been less resistance.
- We are told it is all turned into meta data (Data about data)
How Meta Data Affects Advertising and Monitoring.

- Meta Data is Used to Change Store Layout.
- More Specific Layout/Increase Sales
- Use of Rewards Programs OPT-in for Discounts
- Ads are Generated Off of Online Analytics.
- They Can Increase How Much are They Charging for Store Area.
- Changes in Ad Placement Physical and Web
Collection of ALL cellular/Bluetooth beacons.

• Cellular ESN emid Bluetooth beacons
• What is its purpose what is it abused for
• How to harden you communication best practices.
Collection of car sensors and WIFI Beacon data by billboards.

- Smart Billboard.
- How are they tracking
- Passive?
- In the U.S. the Tread Act mandated that every car built after 2007 must have a tire pressure monitoring system built-in
- (TPMSS) use unencrypted RF
- 314 mhz Unique ID (Every 60 seconds) 19MPH+
Data collected by applications/ Social media.

• Social media explained
• Social advertising
• Data collection
• Abuse in past.
• B) How does it come back to you.
• Reversing the randomness
Operating systems collecting information now to?

- Back in the good old days. XP
- 1984 ? Windows 10 info collection
- Miss information
- P2p updates
- Data collection
- Why are these changes happening
II. Explanation of Attacks

- Blocking Billboard Spying.
- Explain the main attack surface of the passive monitoring systems.
- How To Stop Brick and Mortar Spying
- How to Stop Web & OS Spying.
1. Methods to Stop Billboard Spying.

- Smart Billboard Capture Vehicle sensor Information.
- Capture sensor information. Based on make and model they can expect age, Race, Sex, Income range
- Passive ? And Opt in Applications (BT and WiFi)
- ROLLING TPMSS 10 Codes for around 17 Dollars.
- SHHHHHH mode for your sensors.
- Can Add 3-4 Sets of tires to car also. NO NEED FOR DEALER
- Installing (GHD) Ground Hogs Day 315/433 System on Billboard 3400 Sensors
So What Collected Data Allowed Them To Profile Me Online?

• What categories do they track, Technical level, Age, Sex, Orientation, Religion, Purchase history, Food Preferences, Hobbies, Employment, Political Views ETC How it is compiled
• How do they use it
• Who is of interest.
• How do government portals work how is it shared
• How is data held against people
• When this information is requested by law enforcement or an advertisement agency what is delivered how is it used
• Portals for Law Enforcement/Web Interfaces and Analytics.
UI/UX overview of program Pick what they see as your age and areas of interest.

• Injecting false data
• Profile changing
• Limiting accurate data
• Type FIST program (Never type directly into anything)
• Anti-Type Fist Engine Outputs key strokes at 28-GWPM
• Keystroke Injection From a VM (Emulate Simulate Mouse/KB)
• Browser Bot.
• Not Detected By Search Provider/Web Browser Program
don’t they have methods of tracking this type of activity how to evade tracking flagged or being flagged as a bot.

- I am not a robot. (not completely a robot)
- Evading SE protections
- Make it rain
- Make it snow
- B: The joys of getting advertisements watching first hand your misinformation working.
- How the research progressed from accurate ads to almost random
- Pin and prodding search engines.
- Mapping out collection structure
- Feeding of data input output.
Could this be used as a malware payload? Make your Neighbor Look Like a terrorist or a Justin Bieber fan. (FRAME-WARE)

- How could some one load malware
- How could malware frame some one
- How could it damage some ones life
- Even Worse Like NickleBack Facebook!!!
- Used it to Seed VM for Malware Testing.
Operating systems spy systems why you can’t turn them off – Can’t beat them miss inform them.

- Showing how I tried to make windows 10 (off the HOST Grid) How Others and I Failed
- If I cant have my data no one can !
- Injection from a hypervisor
- How much can you mod OS before Microsoft blocks you
- Is the making me less secure
- 2) Collection levels/ By IP address by system browser details system login.
- External collection methods
- Old school
- IPV6 and how it changes spying on us
- Details they track
- Screen size, browser information
- Type fistig
CSS/HTML injection Proxy based / XML OS macro Based Injection.

- Ghost Writer./ Injection bot for the os
- How does it interact with other programs
- What are the limits ?
- Can windows stop this ?
- Ease of use.
What is your phone telling stores? a look at “NARC” Program for telling what your phone is giving off?

- Blocking output of your phone
- Spoofing
- Non root
- Generating Fake SMS/Email Messages Every Morning for Apps That Read the EULA 50/day rule
- Nice for Defcon/Blackhat Airplane Mode/Defcon Mode
How to inject 100s of fake Wifi BSSID/SSID

- (Hardware) Look at in-store tracking software/Heat mapping user collected data
- Device building
- How it works
- how it effects handsets
- Collection of Beacons
Look at instore tracking how they heat map

- Look at instore tracking how they heat map
- Heatmap VS People counting
III. Review of Devices used in Demo

Injecting Bluetooth beacons/ Vehicle sensor information/ Cellular ID information/ Bluetooth coupon Injection exploitation/ Look at strange responses of customer tracking systems

• Over device reactions
• Search Engine Profile Software
• Brick and Mortar Attack Tool.
How much does it throw off store data?

- The CV program dropped over 90% of customers entering
- Numbers Useless after 2HR
IV. Conclusions Demo

• A. Demonstration of Hardware Beacons laying waste to a SDR waterfall.
• B. Demonstration of “Profile This” software Obfuscating user profile from 32 year old hacker to 12 year old girl who likes horses.
• C. Conclusion of Demonstrations.
• D. Open to questions
  • Demonstrate Type Fisting Hypervisor
  • I am not a Robot
  • Profile Injection
  • Keystroke Operation
Kicking Off Demo

- Demo
- Groundhogs Day Attack (Replay)
- Jacking Up Dwell Time (Passing Customers)
- Threshold CV Based Jamming Using IR
Thanks to

• My Work
• My Wife Kids *Where's Dad*
• Jesus
• My Uncle Stacy.
• Defcon For Having Me Speak. 4th year in a row its an honor.
• Audience for Listening to my talk and giving me feedback.

Twitter: @Westonhecker