I FIGHT FOR THE USERS

EPISODE 1

Attacks Against Top Consumer Products
Who are we?

@zfasel

@SecBarbie
Our Credentials?

(null)
Before we get started...
Con Speaker Rule 101

If you’re naming vendors and don’t want your talk pulled, even if it’s already known and even if the impact is low, don’t disclose too much ahead of time.
TL;dr

- Bluetooth -> All the things!
- Wireless Security Products -> CCTV LOLZ
- Consumer Windows Install -> Whoops

- Q&A after talk
3 Topics in One Talk?

- Keep it close to 20 minutes
- So $15+15+15 = 45!$ MATH!
- Also squirel.
Bluetooth all the things!
Another Bluetooth Talk?

- BlueHydra* - Zero_Chaos & Granolocks
- BLE Locks From Miles Away - Rose & Ramsey
- BLE GATT Proxy Tool - Jasek
- BLE-REPLAY & BLESUITE - Foringer & Trabun
So what’s different here?
“Rules”

• Never reveal the secret

• Never repeat a trick for the same audience

• Practice. Over and Over.
“Rules”

• Never reveal the secret

• Never repeat a trick for the same audience

• Practice. Over and Over.
How do you wirelessly ID someone?

- Car on the way in?
  - ALPR
  - ETC RFID
  - Bluetooth

- Came in by foot?
  - Facial Recognition
  - Voice Recognition
  - Cell Phone?
    - WiFi
    - Bluetooth
    - IMSI Catcher

- Proximity
  - Credit Card RFID
  - Car Keys RFID
  - Work badges

- The not fancy ways
  - Reservation Names
  - RFID Loyalty cards
  - Credit cards
  - Social engineering
How do you wirelessly ID someone?

- **Car on the way in?**
  - ALPR
  - ETC RFID
  - Bluetooth

- **Came in by foot?**
  - Facial Recognition
  - Voice Recognition

- **Cell Phone?**
  - WiFi
  - Bluetooth
  - IMSI Catcher

- **Proximity**
  - Credit Card RFID
  - Car Keys RFID
  - Work badges

- **The not fancy ways**
  - Reservation Names
  - RFID Loyalty card
  - Credit cards
  - Social engineering
We are always looking for ways to improve our customers' shopping experience. Nordstrom is using Euclid to gather publicly-broadcasted information your Smartphone or other Wi-Fi enabled devices sends out when it's attempting to connect to a Wi-Fi network in and around this store. Euclid provides Nordstrom with anonymous, aggregate reports that give us a better sense of customer foot traffic. We do not gather such things as your name, email address, phone number, your device's browsing activity or text, email or voice messages.

To not participate, turn off your device's Wi-Fi function or power off your device.

To opt-out or learn more about Euclid, visit http://euclidanalytics.com/privacy. You can also visit http://shop.nordstrom.com/l/nordstrom-privacy.

---

**BUSINESS**

**Euclid Analytics And Retailers: How Stores Like Nordstrom Track You Via Your Smartphone’s Wi-Fi Signal**

© 05/08/2013 03:10 pm ET | Updated May 13, 2013

---

**MAY 9, 2013 @ 08:23 AM** 81,943 VIEWS

**How Nordstrom Uses WiFi To Spy On Shoppers**

**Peter Cohan, CONTRIBUTOR**

I write about tech stocks and the startup economy. [FULL BIO ▼](#)

Opinions expressed by Forbes Contributors are their own.
Wifi caught on to this

- iOS8 and Android 6.0
- Historical SSIDs identify real mac
- Take it as a data point, but not trust it
That leaves us with

- Came in by foot?
  - Cell Phone?
  - Bluetooth

- Proximity
  - Car Keys RFID
  - The not fancy ways
  - RFID Loyalty card
That leaves us with

- Came in by foot?
- Cell Phone?
- Bluetooth
- Proximity
- Car Keys RFID
- The not fancy ways
- RFID Loyalty card
I’m Blue (dabadeedabad1e)

**Bluetooth Classic**
- 79+1 1Mhz Channels, 1600 hops/second
- NAP + UAP and LAP make up hop sequence
- LAP is included in every message
- We know this. Duh. But many personal devices are now Bluetooth Smart (except for headsets/headphones).

**BLE (Bluetooth Smart)**
- 37+3 2Mhz Channels, Interval/Increment/Channels is dictated by master upon connection.
- 4 byte access address
- 6 byte mac address in advertising announcements
Bluetooth Technology – Protecting Your Privacy

People are increasingly aware of, and concerned about, security—in particular, their privacy in both the physical and the digital world. The term “privacy” alludes to various types of issues, depending upon the context. One privacy issue concerns the possibility of being tracked “where you go” in the physical world without your awareness or consent. “Where you go” could mean the places you drive or the route you walk.
Access Address?

- Address used once connected.
- Change upon disconnect/reconnect
- Long term tracking is not reliable
- Provides as good of short term tracking as random broadcast mac addresses, but applies to connected devices.
GAP and GATT

- Generic Access Profile
- Generic Attribute Profile
- Long story short, methods for sharing info about the connection or devices.
In Preparation For Takeoff

- Why are all these new devices advertising?
- Wait a second...
- if (paired == FALSE)
  ble.mode("advertise")
Can we disconnect BLE?

- Hell yes we can (momentarily and proximity dependent)
- USRP b210 = 56mhz bandwidth
- BLE = 80mhz, minus 6mhz broadcast
- 50-75% coverage
- So jam 2428 to 2478 Mhz...
- GNURadio + Rand Noise = some success
- Depending on the host, odd reliability
Option 2 – Spoof Disconnect

- Blast LL_TERMINATE_IND Control Packet
- Have to sniff the Access Address first and catch it on the right channel / right time
- Some devices don’t take kindly to this and won’t reconnect well
We’ve talked about tracking before, right?

- Sort Of?
- Focused on “it’s possible”, but not researching specific device behaviors.
Leaves us With Implementation Issues
Hello Amazon/Best Buy
Pavlok

- Static Mac
- Mac in Name (Pavlok-XXXX)
- Serial is its mac, also available via GATT in case you didn’t have it already in ascii->hex
Trackr

- Effectively Static Mac Address
- Manufacturer Data In broadcast = MAC
- Broadcasts Constantly
Tile

- Effectively Static Mac Address
- “Tile Identifier” in GATT
- Stays connected...only while app is open.
Fitbit One

- Randomized Mac, but effectively static after >4 months
- Doesn’t remain connected, so it broadcasts
Withings Active

- Mac Randomizes
- But... Advertises MAC as Manufacturer Data in Advertisement Data (ADV_IND)
Pebble Steel

• 2 Bytes of MAC in Manufacturer Name - “Pebble Time LE XXXX”
• Says Mac is random, but after days was still the same even after reboots
• Serial Number in Device Info
• Goes to sleep every so often
• Uses both Classic and BLE
Fitbit Alta

• Randomized Mac, but effectively static after >4 months and battery loss
• Unlike the one, stays connected for notifications
Garmin vivofit

- Static Mac, but...
- Bluetooth only works when in a “sync” mode.
Microsoft Band 2

- Dynamic Mac on reboot
- “<Name>’s Band <XX:XX> LE” as device name
Apple Watch

- Dynamic Mac
- Maintains dynamic mac between disconnects
- Rotates appear time based, but not 100% sure how often
Huawei Watch

- Android Wear
- Random Mac, and doesn’t respond to BLE broadcasts
iOS Devices

• BLE for Safari?!?  
• Other Apps Too  
• Does randomize heavily, and while it announces it as an i<Device>, no trackability
So who’s doing it right?

- Apple Watch
- Android Wear
- iOS Itself
This is where we were going to release a tool to track LAP / BLE Access Addresses / BLE Broadcast MACs.

BlueHydra totally one upped us, and we had no idea...

Go try it out and contribute (we will be)
Where do we go from here?

• We need to continue to test devices to document the implementation issues when it comes to bluetooth device privacy.
• github.com/urbanesec/bledevices
• When MACs are random, look for:
  • Lack of randomization, even if it says it is.
  • GAPs leaking serials
  • GATTs leaking serials
  • Device Names

• You can deauth BLE devices to get some to respond to advertisement channel requests to get advertisement addresses (MACs).

• While the standard supports it, devices don’t.
Consumer Wireless Cameras
Home (and office) “Security”
<table>
<thead>
<tr>
<th>Vendor</th>
<th>Default Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTi</td>
<td>admin/123456 or Admin/123456</td>
</tr>
<tr>
<td>American Dynamics</td>
<td>admin/admin or admin/9999</td>
</tr>
<tr>
<td>Arecont Vision</td>
<td>none</td>
</tr>
<tr>
<td>Avigilon</td>
<td>Previously admin/admin, changed to Administrator/&lt;blank&gt; in later firmware versions</td>
</tr>
<tr>
<td>Axis</td>
<td>Traditionally root/pass, new Axis</td>
</tr>
<tr>
<td>Basler</td>
<td>admin/admin</td>
</tr>
<tr>
<td>Bosch</td>
<td>None required, but new firmwares (6.0+) prompt users to create passwords on first login</td>
</tr>
<tr>
<td>Brickcom</td>
<td>admin/admin</td>
</tr>
<tr>
<td>Canon</td>
<td>root/camera</td>
</tr>
<tr>
<td>Cisco</td>
<td>No default password, IPX-DDK: root/admin or root/Admin</td>
</tr>
<tr>
<td>Dahua</td>
<td>admin/admin</td>
</tr>
<tr>
<td>Digital Watchdog</td>
<td>admin/admin</td>
</tr>
<tr>
<td>DRS</td>
<td>admin/1234</td>
</tr>
<tr>
<td>DVTel</td>
<td>Admin/1234</td>
</tr>
<tr>
<td>DynaColor</td>
<td>Admin/1234</td>
</tr>
<tr>
<td>FLIR</td>
<td>admin/fliradmin</td>
</tr>
<tr>
<td>FLIR (Dahua OEM)</td>
<td>admin/admin</td>
</tr>
<tr>
<td>Foscam</td>
<td>admin/&lt;blank&gt;</td>
</tr>
<tr>
<td>GeoVision</td>
<td>admin/admin</td>
</tr>
<tr>
<td>Grandstream</td>
<td>admin/admin</td>
</tr>
<tr>
<td>Hikvision</td>
<td>Previously admin/12345, but firmware 5.3.0 and up requires unique password creation</td>
</tr>
<tr>
<td>Honeywell</td>
<td>admin/1234</td>
</tr>
<tr>
<td>Intellio</td>
<td>admin/admin</td>
</tr>
<tr>
<td>IQinVision</td>
<td>root/system</td>
</tr>
<tr>
<td>JVC</td>
<td>admin/jvc</td>
</tr>
<tr>
<td>March Networks</td>
<td>admin/&lt;blank&gt;</td>
</tr>
<tr>
<td>Mobotix</td>
<td>admin/meinsm</td>
</tr>
<tr>
<td>Northern</td>
<td>Previously admin/12345, but firmware 5.3.0 and up requires unique password creation</td>
</tr>
<tr>
<td>Panasonic</td>
<td>Previously admin/12345, but firmware 2.40 requires username/password</td>
</tr>
<tr>
<td>Pelco Sarix</td>
<td>admin/admin</td>
</tr>
<tr>
<td>Pixword</td>
<td>admin/admin</td>
</tr>
<tr>
<td>Samsung Electronics</td>
<td>root/root or admin/4321</td>
</tr>
<tr>
<td>Samsung Techwan</td>
<td>admin/111111</td>
</tr>
<tr>
<td>Samsung (new)</td>
<td>Previously admin/4321, but new firmwares require unique password creation</td>
</tr>
<tr>
<td>Samsung (old)</td>
<td>admin/1234</td>
</tr>
<tr>
<td>Sony</td>
<td>admin/admin</td>
</tr>
<tr>
<td>Speco</td>
<td>admin/1234</td>
</tr>
<tr>
<td>Stardot</td>
<td>admin/admin</td>
</tr>
<tr>
<td>Starvedia</td>
<td>admin/&lt;blank&gt;</td>
</tr>
<tr>
<td>Trendnet</td>
<td>admin/admin</td>
</tr>
<tr>
<td>Toshiba</td>
<td>root/ikwd</td>
</tr>
<tr>
<td>VideoIQ</td>
<td></td>
</tr>
<tr>
<td>W-Box</td>
<td>admin/wbox123</td>
</tr>
<tr>
<td>Wodsee</td>
<td>admin/&lt;blank&gt;</td>
</tr>
</tbody>
</table>
What we are **not** talking about

**IP Weakness**

(This guy can help you create some! INTERNETZ FTW!)
What we are not talking about

Deauth 101
What we are **not** talking about

**SHODAN**
Who cares!
What if?
Step 1 – Get into the mood
Step 2 – Get some information
Step 3 – Plan the attack!
The Attack
#DIVERSITY!
Which ones are ‘Security’ Cameras?
What was tested?

- Offline time
- Does it do notification
- How long does the notification take
- Does it notify you if it comes back online?
- Any cached video
- Onboard video storage
- Wired network option
- Type of power (Battery vs. Wired)
- Addition Equipment needed for function?
- Other performance observations
Test Procedures

• **0:00** - Stopwatch starts

• **1:00** - Targeted De-authorization Begins
  • Every :30 Hand wave for motion recognition

• **11:00** - Targeted De-authorization Ends

• **16:00** - Test ends
The Setup

“Timer”

Test Camera

iPad w/ Cam Apps on Separate Network
Time for the Demo Video
You get the idea,
Now the Results...
Kuna

Smart Security Light
- Craftsman Version
Kuna

Results
- Recovers after 1:39 seconds

Positive
- It’s a light
- It’s WIRED!

Negatives
- App Only Notifications
- Status Lights!
- After offline for 10 minutes it doesn’t recover at all
MY KUNA IS OFFLINE

If your Kuna has been offline for more than 10 minutes, you may need to take it back through the set-up process to bring it online again. Here are a few simple steps to try and get it back online:

Step 1 - Power Cycle Your Kuna
Please turn off your Kuna (using the light switch it's connected to) and wait at least 10 seconds. Then, turn the light switch back on.

Step 2 - Check the Status LED
After the power is back on, the status LED at the bottom of your Kuna should flash from red to green, and then to solid blue in about a minute. If it does not turn blue after a minute, please proceed to Step 3.

Step 3 - Run Through the Set-Up Process
Please take your Kuna through the set-up process again to reconnect it to your Wi-Fi network.

Immedia

Blink Wire-Free HD Home Monitoring & Alert System
Immedia Blink

Results
- Recovers after :09 seconds
- Records video in 5-10 second clips

Positive
- Easy to mount?

Negatives
- Requires a base-station (sync module)
- Battery Powered
- No SD or onboard storage
- No wired option
Amcrest

Results
- Recovers after 2:00 minutes

Positive
- 10 seconds onboard memory
- Wired Option

Negatives
- On/Off switch on unit
D-Link

Results
- Recovers after 1 minute

Positive
- SD Option
- Doesn’t claim to be a security camera!

Negatives
- No wired option
Netgear

Arlo Smart Home Security
Netgear Arlo

Results
- Recovers after :45 seconds

Positive
- Versatile!
- That sticker!

Negatives
- Requires a base-station
- Battery Powered
- No SD or onboard storage
- No wired option
Logitech

Logi Circle
Logitech Circle

**Results**
- Recovers after 1:30 seconds

**Positive**
- Consistant device push notifications

**Negatives**
- On/Off switch on unit
- No SD or onboard storage
- No wired option
Belkin

Results
© Recovers after (:10) seconds

Positive
♦ 10 seconds onboard memory

Negatives
☆ On/Off switch on unit
☆ Inconsistent device push notifications
Samsung Smart Cam

Results
- Recovers after 10 seconds *If there is immediate movement

Positive
- SD Card Option
- Wired Option

Negatives
- Cloud option not available - SD Storage Only
Canary

Results
- Recovers after 02 seconds *If there is immediate movement

Positive
- Deauth quick Recovery
- Wired Option
- *Notification after 30 minutes offline

Negatives
- Movement required for recovery
Results

- Recovers after :20 seconds

Positive

- Keeps between :30 - 4min cache
- Push notifications for activity are consistent

Negatives

- No SD Option
- No Wired Option
Bad Guys won’t put in the effort...

Thieves using a $17 power amplifier to break into cars with remote keyless systems.
What should consumers do then?

- Wired > Wireless Cameras
- Verify and understand the limitations of the products
- Cameras have unintended great uses!
  - Real Estate
  - Household / Business Cleaners
  - Dog Walkers
  - Etc.
Windows for Consumers
Late last year, Duo Labs, the security research team of Duo Security, purchased a stack of OEM (Original Equipment Manufacturer) laptops to see how secure they were. Some problems immediately jumped out at us, like the eDellRoot issue, but a few other issues took a bit more sorting through.

I took a look at the network by sniffing the laptops as they were first booted, and then, once configured. The idea was to judge how secure the laptops
What We Tell Users

• Patch your devices
• Install Anti-virus
• Use HTTPS only
• Use a password manager
• Watch out for suspicious downloads
• Don’t use suspicious wifi
• Pick “strong” passwords*
Let's talk about the past

• Back at DEF CON 20 Zack gave a talk...
The Old Focus

- Corporate Accounts
- Internal Networks
- Relay Auth
- Mmmmm. Data
NTLM Hashes

- `Md4(unicode($password))`
- 128 bit hash
- Used for network authentication and signing
NTLM Network Authentication

- 3 way Handshake
  - Client -> Server: Sup, what do you support
  - Server -> Client: We speak klingon, Challenge Code
  - Client -> Server: My voice is my passport, verify me.

- Two Flavors
  - V1 – Server Challenge Only
  - V2 – Client challenge added to server challenge

- Microsoft has recommended to move away from NTLM in favor of Kerberos

- Auto Authentication to Things
WPAD

• DHCP Option
• WPAD from DNS from DHCP
• LLMNR
• NBNS

• Windows 10 seems to be authing less to this, but some applications (LOOKING AT YOU CHROME) do.
Not Just WPAD

• This isn’t another “wpad is bad” talk.
• Injection of UNC paths in IE/Edge
• File formats with UNC Paths
• 3rd party applications without CORS
Corporate Internal Only?

Exchange Web Services
...wait...most orgs....holy crap....
- Negotiate (includes NTLM) by default
- So External impact by NTLM relaying to
MOST ORGANIZATIONS!
- Get all the emails, contacts, calendar, and
setup email rules...

TWNED in 60 Seconds
THIS IS STILL A HUGE ISSUE

You might see where this is going
Corporate Internal Only?

- We’ve never really talked about impact of cracking the NTLM Network Challenges...
  - Corporate? VPN Access, Sharepoint, Shared Passwords, local admin if permissions are set?
- What about personal users?
  - Shared passwords?
  - Local file shares?
  - Provides only guest access remotely and admin.
One account for all things Microsoft

Set up a Microsoft account, and all of your Microsoft services—from Office to Outlook to Skype—work together through a single sign-in. Whether you use Windows, iOS, or Android devices, or switch between all three, your account keeps everything you need on the device in hand.

All of these services work with your Microsoft account

Whether you use a couple Microsoft services or all of them, your account keeps everything important to you—settings, photos, and files—with you on any device.
One account for all things Microsoft

Set up a Microsoft account, and all of your Microsoft services—from Office to Outlook to Skype—work together through a single sign-in. Whether you use Windows, iOS, or Android devices, or switch between all three, your account keeps everything you need on the device in hand.

Sign in  Create account

All of these services work with your Microsoft account

Whether you use a couple Microsoft services or all of them, your account keeps everything important to you—settings, photos, and files—that’s with you on any device.
ZackAttack Update

Release 0.1.2

“for Zacks who can’t code good and wanna learn to do other stuff good too”
<table>
<thead>
<tr>
<th>Email Address</th>
<th>Microsoft Account ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>outlook.com::MicrosoftAccount:8877665511223344:4e1f9c9ae799</td>
<td></td>
</tr>
<tr>
<td>outlook.com::MicrosoftAccount:8877665511223344:dfdb7bea83</td>
<td></td>
</tr>
<tr>
<td>gmail.com::MicrosoftAccount:8877665511223344:f1a22</td>
<td></td>
</tr>
<tr>
<td>gmail.com::MicrosoftAccount:8877665511223344:421420df0887dc</td>
<td></td>
</tr>
<tr>
<td>gmail.com::MicrosoftAccount:998877665543322:ff142bc</td>
<td></td>
</tr>
<tr>
<td>hotmail.com::MicrosoftAccount:8877665511223344:fb8d381f3ae</td>
<td></td>
</tr>
<tr>
<td>gmail.com::MicrosoftAccount:8877665511223344:fb834779908</td>
<td></td>
</tr>
<tr>
<td>gmail.com::MicrosoftAccount:8877665511223344:fa2ae64da151bc77e</td>
<td></td>
</tr>
<tr>
<td>outlook.com::MicrosoftAccount:9988776655443322:f75f2422599</td>
<td></td>
</tr>
<tr>
<td>hotmail.com::MicrosoftAccount:9988776655443322:20d724ad3668df</td>
<td></td>
</tr>
</tbody>
</table>
So what?

- At a minimum, information disclosure of email of the user. That’s bad enough.
- Offline password attacks.
- And if you can crack the password...
Personal info

Privacy and cookies statement
To change the personal info that other people see, go to Profile.

Birthdate
March 13 1937

Gender
Male

Country/region
United States

State
Select...

ZIP code
60657

Time zone
Central Time – CST
Payment options

Add a payment option
Credit and debit cards, PayPal, bank account, etc.

Microsoft account

Redeem a code or gift card
Redeem Bitcoin

Send a gift card by email

Card info

Name on card
Zachary Fasel

Credit card number
**6505

Billing address

Expiration date
09/2016

For purchases in
United States
It turns out, a billing address and the last four digits of a credit card number are the only two pieces of information anyone needs to get into your iCloud account. Once supplied, Apple will issue a temporary password, and that password grants access to iCloud.
<table>
<thead>
<tr>
<th>Search Term</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>how to poison my boss and make it look like...</td>
<td>9:53 am</td>
</tr>
<tr>
<td>is defcon cancelled?</td>
<td>9:52 am</td>
</tr>
<tr>
<td>mcafee for president</td>
<td>9:51 am</td>
</tr>
<tr>
<td>how do i hack microsoft accounts</td>
<td>9:50 am</td>
</tr>
</tbody>
</table>
Heavy Microsoft User?

- Outlook Emails!
- OneDrive
- Remote File Access
- WiFi Sense
Offline Cracking? That’s Original….

- Breaches - both services and local
- Encrypted files / datasets
- Really bad services
- But harvestable from a LAN? And as a single signon token?
What We Tell Users

• Patch your devices
  • Doesn’t Matter
• Install Anti-virus
  • Some HIDS catch 1122334455667788, but that’s it
• Use HTTPS only
  • It’s only a matter of time you hit a HTTP endpoint
• Use a password manager
  • Still have your Microsoft account, but helps with other sites
• Watch out for suspicious downloads
  • Does not apply
• Don’t use suspicious wifi
  • Are you going to not use wifi when on the road?
• Pick “strong” passwords
What We Shouldn’t Be Telling Users

- Use this cool VPN service! Totally Trustworthy!
What We Need To Tell Users

• Pick strong passphrases
• Enable 2-Factor (yes, it’s 10+ steps)
• Use unique creds per site
• Maybe avoid hotmail/outlook mail for a bit
How can we fix it?

• Disable NTLM Auth (but what user is going to do that)
• Don't use a Microsoft account to log in to your Windows system
So TL;DR

• Got a Stock Windows Laptop?
• Attacker on the same network?
• Use a Microsoft Account to log in?
• You’re pwned.
Summary of Issues

- Fitness / Notification Devices can be tracked through various means
- WiFi Security Cameras can get blasted offline and see/know nothing
- Consumer Windows Laptops leak identity and creds for offline cracking
Acknowledgements

Hat Tip to Other Research
• Mike Ryan, Michael Ossmann, Dominic Spill, Zero_Chaos, and Scott Lester on BLE
• Simple Nomad for OEM device research
• Mubix for complaining about ZackAttack enough