



IoT and Wearables

Secure Mobile IoT Application Development

Dr. Hale

University of Nebraska at Omaha
Secure Mobile IoT Development

Today's Class: More on Hybrid apps and Lab time

Part 1: IoT Background

stats and intro

attack types

protocol

Part 2: Demo (Demo Gods Permitting)

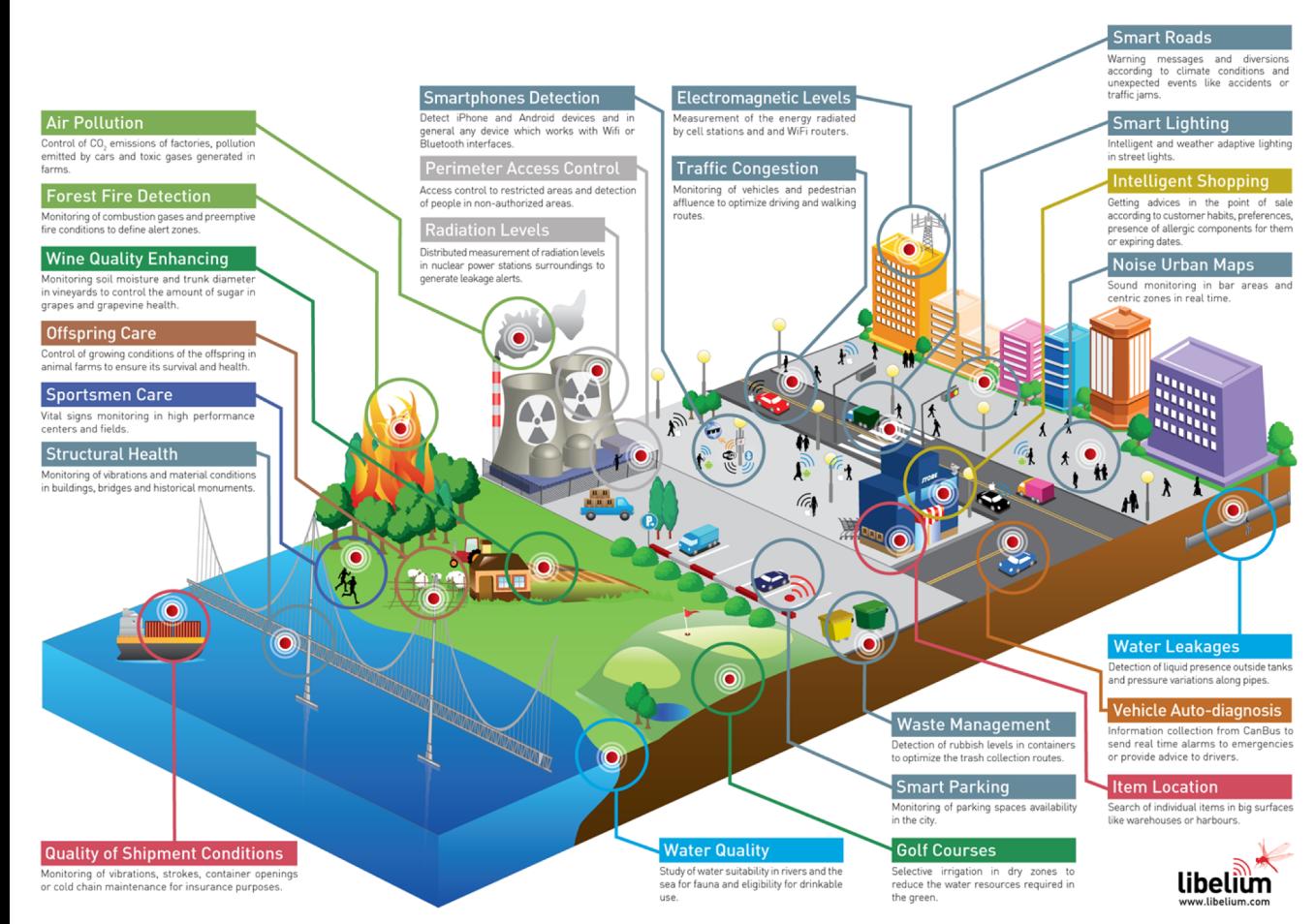
Part 3: Lab time (new IoT lab up)



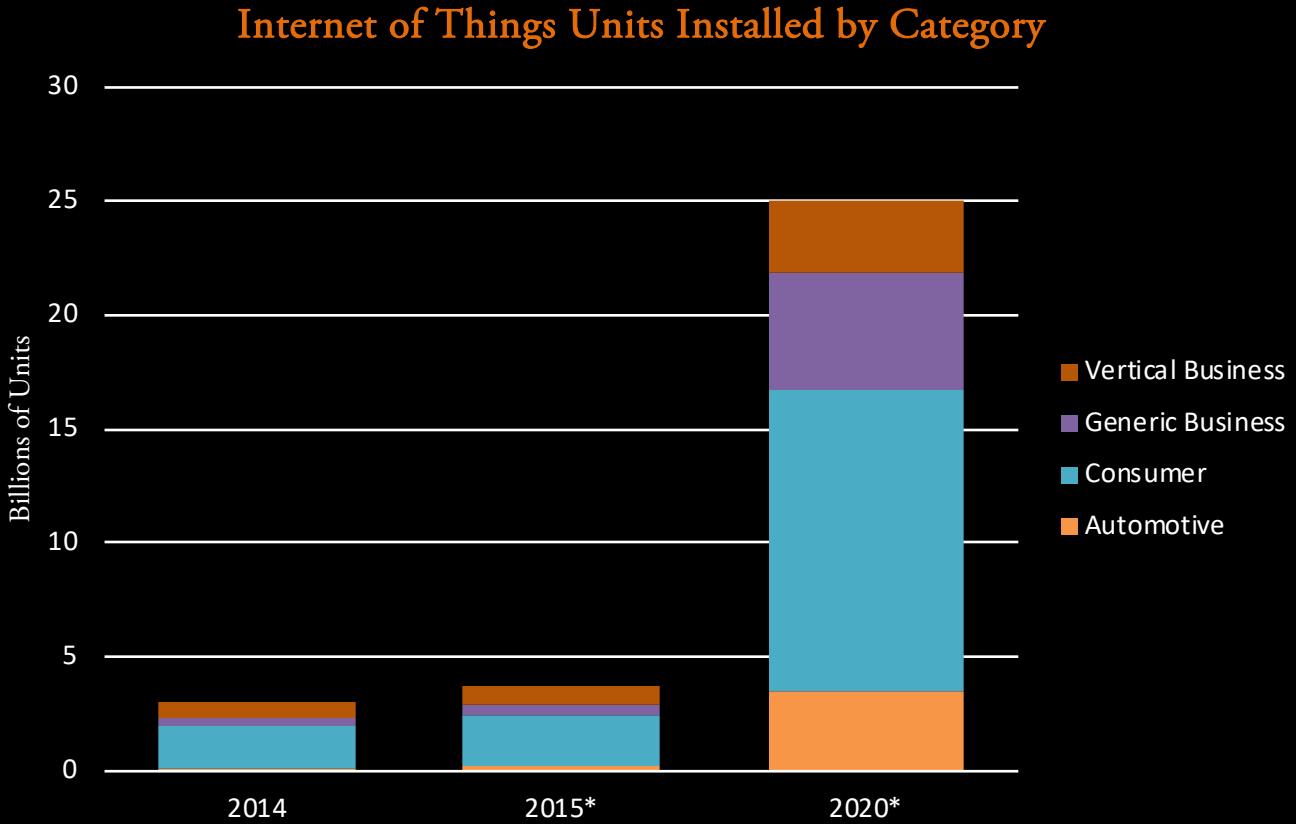
What is the internet of things and
why should you care?

What is the internet of things?

Sensors Embedded Everywhere



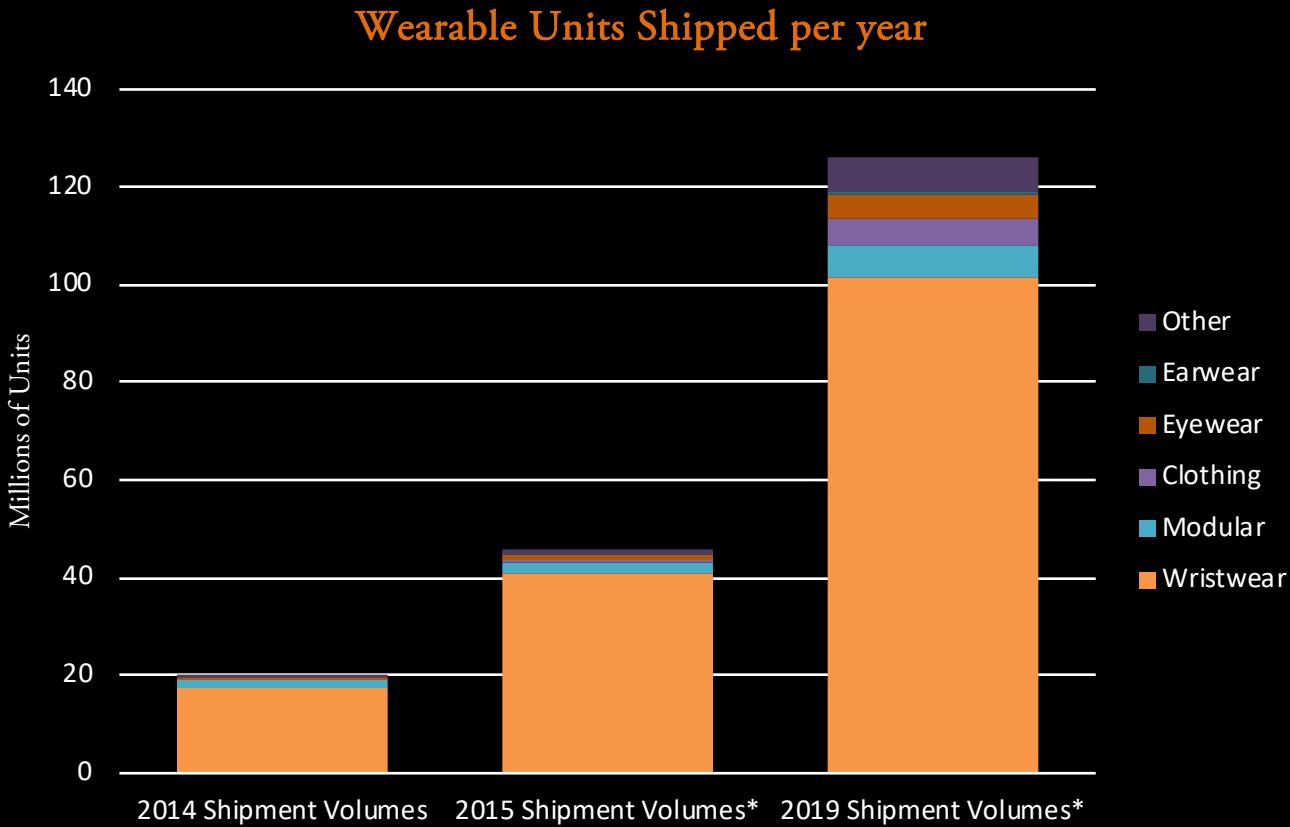
An Idea of Scale (IoT)



* Forecasted figures

Source: Gartner: 4.9 Billion Connected “Things” will be in use by end of 2015, November, 2014

An Idea of Scale (Wearables)



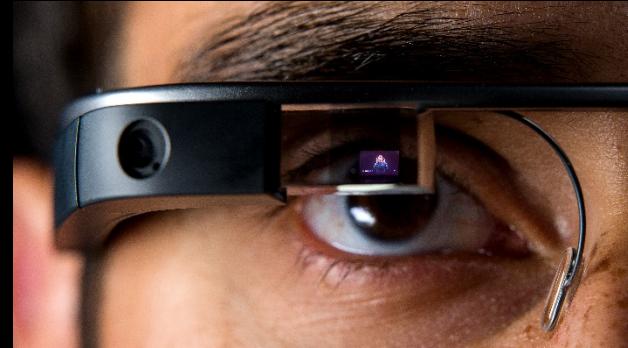
* Forecasted figures

Source: IDC Worldwide Quarterly Wearable Device Tracker, March 30, 2015

133.4% Growth from 2014 to 2015 (19.6M to 45.7M)

45.1% Five-year compound annual growth rate (19.6 to 126.1)

fitbit
surge™



GLASS

NIKEFUEL

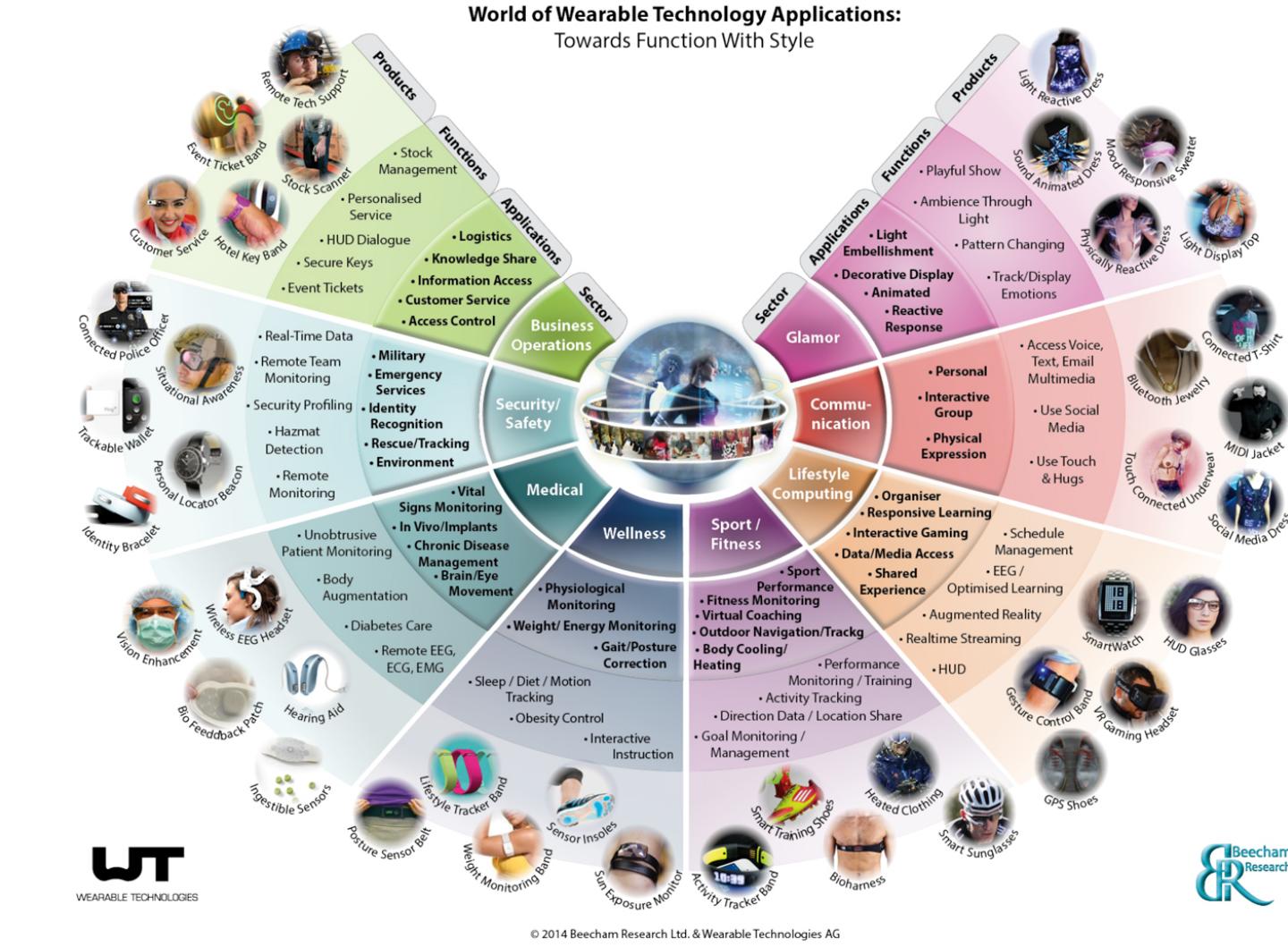


...ok so what? its sleep and pedometer data.

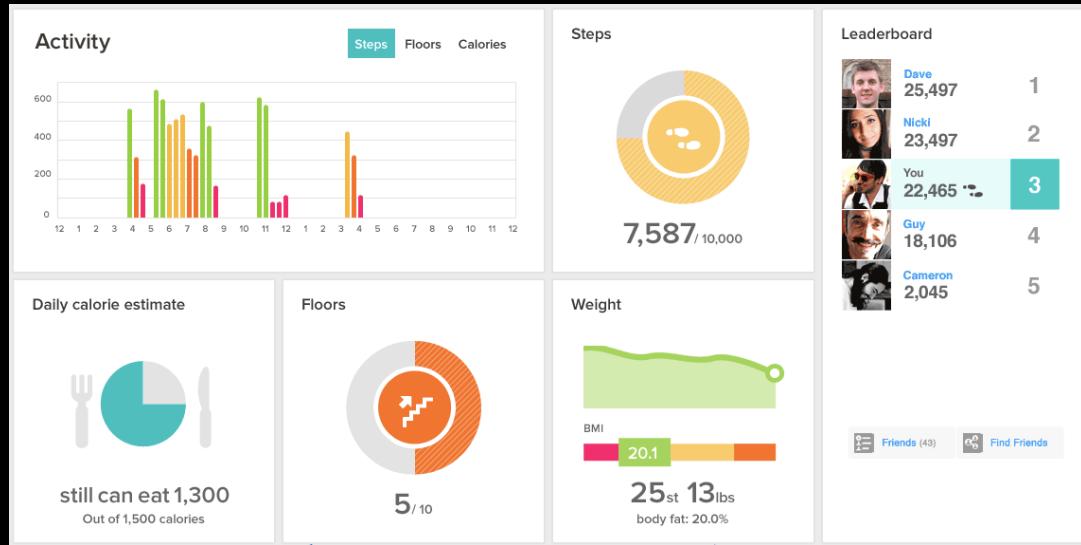
UP
by JAWBONE™



Not
exactly.



The possibilities:



Big data is also important for other sectors

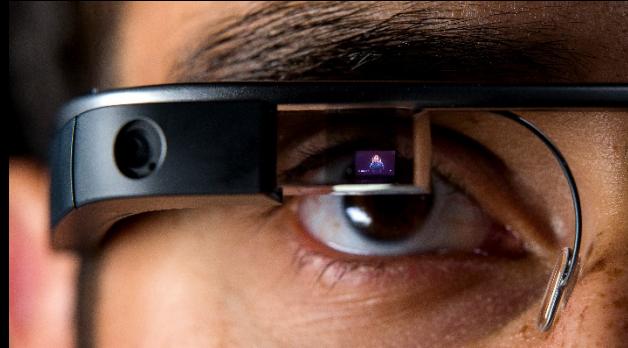
Medical -> patient well being & diagnosis

Military -> warfighter well being / operational intelligence



SITUATIONAL AWARENESS
Yeah it's important

fitbit
surge™



GLASS

...there are many security challenges

NIKEFUEL



UP
by JAWBONE™



(in)security landscape

Hackers are coming for your smartwatch



CALE GUTHRIE WEISSMAN | [✉](#) [Twitter](#)

APR. 13, 2015, 1:35 PM



Nike+ FuelBand SE BLE Protocol Reversed
Simon Margaritelli

AUTHENTICATION, BLUETOOTH, NIKEFUEL

29 Jan 2015 IN

REVERSING, NIKE, NIKE+ FUELBand SE, FUELBand, NIKE FUEL

Researchers find about 25 security vulnerabilities per Internet of Things device

Computerworld | Aug 4, 2014 12:32 PM PT

Security Analysis of Wearable Fitness Devices (Fitbit)

Britt Cyr, Webb Horn, Daniela Miao, Michael Specter
Massachusetts Institute of Technology
Massachusetts, U.S.A.
[.edu](mailto:bcyr@mit.edu), dmiao@mit.edu, specter@mit.edu

How I hacked my smart bracelet*

By Roman Unuchek on March 26, 2015, 11:00 am

Anonymity is the internet's next big battleground

Jon Card

Bluetooth: With Low Energy comes Low Security

Mike Ryan
iSEC Partners

Domain security issues

User Awareness and Privacy Behaviors

Don't recognize data sensitivity or misuse
May install malware or malicious apps
Apps may be an invasion of privacy

Web Application

Standard Web attacks (XSS, SQL injection, CSRF, etc)
Information Leakage (e.g. geotagging in social media)
Secure data storage and acceptable data usage

Mobile Application

Third party tracking apps accessing data (stored/in-transit)
Data encoding and transmission
Resource consumption

Wearable Hardware

Physical tampering
Data encoding and transmission
Resource consumption

Inter-domain security issues

User Awareness and Privacy Behaviors

Web Application

Insecure Wi-Fi or 4G
Lack of API Security (HTTPS/CORS/CSRF)

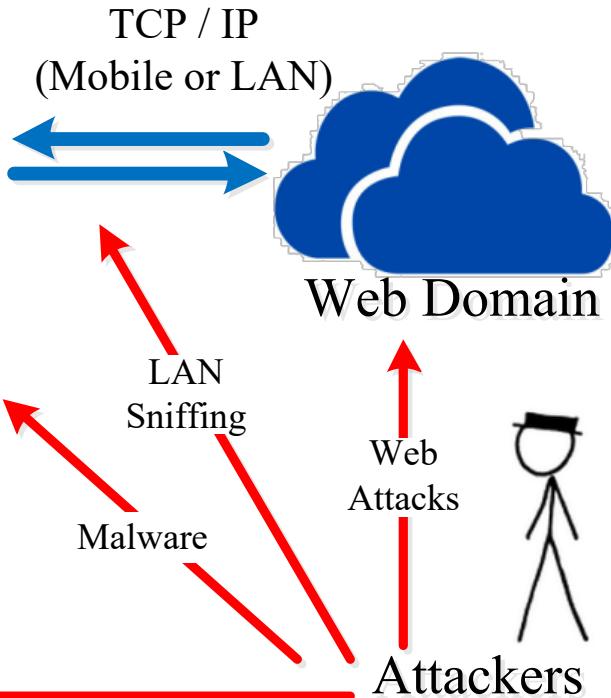
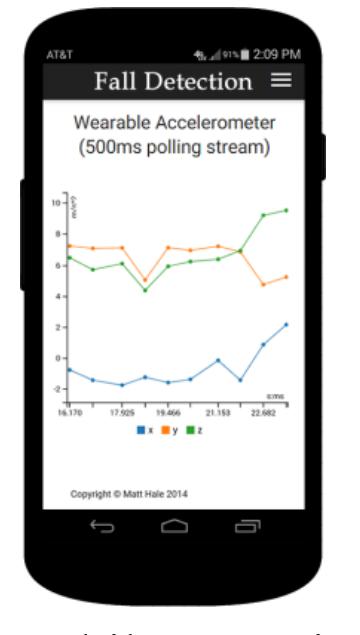
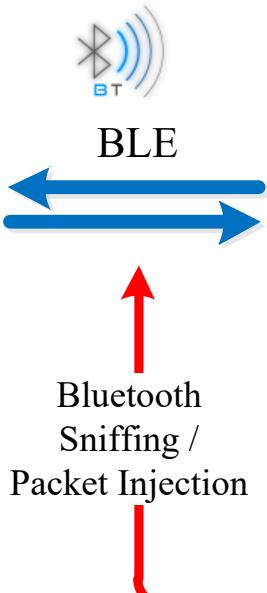
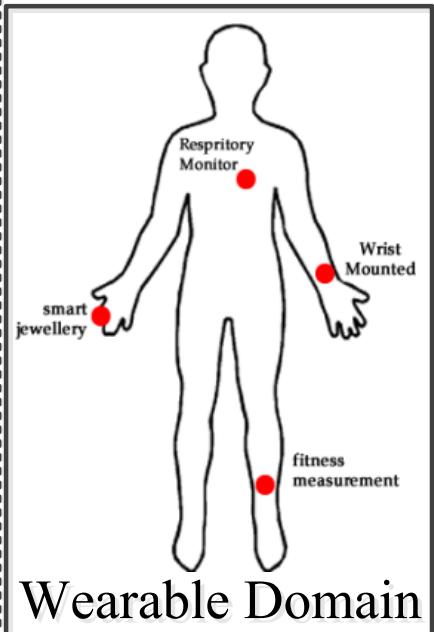
Mobile Application

Lack of over-the-air encryption
Man-in-the-middle attacks
Denial of service / Resource consumption

Wearable Hardware

Attack vectors for a typical app

Wearable Application



Select logitem to change

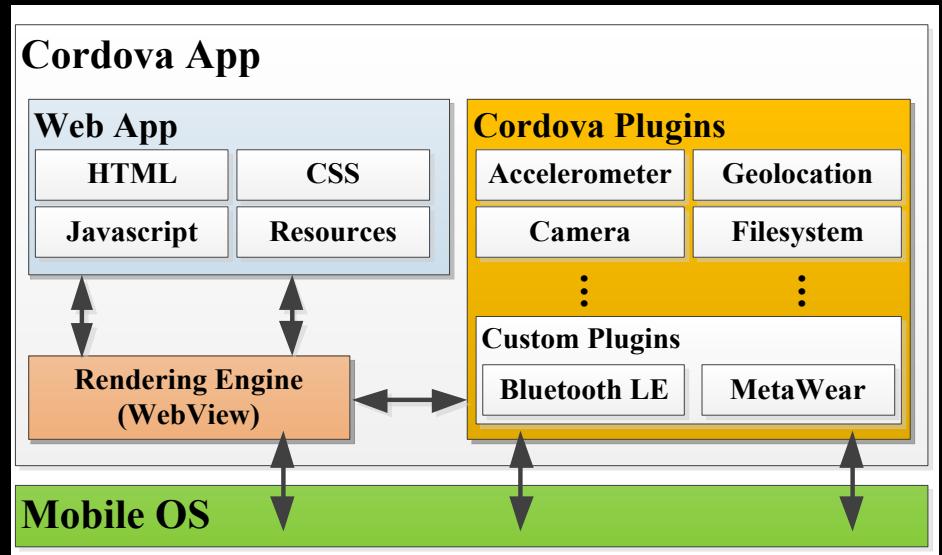
Action: ▼ 0 of 100 selected

id	type	data	datetime
3386	9 (LED Event)	{"op": "off", "color": "green", "timestamp": 1427179.....}	March 1, 2015, 6:41 a.m.
3385	10 (Temperature)	{"temp": 22.71, "timestamp": 1427179691010}	March 1, 2015, 6:40 a.m.
3384	11 (Accelerometer)	{"op": "on-flash", "color": "green", "timestamp": 14.....}	March 1, 2015, 6:39 a.m.
3383	11 (Accelerometer)	{"x": 0.21847090125083923, "y": -1.2078747749328613, ".....}	March 1, 2015, 6:39 a.m.
3382	11 (Accelerometer)	{"x": 0.20290859043598175, "y": -1.184531331062317, "z":	March 1, 2015, 6:39 a.m.
3381	11 (Accelerometer)	{"x": 0.11851298063993454, "y": -0.8038532137870789, ".....}	March 1, 2015, 6:39 a.m.

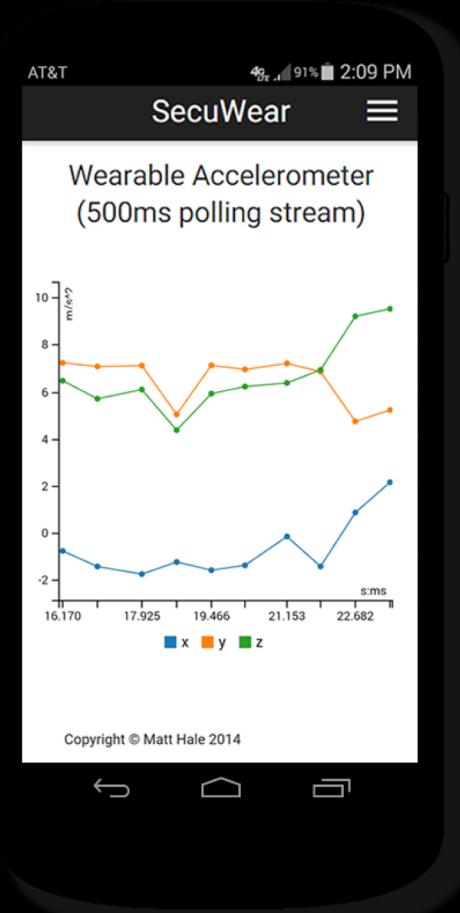
example API*
(Web Domain)

* Similar to what we used in class to store persistent mobile attacks (e.g. XSS)

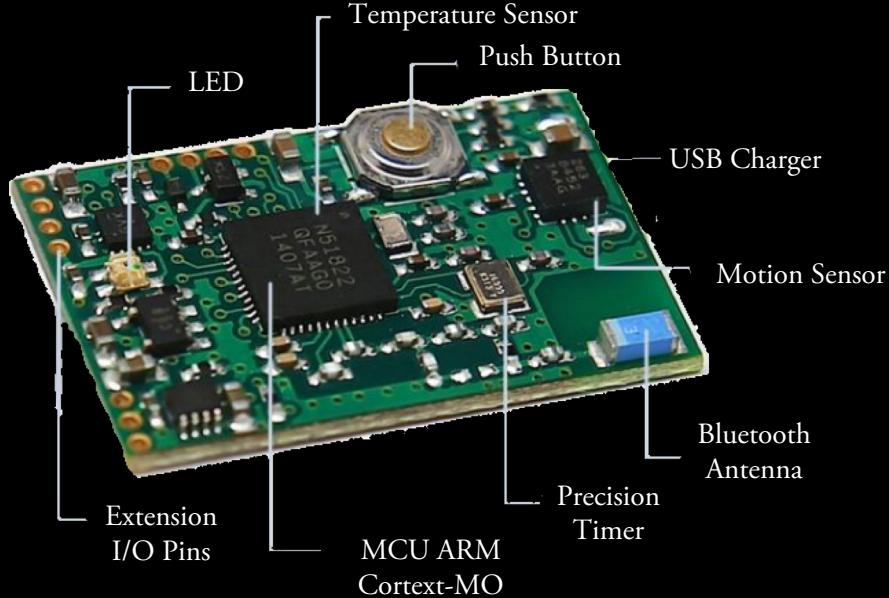
Ex Mobile App
(Mobile Domain)



Ex Mobile App* (Mobile Domain)



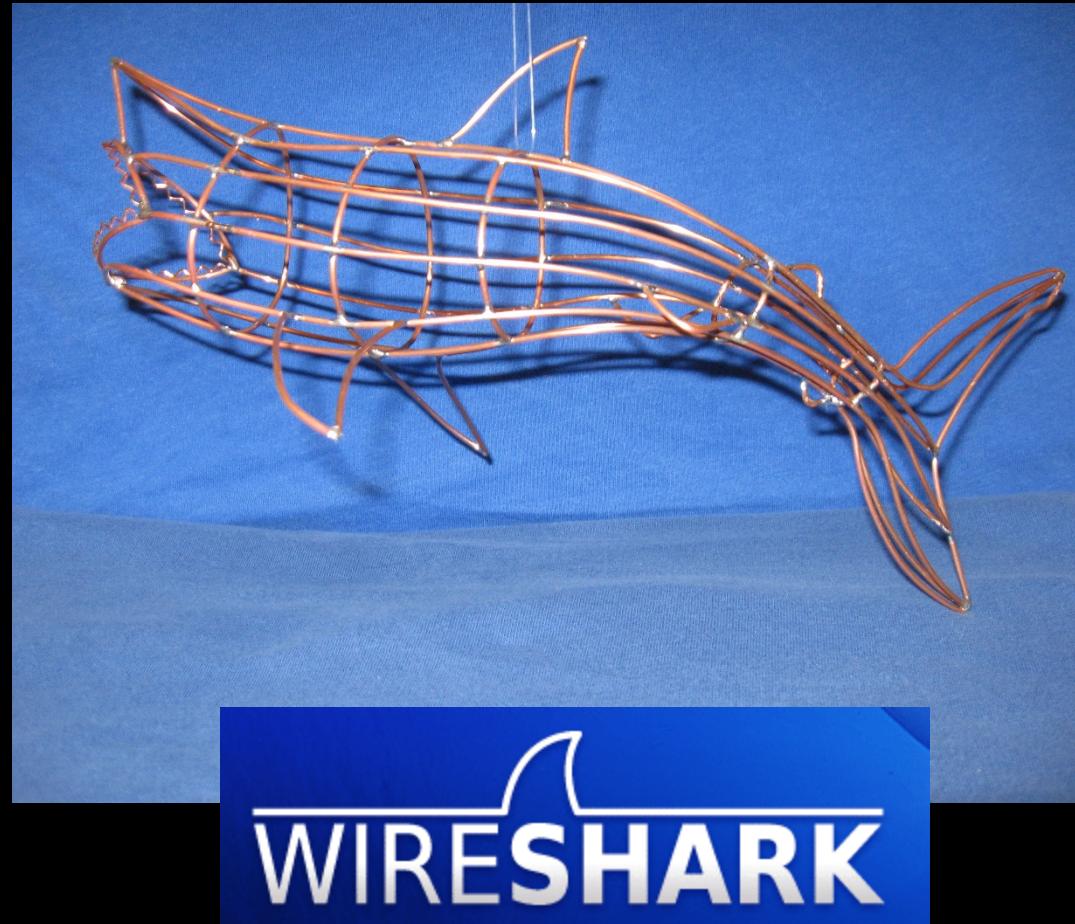
* Other accessible features include temperature sensor, LED, and battery level (based on MetaWear module)



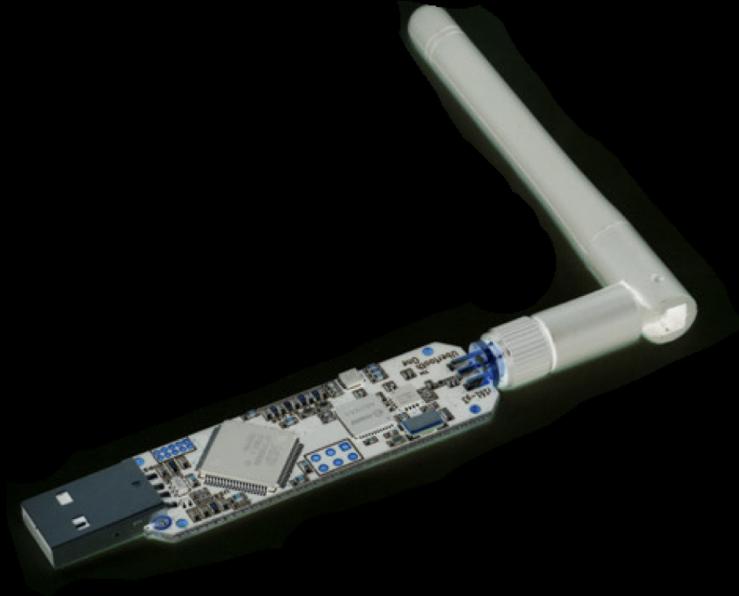
Ex. Wearable – Metawear
(Wearable Domain)



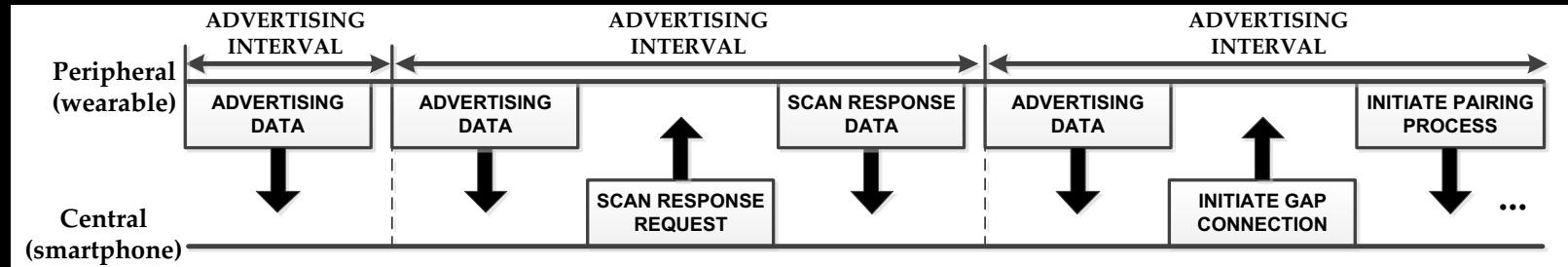
Sniffing Tools (Inter Domain)



Sniffing Tools (Inter Domain)

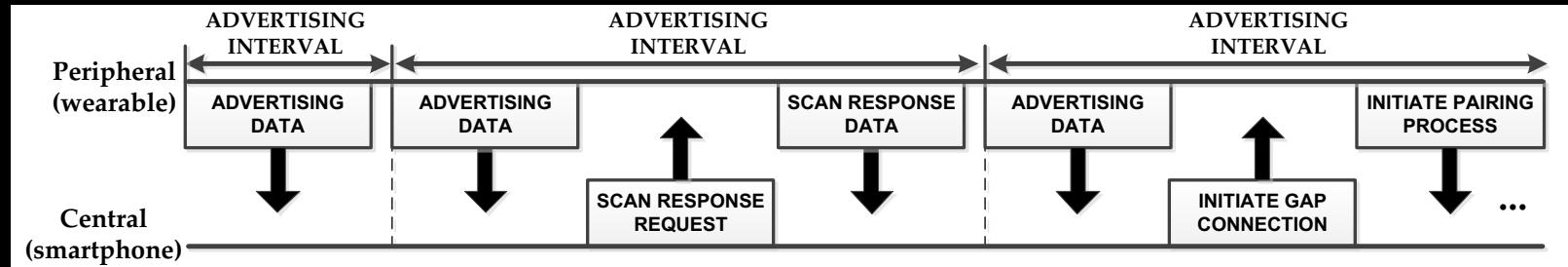


Ubertooth One



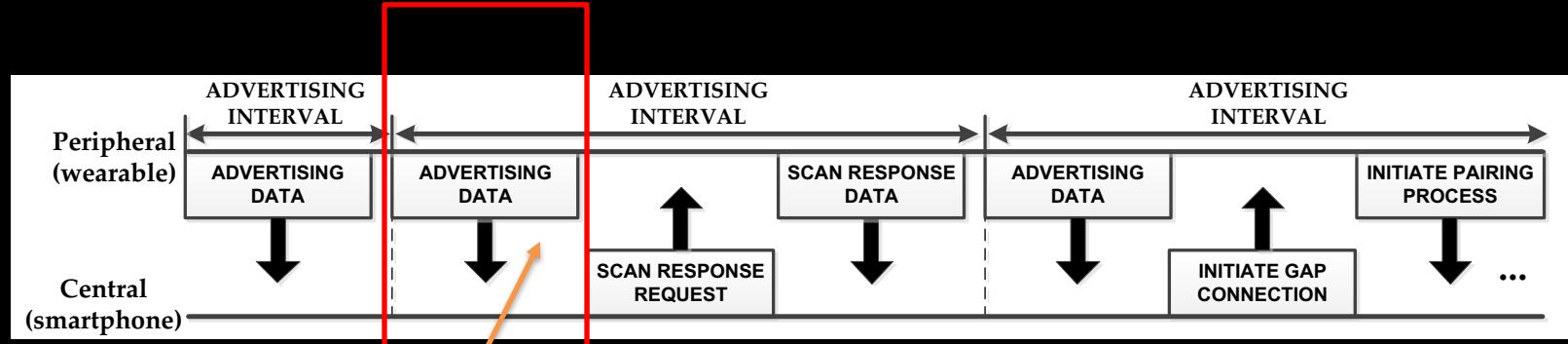
Mainly focused on Bluetooth LE

Sniffing Process



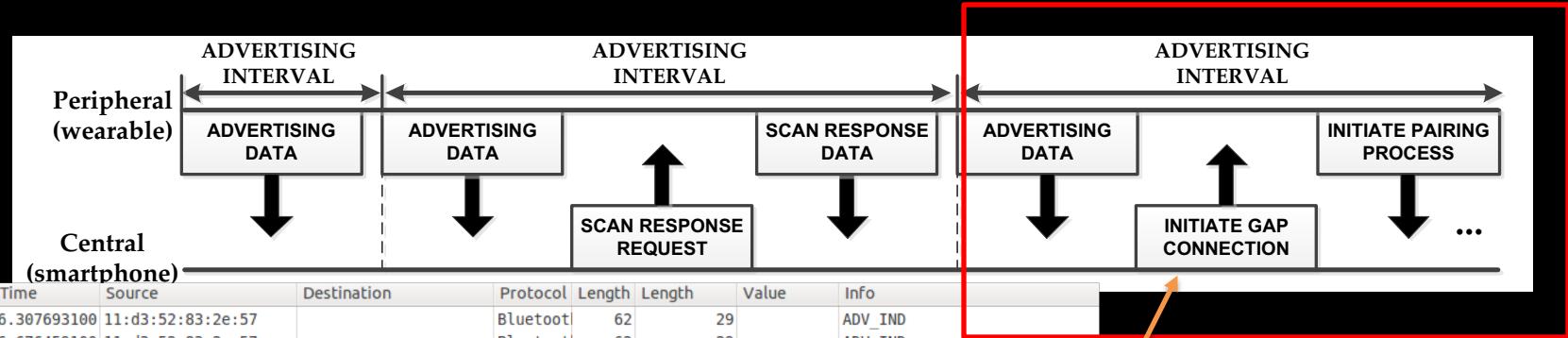
Here is what it looks like...

Sniffing Process



No.	Protocol	Length	Advertising Address	PDU Type
12	LE LL	70	dc:46:a3:10:b7:43	ADV_IND
▶ Packet Header: 0x2540 (PDU Type: ADV_IND, TxAdd=false, RxAdd=false)				
Advertising Address: dc:46:a3:10:b7:43 (dc:46:a3:10:b7:43)				
▼ Advertising Data				
▶ Device Name (shortened): MetaWear				
▶ Flags				
▶ 128-bit Service Class UUIDs (incomplete)				
▶ CRC: 0xd98e50				
0010	53 87 77 21 80 7f 00 00	d6 be 89 8e 40 25 43 b7	S.w!....@%C.	
0020	10 a3 46 dc 09 08 4d 65	74 61 57 65 61 72 02 01	.F...Me taWear..	
0030	06 11 06 5a e7 ba fb 4c	46 dd d9 95 91 cb 85 00Z...L F.....	
0040	90 6a 32 9b 71 0a		.j2.q.	

Sniffing Process



No.	Time	Source	Destination	Protocol	Length	Length	Value	Info
96	6.307693100	11:d3:52:83:2e:57		Bluetooth	62	29		ADV_IND
97	6.676459100	11:d3:52:83:2e:57		Bluetooth	62	29		ADV_IND
98	6.695579800	57:23:d7:fe:b4:d9		Bluetooth	70	37		ADV_IND
99	6.696074300	74:e4:72:c6:ca:4e	57:23:d7:fe:b4:d9	Bluetooth	67	34		CONNECT_REQ
100	6.705760000			Bluetooth	33	0		Empty Data PDU
101	6.705985600			Bluetooth	33	0		Empty Data PDU
102	6.706248100			Bluetooth	39	6		LL Control PDU: LL_VERSION_ID

DLT: 147, Payload: btle (Bluetooth Low Energy)

Bluetooth Low Energy

Access Address: 0x8e89bed6

Packet Header

Init Address: 74:e4:72:c6:ca:4e (74:e4:72:c6:ca:4e)

Advertising Address: 57:23:d7:fe:b4:d9 (57:23:d7:fe:b4:d9)

Connection Request

Connection AA: 0xaf9a825d

CRC Init: 0xf9a13e

Window Size: 0x03

Window Offset: 0x0006

Interval: 0x0018

Latency: 0x0000

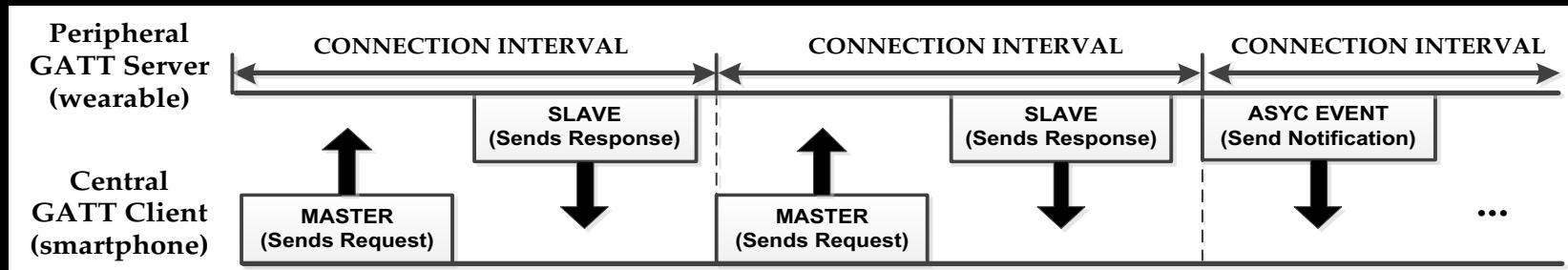
```

0000 00 00 18 00 93 00 00 00 36 75 0c 00 00 62 09 00 ..... 6u...b..
0010 81 19 1c 08 80 7f 00 00 d6 be 89 8e c5 22 74 e4 ..... ...."t.
0020 72 c6 ca 4e 57 23 d7 fe b4 d9 5d 82 9a af 3e a1 r..NW#...]...>.
0030 f9 03 06 00 18 00 00 00 48 00 ff ff ff ff 1f a9 ..... H.....
0040 0 01 01

```

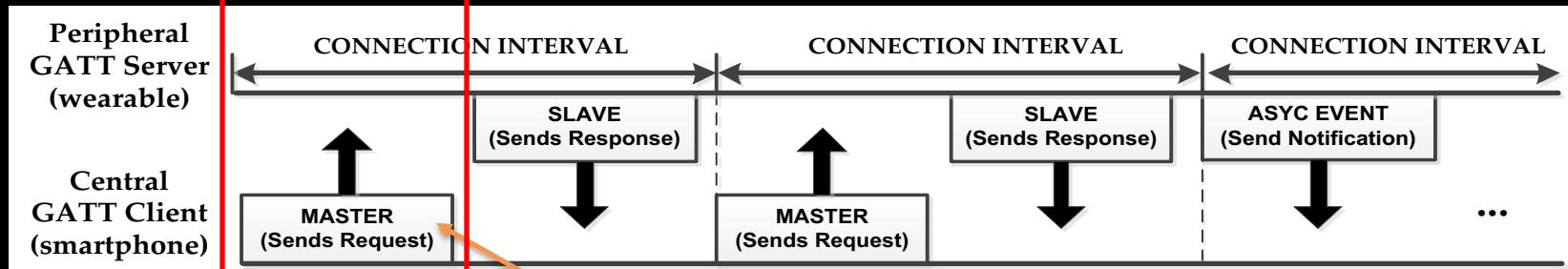
Capture this and you can follow a connection

Sniffing Process



(after pairing)

Sniffing Process



Sniffing Process

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Length	Value	Info
113	6.856750100			Bluetooth	33	0		Empty Data PDU
114	6.855829700			L2CAP	42	9		Connection oriented channel
115	6.856059600			Bluetooth	33	0		Empty Data PDU
116	6.856354000			L2CAP	44	11		
117	6.856904000			L2CAP	44	11		
118	6.857159600			Bluetooth	33	0		Empty Data PDU
119	6.857454000			ATT	44	11		Read By Group Type Request, GATT Primary Service Desc
120	6.857709900			Bluetooth	33	0		Empty Data PDU
121	6.885756300			Bluetooth	33	0		Empty Data PDU
122	6.886180400			ATT	57	24 0018,0118,0		Read By Group Type Response, Attribute List Length:
123	6.915818700			ATT	44	11		Read By Group Type Request, GATT Primary Service Desc
124	6.916074400			Bluetooth	33	0		Empty Data PDU
125	6.945460500			Bluetooth	33	0		Empty Data PDU
126	6.946082800			ATT	45	12 0a18		Read By Group Type Response, Attribute List Length:

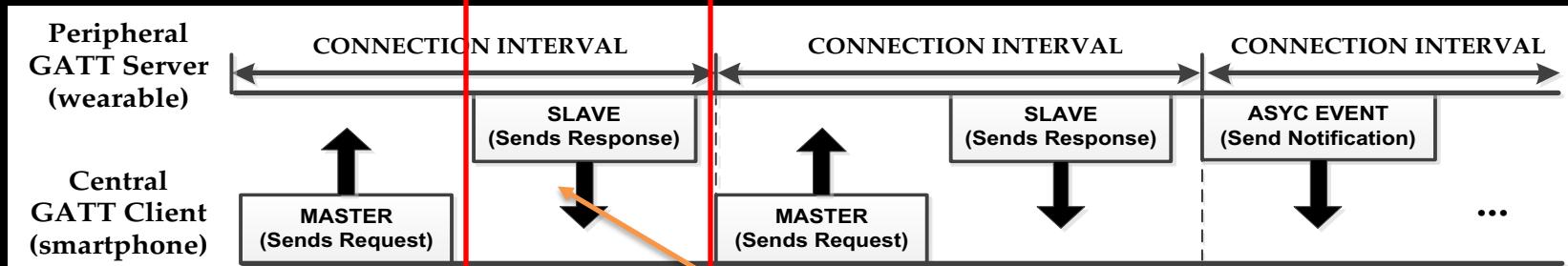
Access Address: 0xaf9a825d
 ▶ Data PDU Header: 0x0b0e
 ▼ Bluetooth L2CAP Protocol
 Length: 7
 CID: 0x0004
 ▶ Bluetooth Attribute Protocol
 CRC: 0x6c88b1

```

0000 00 00 18 00 93 00 00 00 36 75 0c 00 00 88 09 00 ..... 6u.....
0010 66 b9 34 08 80 7f 00 00 5d 82 9a af 0e 0b 07 00 f.4..... ]....
0020 04 00 10 01 00 ff ff 00 28 b1 88 6c ..... (.1
  
```

Frame (frame), 44 bytes. Packets: 3380 Displayed: 3380 Marked: 0 Load time: 0:00:030 Profile: Default

Sniffing Process



Some actual
(accelerometer) data sent
from MetaWear to our app

Sniffer capture showing Bluetooth traffic:

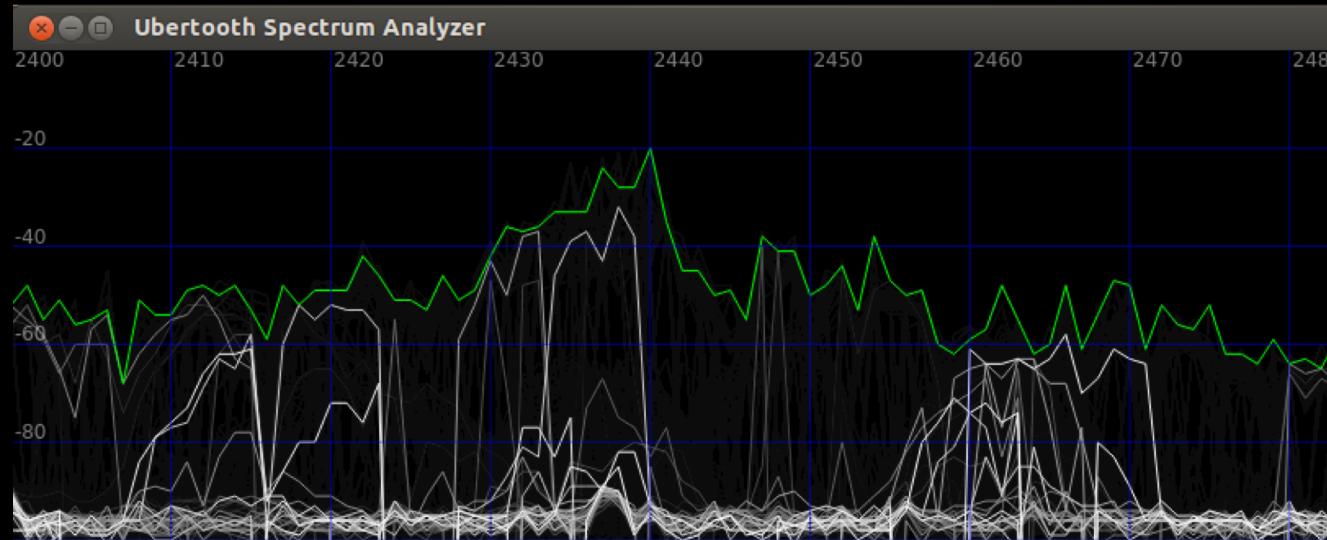
No.	Time	Source	Destination	Protocol	Length	Length	Value	Info
113	0.020750100			L2CAP	45	9		Empty Data PDU
114	6.855829700			L2CAP	42	9		Connection oriented channel
115	6.856059600			Bluetooth	33	0		Empty Data PDU
116	6.856354000			L2CAP	44	11		
117	6.856904000			Bluetooth	33	0		
118	6.857159600			L2CAP	44	11		
119	6.857454000			Bluetooth	33	0		
120	6.857709900			ATT	44	11		Read By Group Type Request, GATT Primary Service Decl
121	6.885756300			Bluetooth	33	0		Empty Data PDU
122	6.886180400			Bluetooth	33	0		Empty Data PDU
123	6.915818700			ATT	57	24	0018,0118,0	Read By Group Type Response, Attribute List Length: 3
124	6.916074400			Bluetooth	44	11		Read By Group Type Request, GATT Primary Service Decl
125	6.945460500			Bluetooth	33	0		Empty Data PDU
126	6.946082800			Bluetooth	33	0		Empty Data PDU
				ATT	45	12	0a18	Read By Group Type Response, Attribute List Length: 1
GATT 0x0004								
▾ Bluetooth Attribute Protocol Opcode: Read By Group Type Response (0x11) Length: 6								
▾ Attribute Data, Handle: 0x0001, Group End Handle: 0x0007 ▾ Attribute Data, Handle: 0x0008, Group End Handle: 0x000b ▾ Attribute Data, Handle: 0x000c, Group End Handle: 0x000f								
9010	86 1b 39 08 80 7f 00 00 5d 82 9a af 06 18 14 00	...	9.....].....					
9020	04 00 11 06 01 00 07 00 00 18 08 00 0b 00 01 18					
9030	0c 00 0f 00 0f 18 8e f5 ee					

Sniffing Process

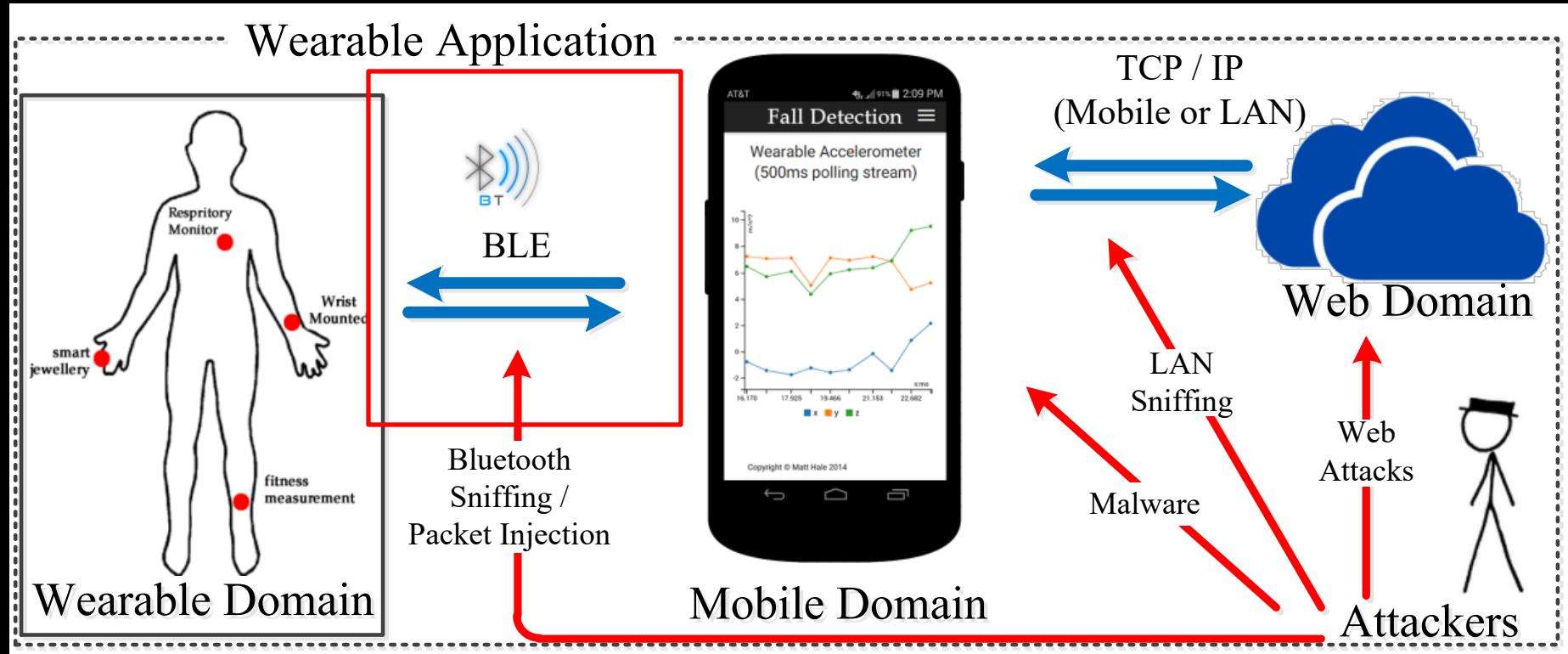
No.	Time	Source	Destination	Protocol	Length	Length	Value	Info
13	7.169893	43:b7:10:a3:46:dc		Bluetooth LE	70	37		ADV_IND
14	7.591865	43:b7:10:a3:46:dc		Bluetooth LE	70	37		ADV_IND
15	8.014875	43:b7:10:a3:46:dc		Bluetooth LE	70	37		ADV_IND
16	8.431830	43:b7:10:a3:46:dc		Bluetooth LE	70	37		ADV_IND
17	8.854841	43:b7:10:a3:46:dc		Bluetooth LE	70	37		ADV_IND
18	9.271834	43:b7:10:a3:46:dc		Bluetooth LE	70	37		ADV_IND
19	9.282481	f4:b6:d9:40:0b:38	43:b7:10:a3:46:dc	Bluetooth LE	67	34		CONNECT_REQ
20	9.291807			Bluetooth LE	42	9		LL Control PDU: LL_FEATURE_REQ
21	9.300744			Bluetooth LE	33	0		Empty Data PDU
22	9.346752			ATT	42	9 0100		Write Request, Handle: 0x000f
23	9.354748			Bluetooth LE	42	9		LL Control PDU: LL_FEATURE_RSP
24	9.399811			Bluetooth LE	33	0		Empty Data PDU
25	9.410453			ATT	38	5		Write Response
26	9.444813			ATT	42	9 0100		Write Request, Handle: 0x001e
27	9.454817			Bluetooth LE	33	0		Empty Data PDU
28	9.489756			Bluetooth LE	33	0		Empty Data PDU
29	9.496725			ATT	38	5		Write Response
30	9.504814			Bluetooth LE	33	0		Empty Data PDU
31	9.511754			Bluetooth LE	33	0		Empty Data PDU
32	9.519737			Bluetooth LE	33	0		Empty Data PDU
33	9.539768			ATT	42	9 0485		Write Command, Handle: 0x001b
34	9.546731			Bluetooth LE	33	0		Empty Data PDU
35	9.554753			Bluetooth LE	33	0		Empty Data PDU
36	9.561701			ATT	48	15 030418fcfcfHandle Value Notification, Handle: 0x001d		
37	9.569749			Bluetooth LE	33	0		Empty Data PDU
38	9.576738			ATT	48	15 030418fcfcfHandle Value Notification, Handle: 0x001d		
39	9.584759			Bluetooth LE	33	0		Empty Data PDU
40	9.591831			ATT	48	15 030418fcfcfHandle Value Notification, Handle: 0x001d		
41	9.599778			Bluetooth LE	33	0		Empty Data PDU
42	9.606738			ATT	48	15 030418fcfcfHandle Value Notification, Handle: 0x001d		
43	9.614756			Bluetooth LE	33	0		Empty Data PDU

A Larger view of a Bluetooth PCAP file

Spectrum Analysis



DEMO





Questions?

Matt Hale, PhD

University of Nebraska at Omaha

Interdisciplinary Informatics

mlhale@unomaha.edu

Twitter: [@mlhale_](https://twitter.com/mlhale_)

