Security and Privacy of Wearable Devices

Juan Loja
Shun-Nam Wilson Chow
Shahbaz Virk

Added a theme, to make it visually more interesting. Feel free to change it to another theme.

What are wearable technology devices?

Low processing power devices that are meant to be worn by users

These are often paired with a “master” device, such as a smartphone

Such devices are used to provide extra information or as a specialized sensor which provides data that a master device may not be able to detect

Examples of wearable devices are

- Heart rate monitors
- Google glass
- Smart watches
- Fitness trackers

Wearable devices are defined by 6 characteristics:

- Not Monopolizing
- Unrestrictive
- Observable
- Controllable
- Attentive
- Communicative

Applications include fitness, healthcare, and entertainment

Wearable devices allow for new ways of monitoring our bodies with the use of small embedded sensors

- As technology gets better and better, computers get smaller and more powerful thus allowing for such devices

Issues and Challenges

When designing wearable devices, important things to consider are power, size, weight, communication throughput and range, as well as security and privacy

These wearable devices are prone to security vulnerability partly because have low processing power

Convenience/ease of use is often the highest priority, security comes after

Security attacks can occur in different ways based on how data is being transferred

Lack of policy

- The fact that such devices are not stand alone (i.e. require to be paired with other devices) makes the transfer of data between the two less safe
    - Creates the man-in-the middle type security threat
    - More vulnerable to brute force attacks
    - Confidentiality issue: easy to get sniffed due to open nature of wireless data transfer
    - Availability issue: we want such devices to be really easy to use to data should be open for view by anyone but unauthorized users will also have the data available
- The main security vulnerabilities that wearable devices often have are:
    - Unauthenticated transmission of data via bluetooth to local storage
    - Retrieving, sending, and communicating data to the Cloud via Wi-Fi or cellular networks
    - Unsafe data storage in the cloud
    - No proper authentication and authorization
    - No physical controls that can be used as a means of authentication (i.e. a keyboard to input a password or a fingerprint reader)

Privacy

Studies have shown that people are concerned about wearable technology exposing personal information captured

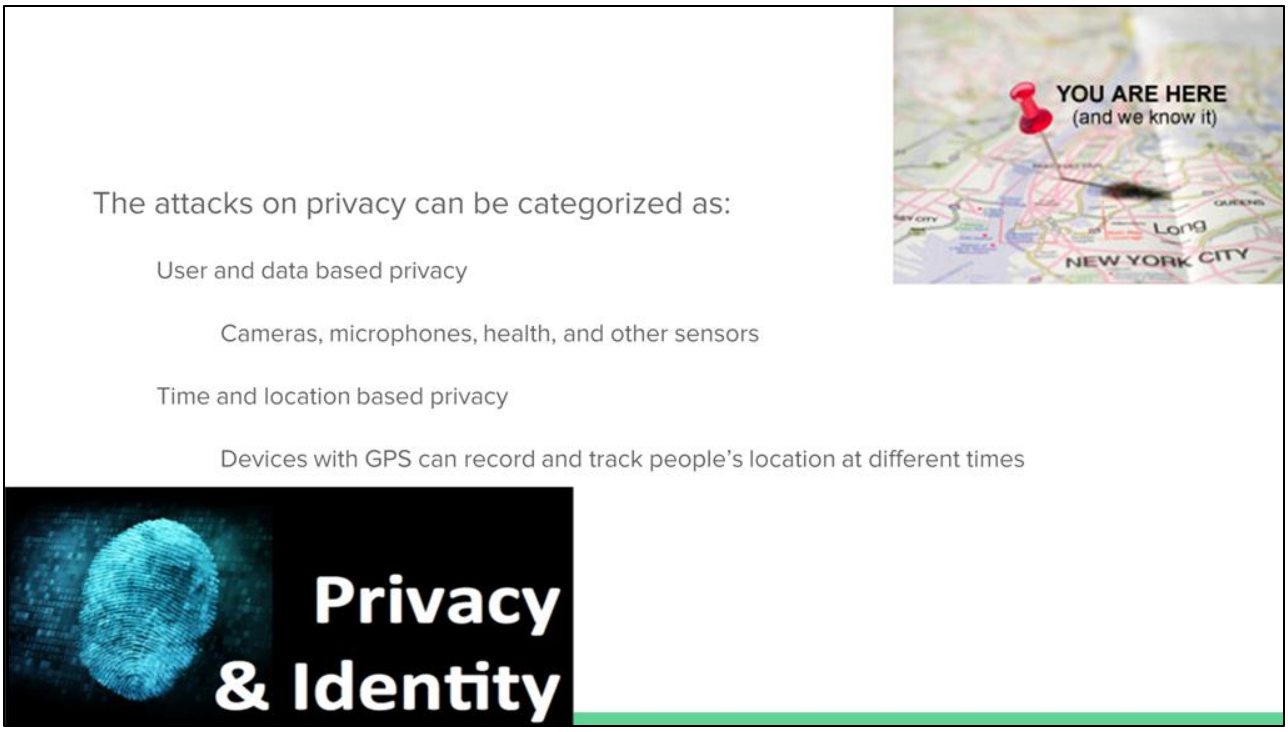
Privacy is a major challenge

- The confidentiality of data can be at risk

Wearable devices today can record many things including location, health status, personal information, and contact information

Why would hackers be interested

- Immediate/relatively quick payoff (wearable wallet/contactless payment)
- Personal health information is about 10 times more valuable than a stolen credit card number on the black market
- Social engineering by using information sniffed
- One vulnerability exploit could be all it needs for hacker to compromise the database
- Wearable device as a mean to connect to the network/database that holds personal information



Wikileaks: samsung tv (furniture, non-wearable) are spying on consumer → Wearable devices...mass surveillance?

Wireless Health

Wireless sensor: diagnosis, therapy, monitoring condition

- via biometric readings, relevant biomarkers, managing treatment regimen

Precise and accurate value reading is required

A way to tamper those values, causing fatal mistreatments (or lack of)

Health Insurance Portability and Accountability Act's (HIPAA) Privacy Rule

- Data won't be seen by entities outside of user's health-care network

Rare to find consumer wearable that deployed FIPS 140-2 encryption in the product

Bluetooth Vulnerabilities

- Certain bluetooth wearable devices often require a pin as an authentication method when pairing to other devices
- However such pin usually consists of a small amount of digits (6 digits sometimes) which is not hard to crack
- This would allow a hacker to easily have access to the information stored and obtained from the wearable device
    - Such information can even be location, time, social media information
- Researchers from Bitdefender showed that once the simple password for the bluetooth device was cracked, information can be easily retrieved

HP Fortify research on IoT

Research from HP Fortify revealed 100% of smartwatches tested contained significant vulnerabilities

Lack of 2 factor authentication of mobile

Unlimited amounts of retries, no locking out

30% vulnerable to account harvesting

40% cloud connections vulnerable to Man-in-the-middle POODLE (Padding Oracle on Downgraded Legacy Encryption) attack

70% concerns with protection of firmware updates, transmitting firmware updates without encryption

All smartwatches collected some form of personal information

Current measures for security in Wearable Devices

- Ban use of Bluetooth or Pairing apps (Not well received)
- Education
- Use NFC
- Applications supporting encryption
- WYOD policies along with BYOD

Policies and Regulations

- Legislation imposes obligations only on data controllers, not processors
  - Definition of processing is vague
  - Information that cannot be used to identify
  - General Data Protection Regulation in May 2018
  - GDPR: Minor changes to definition. Imposes stricter laws on processors

Policies and Regulations (cont.)

- Accommodations for employees not using wearable tech or apps
  - Myrna Arias against Intermex Wire Transfer on Xora app
  - Employees required to download and keep tracking apps on phone
  - Location data viewable even when outside of work hours
  - Removing app results in job termination

Future of Wearable Devices

Cisco predicts more than 600 million wearable devices in use by 2020

Demand in field services

Human Condition Safety testing factories, construction sites

Increasing productivity in oil and gas manufacturing, decreasing accidents

Rio Tino using SmartCap(measures brain activity) to measure truck driver's fatigue

Battery life, screen size, wifi range

Question 1

What are wearable device? What are its characteristics?

Low processing power devices worn by users that is:

Not Monopolizing, unrestrictive, observable, controllable, attentive, and communicative

Question 2

What are the main security issues associated with wearable devices?

Authentication of user and safe data transfer and storage

Question 3

Wearable devices mainly focus on information in storage and information in transmission, how can we deal with security threats that are present?

Education, use NFC, applications supporting encryption and WYOD policies along with BYOD

Reference

https://motherboard.vice.com/en_us/article/this-ai-wearable-helps-make-you-less-socially-awkward

http://investor.cisco.com/investor-relations/news-and-events/news/news-details/2016/10th-Annual-Cisco-Visual-Networking-Index-VNI-Mobile-Forecast-Projects-70-Percent-of-Global-Population-Will-Be-Mobile-Users-With-15-Connections-per-Capita-by-2020/default.aspx

http://www.wearabletechnology-news.com/news/2014/dec/15/bitdefender-proves-bluetooth-wearables-vulnerability/

http://aircconline.com/ijnsa/V8N3/8316ijnsa02.pdf

https://www.forbes.com/sites/adrianagardella/2015/06/05/employer-sued-for-gps-tracking-salesperson-247/#795f4d2e23e3

https://www.ft.com/content/d0bfea5c-f820-11e5-96db-fc683b5e52db

https://threatpost.com/wearable-warning-ieee-highlights-top-security-risks-for-fitness-trackers/116291/

http://www8.hp.com/us/en/hp-news/press-release.html?id=2037386

http://www.cnbc.com/2015/12/12/price-of-wearable-craze-your-health-data-hacked.html

http://www.welivesecurity.com/2016/01/12/fitbit-hacking-mean-wearables-iot/

https://www.wareable.com/wearable-tech/wearable-security-8865