SECURITY & PRIVACY
CHALLENGES IN MOBILE
HEALTH (MHEALTH) SYSTEMS

David Kotz
Professor of Computer Science

Institute for Security, Technology, and Society
Dartmouth College

January 2015
mHealth

The use of mobile computing and communications technology in the delivery of healthcare or collection of health information.
mHealth - in the clinic
Inpatient monitoring
Remote patient monitoring
Personal wellness applications

Fitbit Force

Fitbit Classic
mHealth in the developing world
mHealth platforms: Smart phones

- NFC
- Camera
- GPS
- Gyroscope
- Accelerometer
- Magnetometer
- Radio Receivers
- Proximity
- Light
- Touch
- Microphone
mHealth devices are emerging

smart phones

Stella wearable sensors

Samsung Gear

Corventis wearable medical sensors

Philips emotion sensor

Fitbit Force
Shared sensors, environmental sensors

Withings wireless body scale

Caliber III
(temperature and humidity)

Wireless Heart Rate Monitor
(ProForm AccuRate)

Blood Pressure Monitor
(Omron M10)
mHealth – what’s different?

• Security
  • Immediate, personal impact
    • mHealth devices directly affect your health, or health decisions

• Privacy
  • Sensitivity of data:
    • mHealth data is inherently personal, literally about you
  • Volume of data:
    • mHealth collects far more medical data, over extended periods
  • Diversity of data:
    • mHealth collects a broader range of information, including lifestyle, activities, and context
  • Uses of data:
    • mHealth enables a broad range of apps, outside the doctor-patient relationship
survey paper:
- privacy framework
- security properties
- threat taxonomy
- research challenges

TRUSTWORTHY HEALTH AND WELLNESS (THAW)

thaw.org

seeking new students and postdocs...