RSA Conference 2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: ECO-W01

The promise and the perils of wearables

Andrés Molina-Markham
Principal Research Scientist
RSA Labs / RSA, The Security Division of EMC
Andres.Molina-Markham@rsa.com

Shrirang Mare
PhD Candidate
Dartmouth College
shrirang@cs.dartmouth.edu

Intel Mica

Misfit shine

Apple watch

DESIGN

There's an Apple Watch for everyone.

Selecting a watch is very personal. As with all things you wear, how it looks is at least as important as what it does. So we set out

Google Glass

Fitbit flex

Android wear

Nod Ring

The promise and the perils of wearables

New opportunities

- Novel user interfaces
- Novel data collection uses
- More personal
- More available

Big challenges

- Power efficiency
- Diverse HW/SW
- Security

Overview of the talk

New opportunities

- BRACE: Bilateral recurring authentication conducted effortlessly

An example of a novel use of wearables in security applications

Big challenges

- Amulet: Secure computational jewelry for wearable mHealth applications

An architecture that addresses the challenges of implementing a secure low-power wearable device

RSA Conference 2015
San Francisco | April 20-24 | Moscone Center

BRACE

Shrirang Mare, *Dartmouth*

Andrés Molina-Markham, *RSA Labs*

Cory Cornelius, *Intel Labs*

Ronald Peterson, *Dartmouth*

David Kotz, *Dartmouth*

#RSAC

Motivation: Clinical workstations

- Unattended logged-in computers
- Security risk
- Compliance issues

The De-authentication Problem

- Users forget to logout
- They intentionally do not logout

http://millerhealthlaw.com/company

Existing solutions

- Timeouts are too long, or too quick
- Human proximity detector
  - Styrofoam cup story

Our solution

What interactions a user performs

- Monitor wrist movement with wristband
- Correlate wrist movement and input to computer

Bilateral authentication

Device

Observer #1

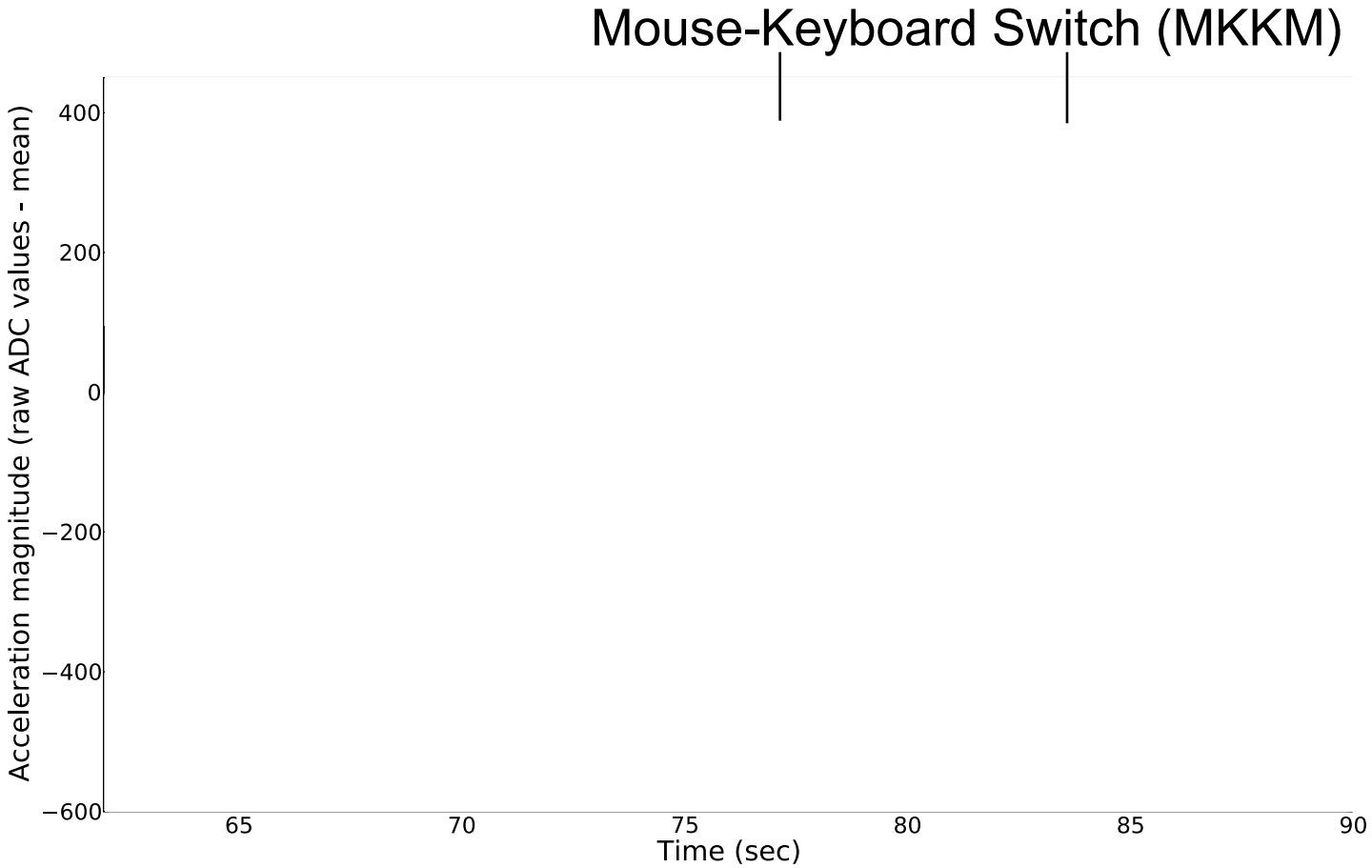
Observed Event

User-Computer Interactions

Observer #2

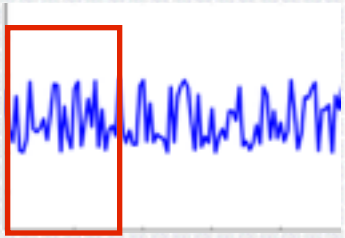
Sensors on wrist

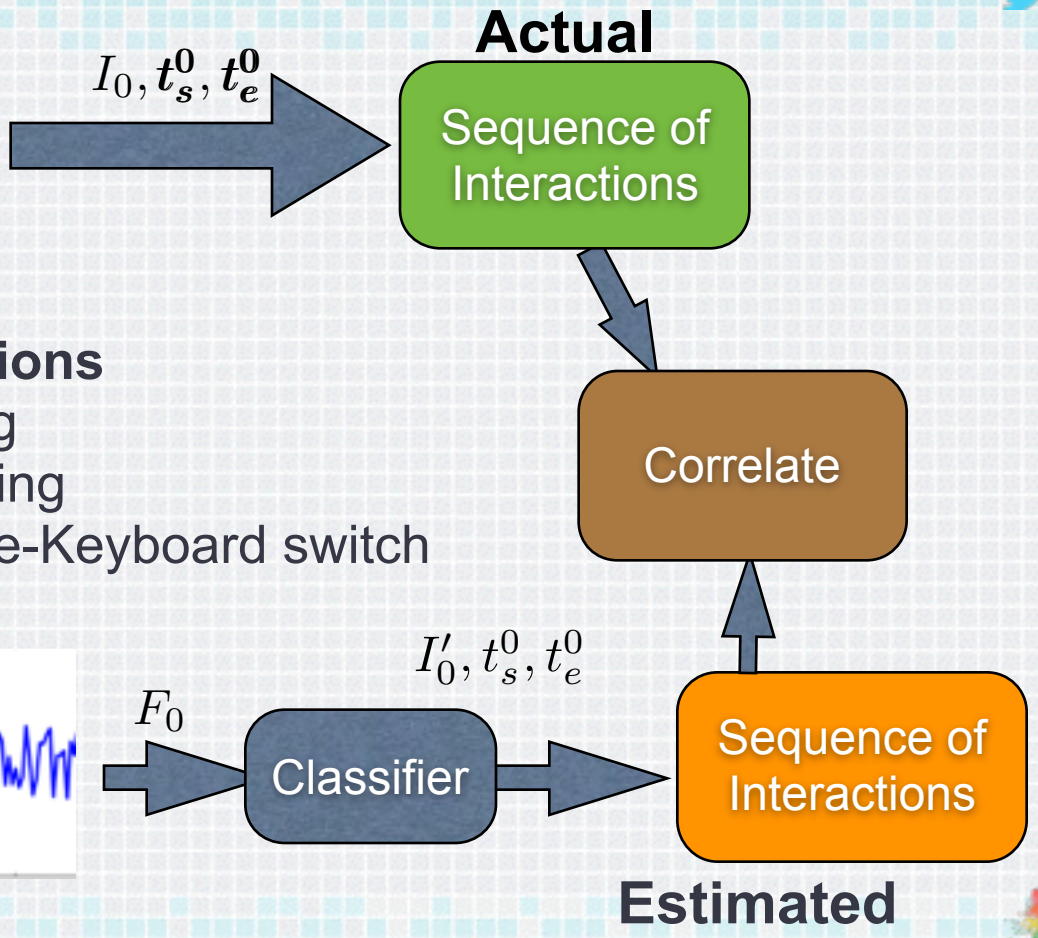
Authenticate by correlating their observations



Wrist movement during computer interaction

Interactions
1. Typing
2. Scrolling
3. Mouse-Keyboard switch





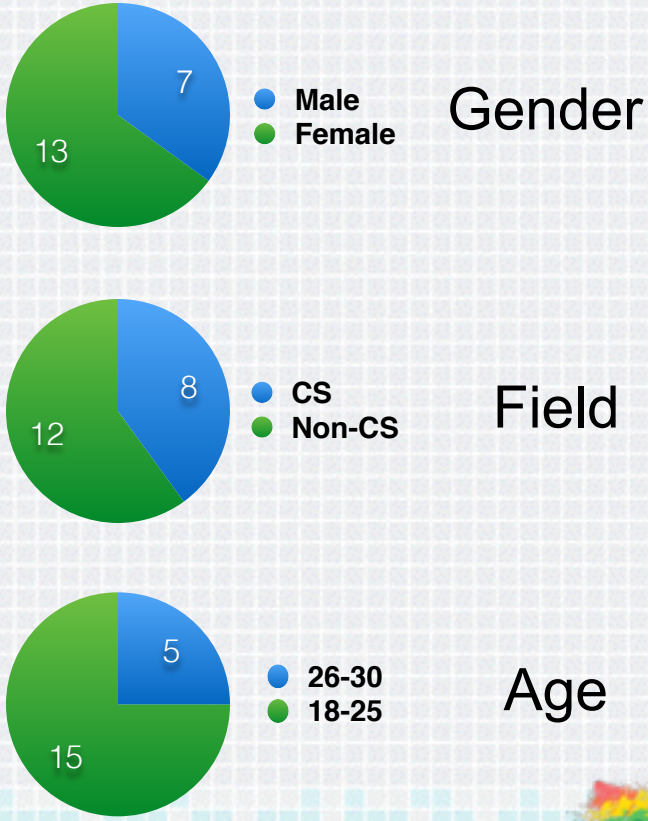
Evaluation

User study

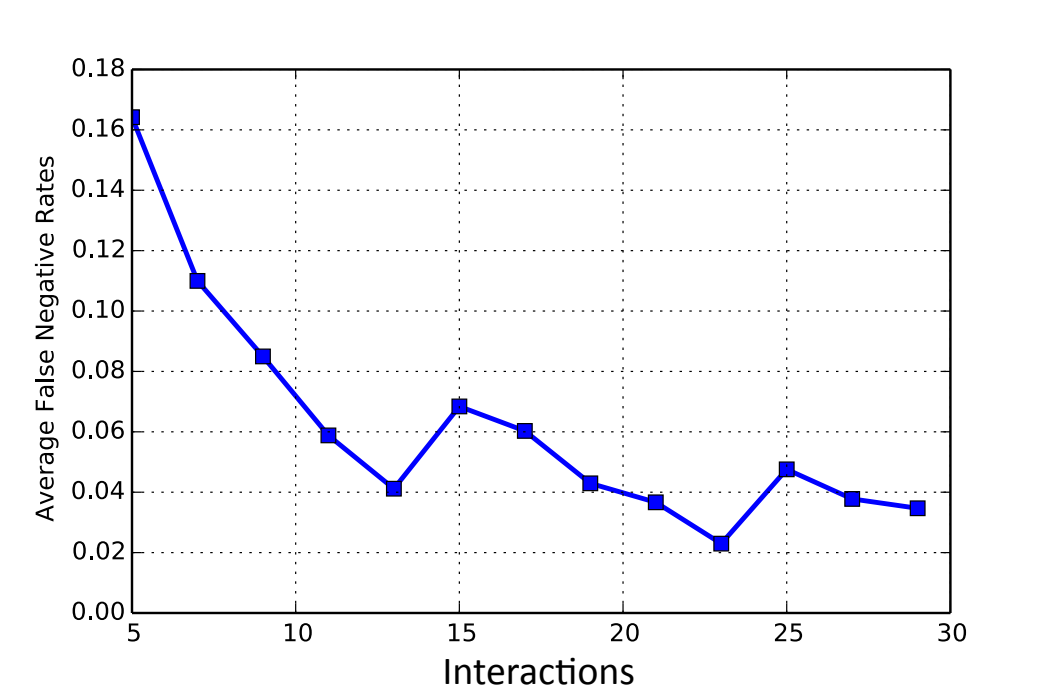
- 20 subjects
- 30-40 mins study session

Tasks during study:

- Fill out web survey
- Browse internet
- Mimic another user

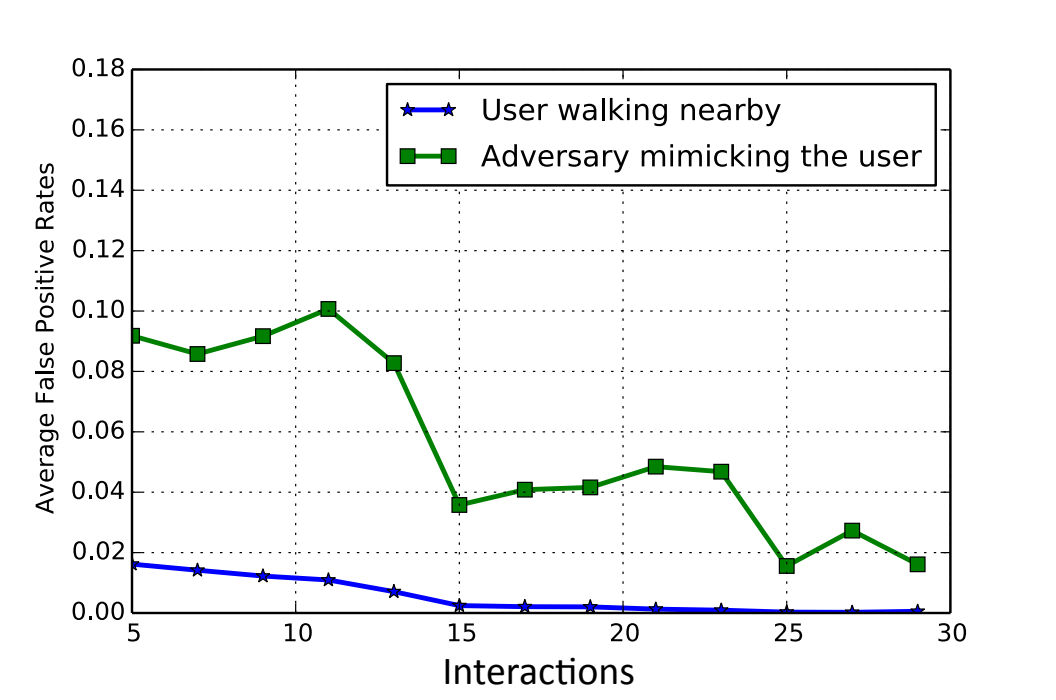


Usability



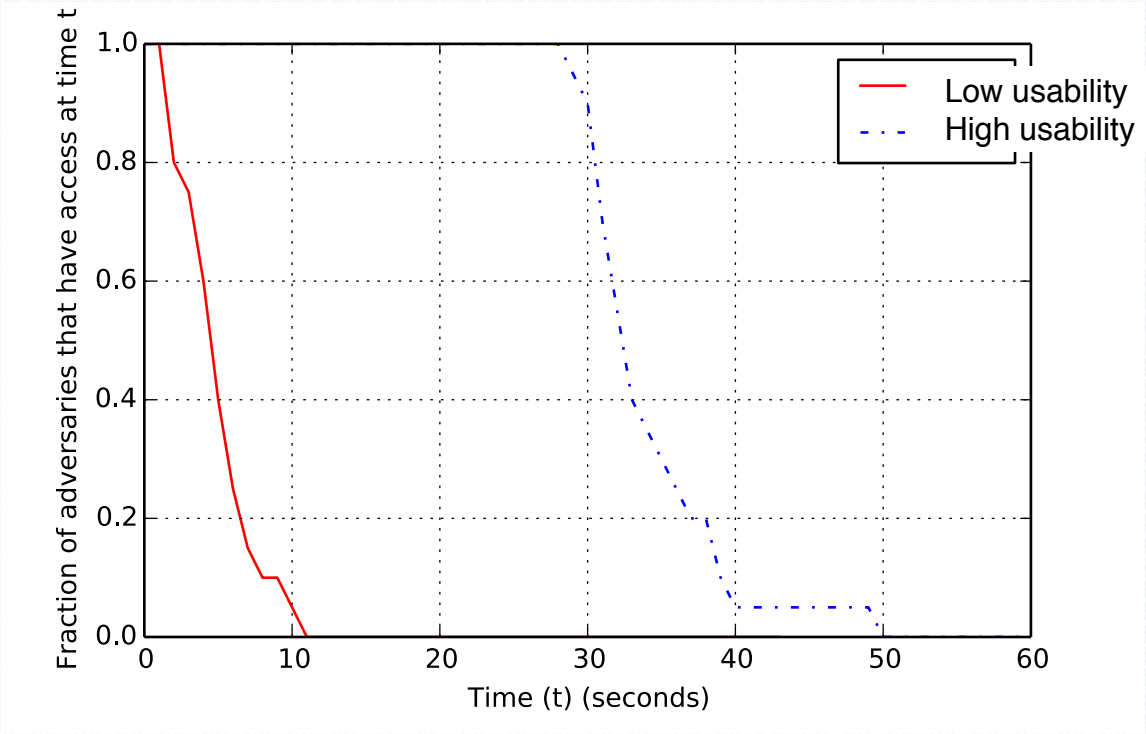
Average False Negative Rate vs. Number of interactions

Security



Average False Positive Rate vs. Number of interactions

Security



Identified adversary in 11 seconds

Fraction of **adversaries** that have access at time *t*

BRACE Summary

- Bilateral authentication approach
- BRACE for continuous authentication
- Evaluated feasibility with a user study
  - High-usability setting: 90% accuracy; 50 sec to identify adversary
  - Low-usability setting: 85% accuracy; 11 sec to identify adversary

RSA Conference2015
San Francisco | April 20-24 | Moscone Center

Amulet: Secure computational jewelry for wearable mHealth applications

amulet-project.org

Wearable mHealth

EEG (Emotiv)

Image:www.athena-gatech.org

Footpod (Suunto)

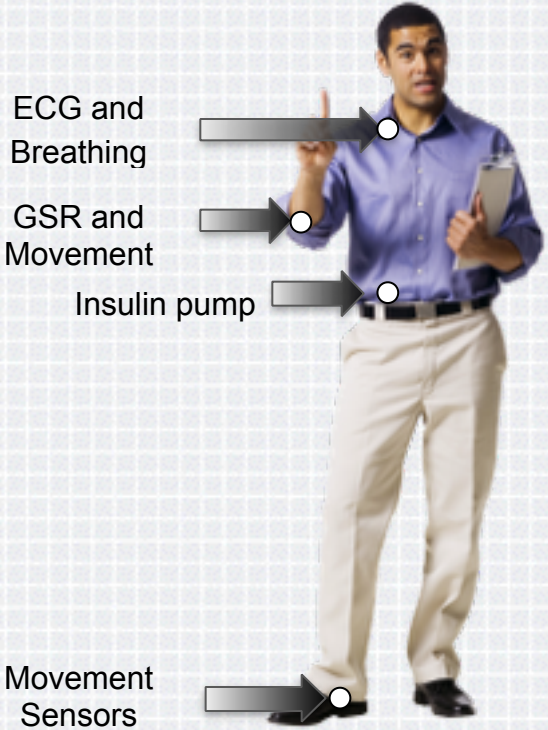
Respiratory management platform (Puffminder)

Sleep and activity monitor (Shine)

Hearing aid (gizmo diva)

Heart rate monitor (teamwildathletics.com)

Today's wearable data flow



Body
Area
Network

External
Weight
Sensor

Mobile phone provides a hub for monitoring body-area devices

image: winarticles.net

Problem:

Smartphones break

or get lost …

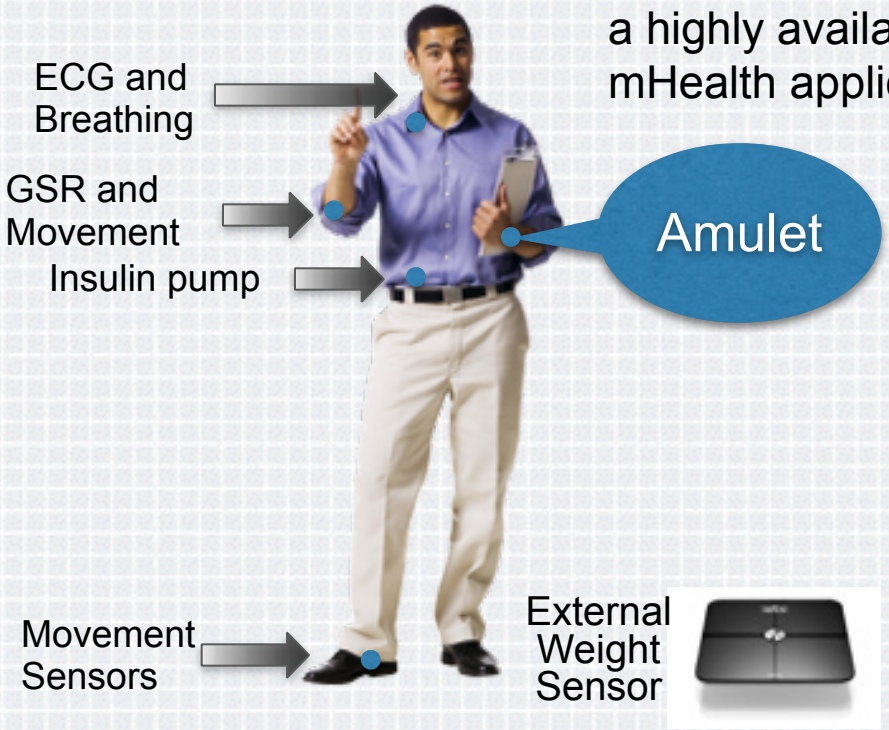
image: thetimes.co.uk

image: techgc.net

or are simply
left behind

One alternative: Amulet for mHealth

A wearable device that provides a highly available runtime for mHealth applications



Wearable platform requirements

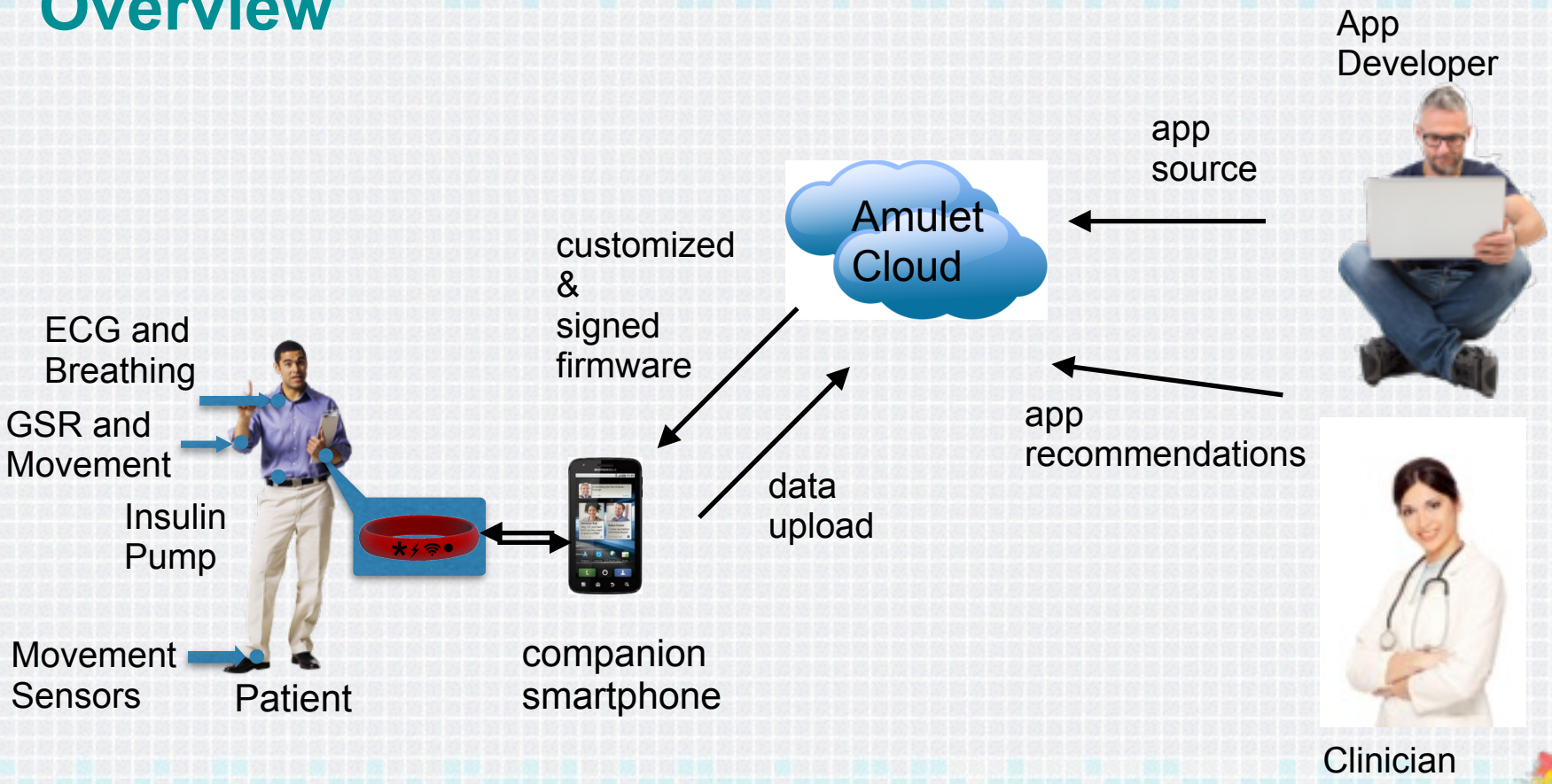
- **Secure** application runtime
- **Independent** from the smartphone and more present
- **Small** enough to wear
- **Efficient** enough to last for a day or longer
- **Extensible** because it supports the easy addition of devices and applications
- **Open** for others to use and improve

Amulet challenges

- Security-focused architecture
- Power-efficient hardware & software
- Programming model for third-party apps

[Netflix]

Overview

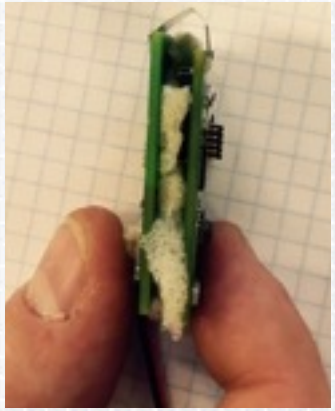

App Developer
app source
Amulet Cloud
customized & signed firmware
ECG and Breathing
GSR and Movement
Insulin Pump
Movement Sensors
Patient
companion smartphone
data upload
app recommendations
Clinician

Security

- Apps **sandboxed** at compile-time
  - Safe subset of C sandboxes each app
  - Amulet installs only trusted firmware images
- Apps **limited to authorized resources**
  - Every app request is checked against policy
- App **actions logged** for later auditing
  - Secure audit trail in persistent memory

Inside the amulet

- Two-board design
  - “Radio board” manages communications
  - “App board” runs apps and UI
- App board is off when idle
  - Radio board boots it only when needed
  - Must be quick to boot and reload apps
  - Apps must survive such reboots
- Apps: finite-state machines w/memory
  - Set of states, variables, and event handlers
  - All state is explicit, in non-volatile storage
  - No threads: handlers run to completion



Feasibility applications

- Fall detector
  - Accelerometer
- Emergency Response
  - Buttons
- Drowsiness detector
  - External heart-rate monitor (Mio)
- Bite counter
  - IMU sensor

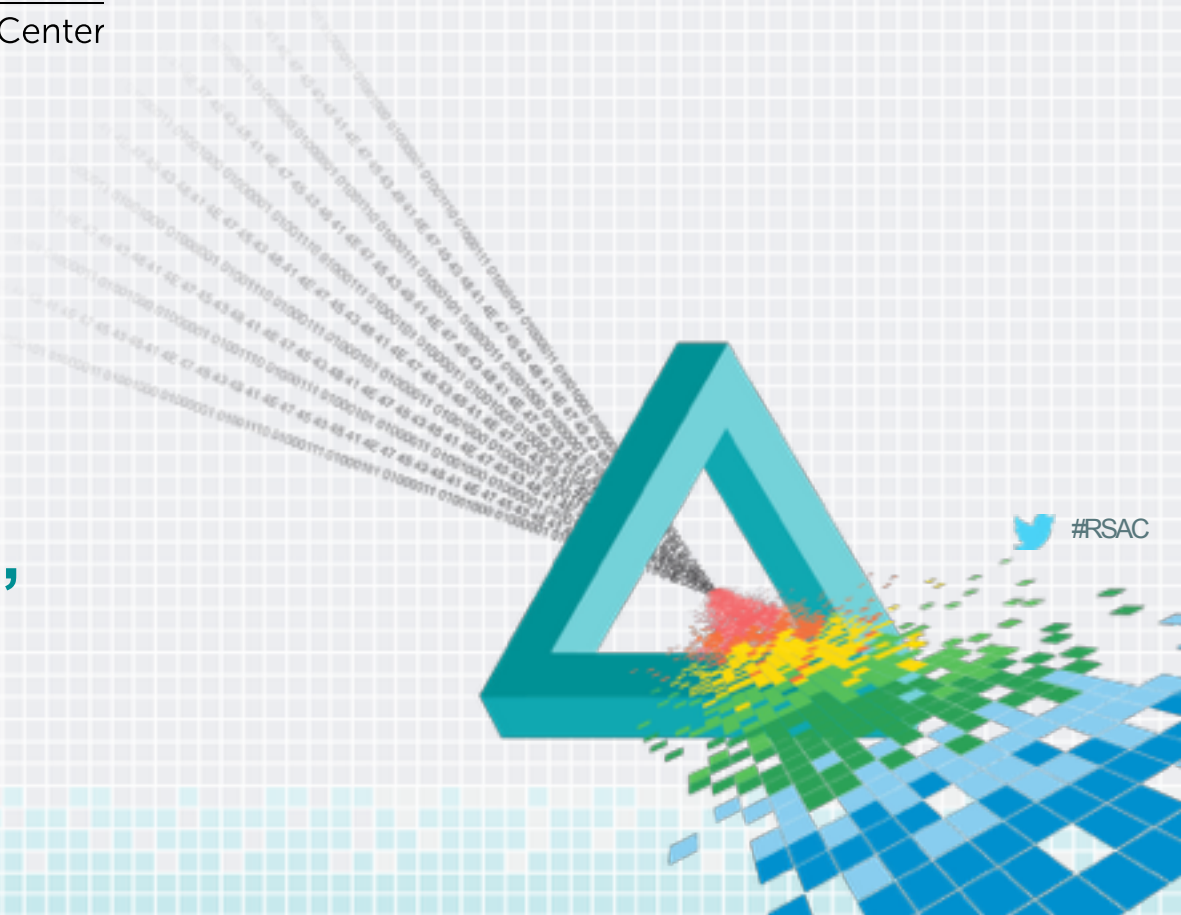
- Battery lifetime 3.5–4.3 days
  - Can improve with optimization

Amulet summary

An Amulet for mHealth networks

- **Highly available**: wearable, compact device
- **Efficient**: dual-board event-driven architecture
- **Customizable**: third-party apps written in C
- **Secure**: app isolation, managed resources, audit log, trusted firmware, encrypted communications

More info: amulet-project.org



Take away “Apply”

Apply

1. Think of how wearables may open opportunities for you
   - Novel use cases in security?
   - Novel private user interfaces?
   - New data streams for security mechanisms?

2. Think about the new challenges to security
   - Wearables are not tiny smartphones
   - Integration with other devices and services

Apply

1. Does your novel use case with a wearable need:
   - Data?
   - Control?
   - Or more complex applications running on wearables?

2. Will wearables in your application be single purpose?
   - Or will they have multiple purposes with software from multiple vendors? (e.g., running on Android Wear)
   - Will data be primarily streamed in “data silos” or will your application interact with data from other applications?

Acknowledgements

andres.molina-markham@rsa.com, shrirang@cs.dartmouth.edu

joint work with

Kelly Caine, Eric Chen, Kevin Freeman, Bhargav Golla, Emily Greene, Ryan Halter, David Kotz, Xiaohui Liang, Sarah Lord, Vivian Motti, Travis Peters, Gunnar Pope, Ronald Peterson, Joseph Skinner, Jacob Sorber, and Tianlong Yun

amulet-project.org

Supported by the National Science Foundation award numbers CNS-1314281, CNS-1314342, and TC-0910842, by the Department of Health and Human Services (SHARP program) under award number 90TR0003-01.
The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsors.

RSA Conference 2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: ECO-W01

The promise and the perils of wearables

Andrés Molina-Markham
Principal Research Scientist
RSA Labs / RSA, The Security Division of EMC
Andres.Molina-Markham@rsa.com

Shrirang Mare
PhD Candidate
Dartmouth College
shrirang@cs.dartmouth.edu