Security and Privacy of Wearable Computing

David Wagner

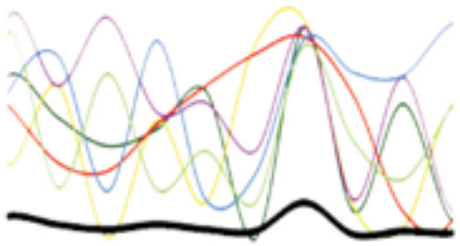
technology


7129


XBOX 360
KINECT


8:20
Monday, September 21
slide to unlock

Processing
Graphical User Interface



Gait Classification

Python
Machine Learning Algorithm

Digital Data

Xbee
Wireless Transmission Device

Digital Data

Arduino Microcontroller
Computation Core of Shoes

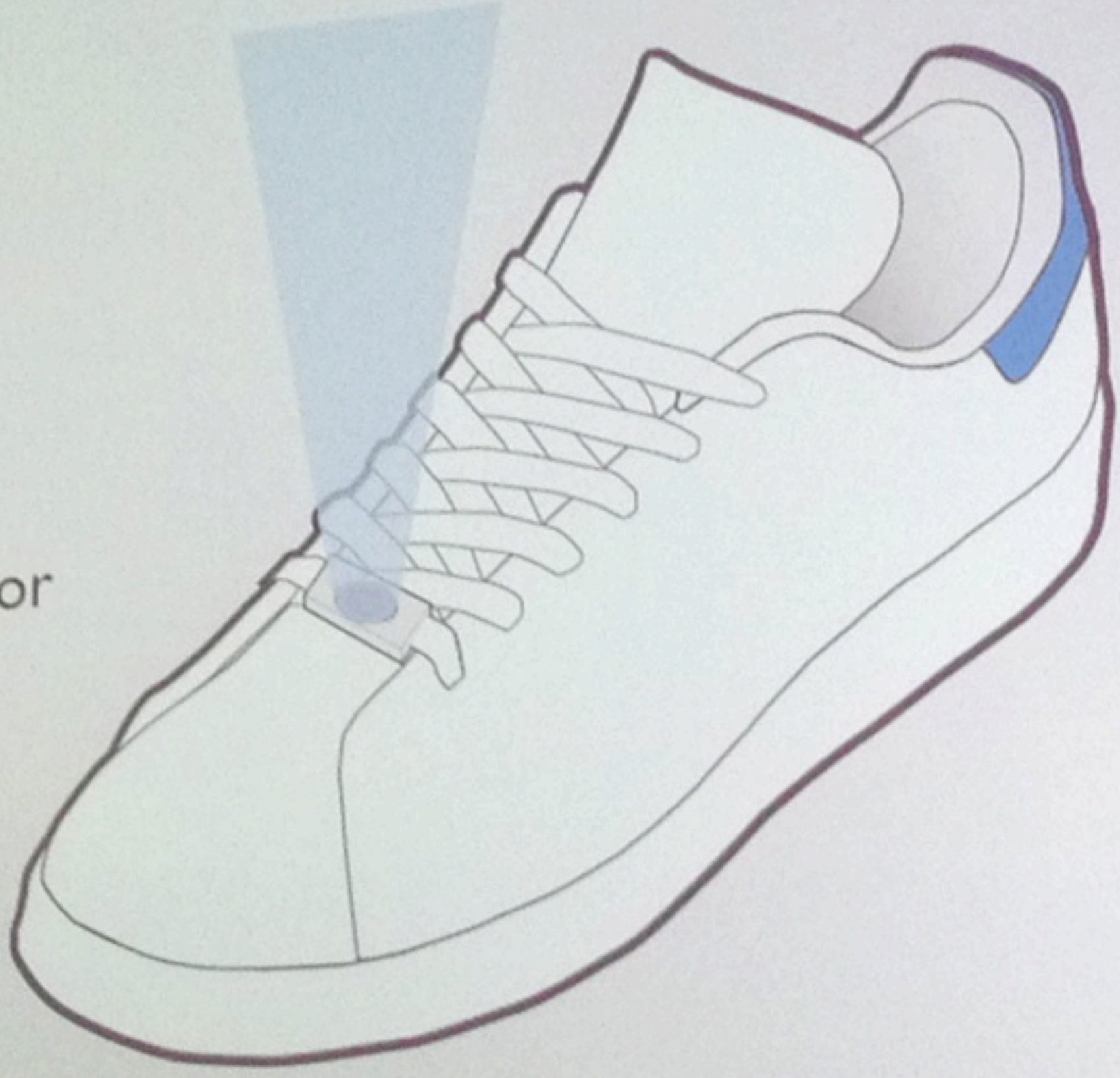
Analog Data

Force-Sensing Resistor
Meature The Pressure of Shoes.

Conclusion

ShoeSense

- Wearable system
- Shoe-mounted sensor



continuous computer vision

continuous speech recognition

real-time, unobtrusive interaction with humans

applications

augmented reality

augmented reality

augmented reality

augmented reality

personal assistant

augmented reality

personal assistant

collaborative sensing

augmented reality

personal assistant

health and monitoring

collaborative sensing

augmented reality

personal assistant

health and monitoring

sports and exercise

collaborative sensing

augmented reality

personal assistant

health and monitoring

real-time advice

sports and exercise

collaborative sensing

papers

A Scanner Darkly: Protecting User Privacy From Perceptual Applications

Suman Jana* Arvind Narayanan† Vitaly Shmatikov*
*The University of Texas at Austin
†Princeton University

***ract*—Perceptual, "context-aware" applications that ob-heir environment and interact with users via cameras her sensors are becoming ubiquitous on personal com- mobile phones, gaming platforms, household robots, gmented-reality devices. This raises new privacy risks. describe the design and implementation of DARKLY, a al privacy protection system for the increasingly com-enario where an untrusted, third-party perceptual ap-n is running on a trusted device. DARKLY is integrated penCV, a popular computer vision library used by such tions to access visual inputs. It deploys multiple privacy ion mechanisms, including access control, algorithmic transforms, and user audit.**

valuate DARKLY on 20 perceptual applications that per-iverse tasks such as image recognition, object tracking, surveillance, and face detection. These applications DARKLY unmodified or with very few modifications inimal performance overheads vs. native OpenCV. In ases, privacy enforcement does not reduce the appli-' functionality or accuracy. For the rest, we quantify deoff between privacy and utility and demonstrate that

programmable robots, even moving around—raises int ing privacy issues for their users. Many people are al uncomfortable with law enforcement agencies condu large-scale face recognition [2, 17]. Perceptual applic running in one's home or a public area may co unauthorized surveillance, intentionally or unintenti overcollect information (e.g., keep track of other p present in a room), and capture sensitive data such as card numbers, license plates, contents of computer mo etc. that accidentally end up in their field of vision.

General-purpose, data-agnostic privacy technologies as access control and privacy-preserving statistical an are fairly blunt tools. Instead, we develop a *domain-sp* solution, informed by the structure of perceptual applic and the computations they perform on their inputs, an pable of applying protection at the right level of abstra

Our system, DARKLY, is a privacy protection lay

A Scanner Darkly: Protecting User Privacy From Perceptual Applications

Suman Jana* Arvind Narayanan† Vitaly Shmatikov*

Enabling Fine-Grained Permissions for Augmented Reality Applications With Recognizers

Suman Jana[1], David Molnar[2], Alexander Moshchuk[2], Alan Dunn[1], Benjamin Livshi
Helen J. Wang[2], and Eyal Ofek[2]

[1]University of Texas at Austin
[2]Microsoft Research

Abstract

Augmented reality (AR) applications sense the environment, then render virtual objects on human senses. Examples include smartphone applications that annotate storefronts with reviews and XBox Kinect games that show "avatars" mimicking human

1 Introduction

An *augmented reality* (AR) application take
ural user interactions (such as gestures, voic
eye gaze) as input and overlays digital cont
top of the real world seen, heard, and exper
by the user. For example, on mobile phones
mented reality "browsers" such as Layar and
allow users to look through the phone and s
notations about a magazine article or a stor

A Scanner Darkly: Protecting User Privacy From Perceptual Applications

Suman Jana* Arvind Narayanan† Vitaly Shmatikov*

Enabling Fine-Grained Permissions for Augmented Reality Applications With Recognizers

Suman Jana[1], David Molnar[2], Alexander Moshchuk[2], Alan Dunn[1], Benjamin Livshi
Helen J. Wang[2], and Eyal Ofek[2]

Operating System Support for Augmented Reality Applications

Loris D'Antoni[1], Alan Dunn[2], Suman Jana[2], Tadayoshi Kohno[3], Benjamin Livshits[4], David Molnar[4], Alexander Moshchuk[4], Eyal Ofek[4], Franziska Roesner[3], Scott Saponas[4], Margus Veanes[4], Helen J. Wang[4]

[1]University of Pennsylvania [2]University of Texas at Austin
[3]University of Washington [4]Microsoft Research

Abstract

Augmented reality (AR) takes natural user input (...) tures, voice, and eye gaze) as input and overlays digital content on top of the real world. For example, on mobile phones, augmented reality "browsers" such

discussion

discussion

what technical problems should the research community be focusing on?

privacy for bystanders

privacy for wearer

wearables in the corporate enterprise

what will attackers' motives and methods?

open discussion