

Continuous and Active Authentication for Mobile Devices Using Multiple Sensors

**Cyber Security Division
2012 Principal Investigators' Meeting
TTA: Usable Security**

Oct 11 2012

**PI. Weidong Shi PhD (larryshi@cs.uh.edu)
(678)429-7787
University of Houston**

Introduction

What is it about?

- Part of TTA 3
- Type II

Seamless user authentication solution to balance authentication strength and usability

- Protecting personal and confidential data stored on mobile computing devices
- Enforcing proper access control
- Providing a user friendly solution

Team

- One PI
- Two full-time research scientists
- Two PhD graduate research assistants

Market analysis and prediction

	2011 (M units)	2015 (M units)
Tablets	75	640
Smartphones	627	1500
Laptops	647	966
	1.35E+03	3.11E+03

•Worldwide smartphone markets: 2011 to 2015 - analysis, data, insight and forecasts.

http://www.researchandmarkets.com/research/7a1189/worldwide_smartpho

•Kathryn Huberty, Mark Lipacis, Adam Holt, Ehud Gelblum, Scott Devitt, Benjamin Swinburne, Francois Meunier, Keon Han, Frank A.Y. Wang, Jasmine Lu, Grace Chen, Bill Lu, Masahiro Ono, Mia Nagasaka, Kazuo Yoshikawa, and Mathew Schneider. Tablet demand and disruption: Mobile users come of age, 2011.

Usability and security

Avoid same pw for different sites

No "remember me"

No automatically sign in on boot-up

Use password with strong entropy

Change password frequently

Interaction speed

Instant access

Touch based interface

Small screen

No keyboard

Usability often wins in this battle for mobile devices (reason of economics)

Smudge attack



Applied fingerprint powder

One-shot user authentication

One-shot
user authentication



No control after login



Next login session



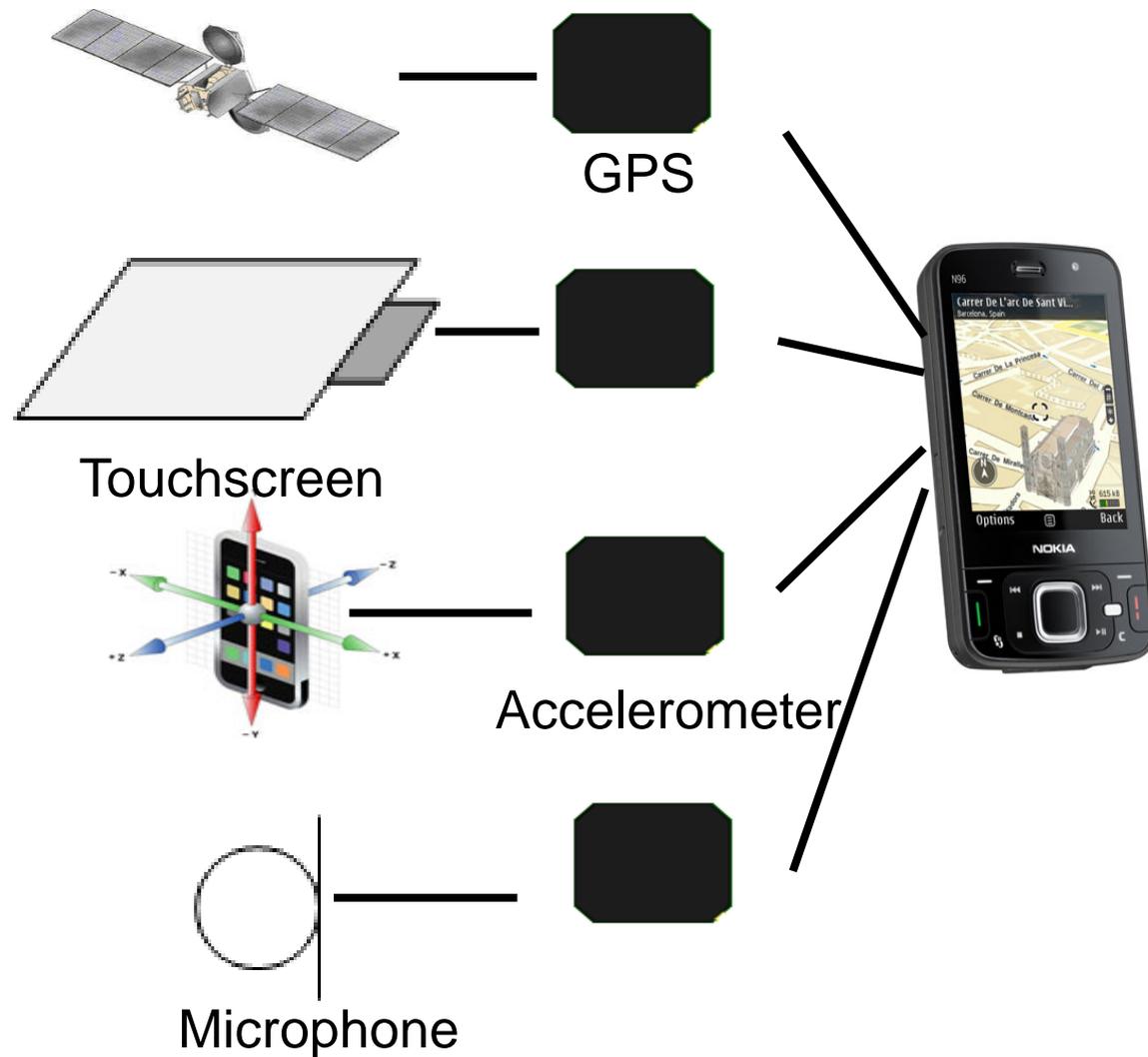
Assume the same user after an one-shot user authentication event and before the next login event.



Implicit and continuous user authentication

- Authenticate user in the background
- Invoke explicit authentication only when very likely user has changed
- Continuous
- User transparent
- Leverage multiple sensors already available on commercial mobile devices

Smartphone has many sensors



Sensor Based User Authentication

- Cell ID/GPS history
- Touchscreen
- Voices
- Accelerometer
- Camera

Touch authentication and protection



**Enhance Shape Drawing
Access with User
Specific Touch Features**

**Touch Gesture Based
Authentication**

**Virtual Typing Dynamics
Based Authentication**

**Shape Drawing Login
Manager**

**Multi-touch Gesture
Engine**

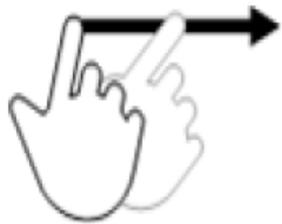
Virtual Keyboard

Multi-touch Driver



Touchscreen

Multi-touch



Flick



Pinch



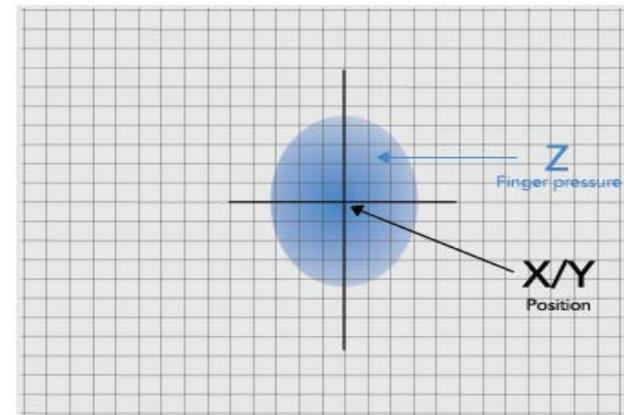
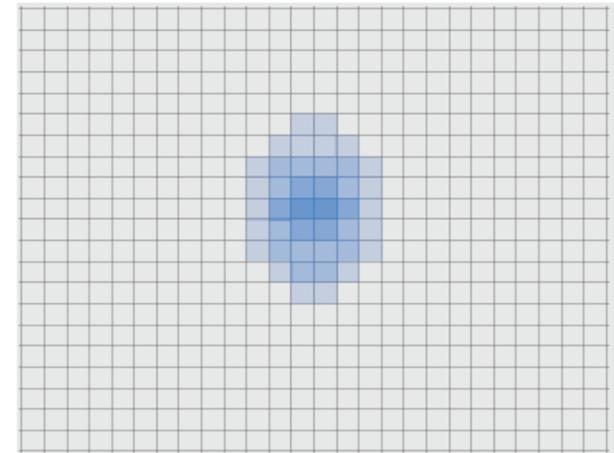
Spread



Drag



Rotate



- Multi-touch gestures
- Touch based drawing credential
- Virtual typing

Metrics

Security

A low FAR and a high FRR is more secure but not user friendly

Usability

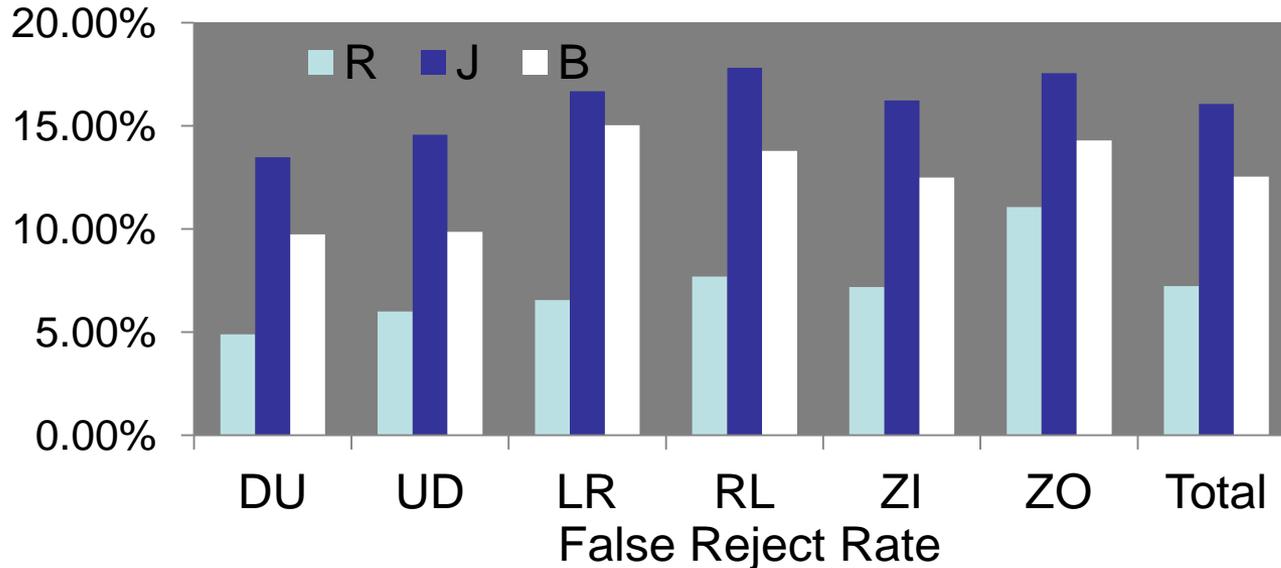
Low FRR and a high FAR is more user friendly but less secure

- The **False Accept Rate** (FAR) is the percentage of authentication decisions that allow access to an unauthorized user.
- The **False Reject Rate** (FRR) is the percentage of authentication decisions where an authorized user is denied access.
- **When no verification/control after login, FAR is 100% and FRR is 0%.**

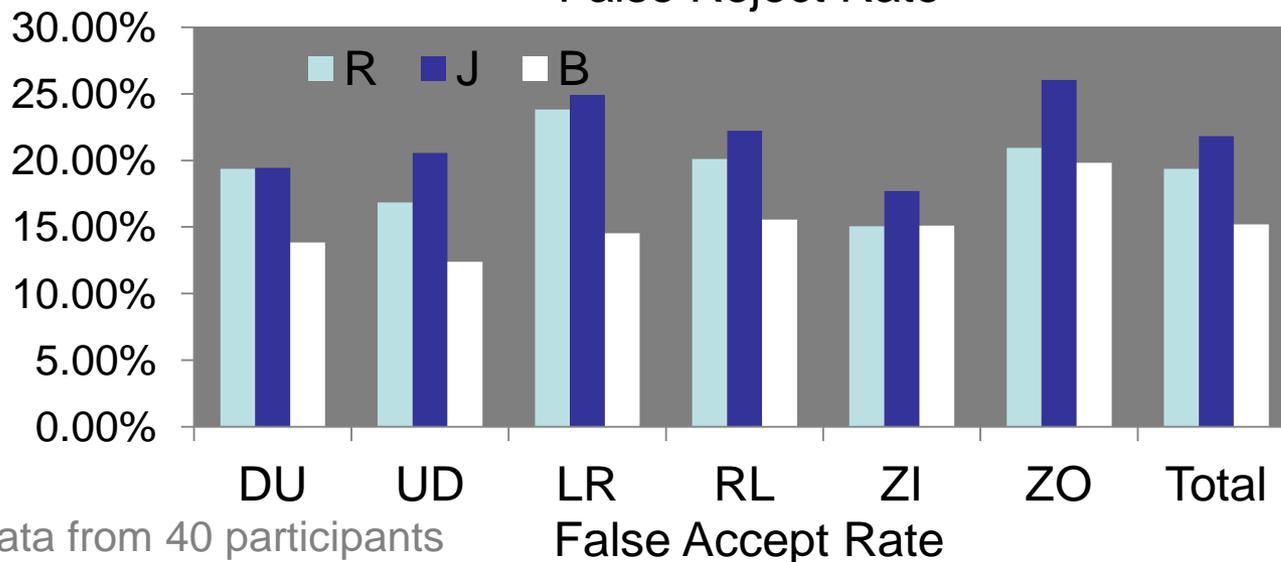
Challenges

	Solution Direction
Security vs. Usability	Balance between FAR and FRR
Poor performance of single modality	Aggregation of multiple sensor modalities
Protection subversion/bypass	Mobile virtualization
Privacy	Template protection, techniques similar to “fuzzy” vault
Power overhead	Opportunistic sensing, capture data during normal mobile device - user interactions

Performance of single touch gesture

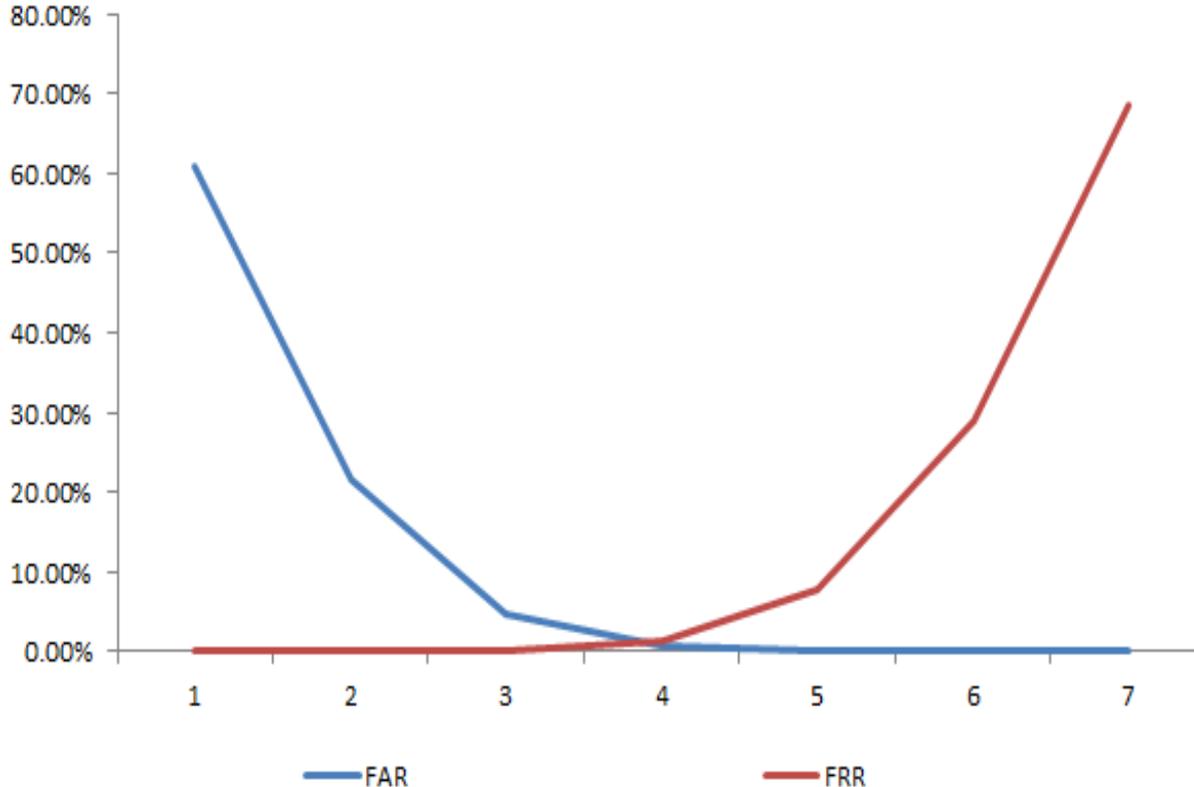


R - Random Forest Classifier
 B - Bayes Net classifier
 J - Decision Tree



swipe from down to up (DU)
 swipe from up to down (UD)
 swipe from left to right (LR)
 swipe from right to left (RL)
 zoom-in (ZI)
 zoom-out (ZO)

Performance of touch aggregation using sliding windows



Threshold = 2

FAR=21.54%

FRR=0.01%

Threshold = 3

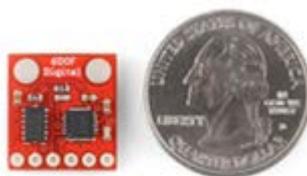
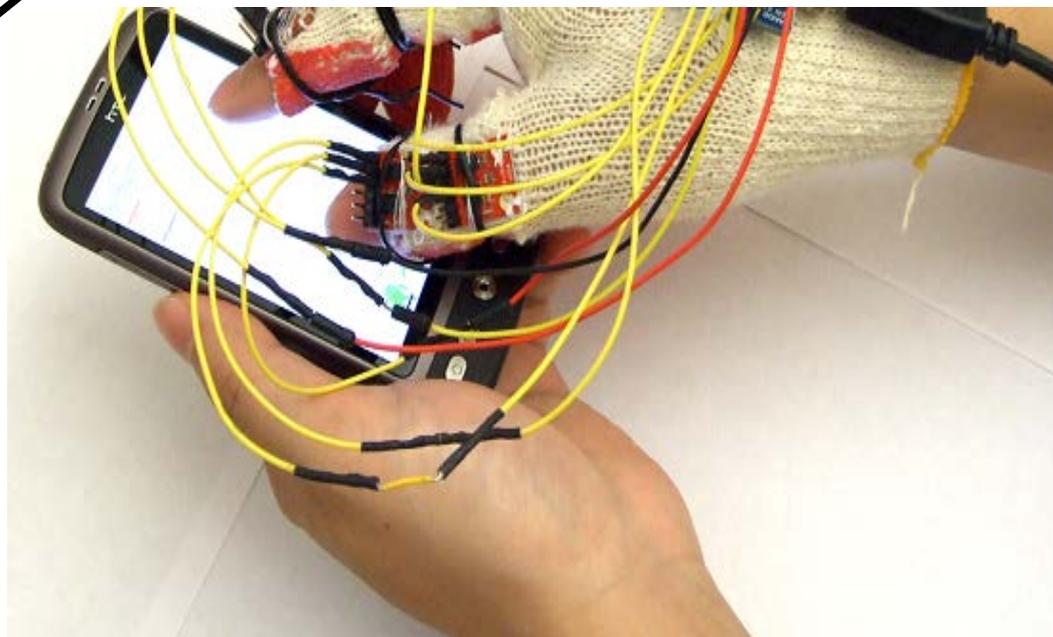
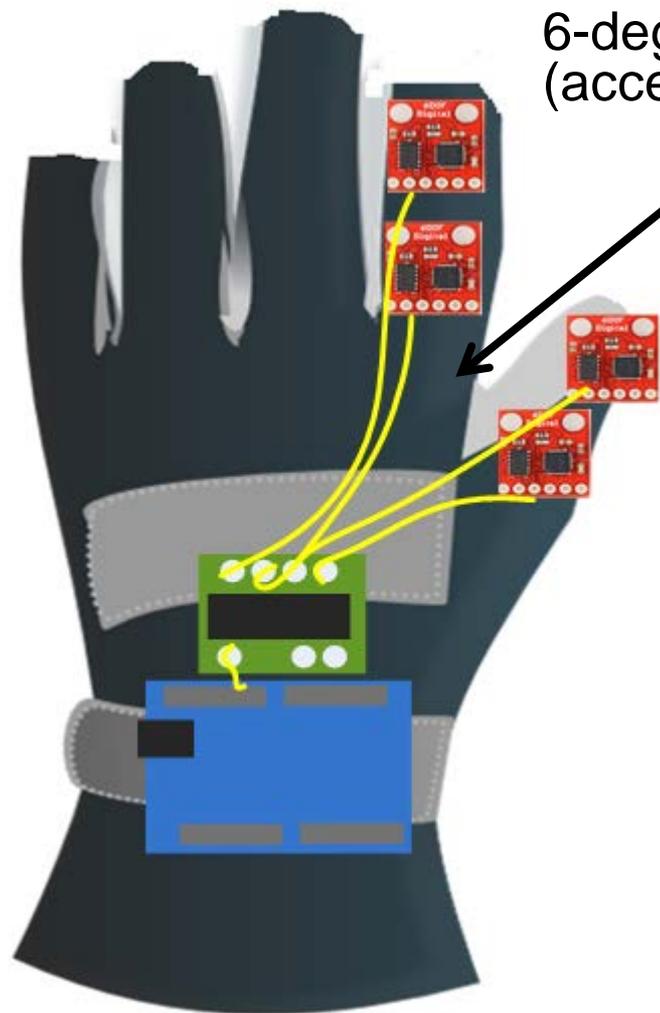
FAR=4.66%

FRR=0.13%

For each group of valid touch gestures (default = 7), test if n (e.g., 3) or more gesture inputs are recognized as inputs from the authorized user.

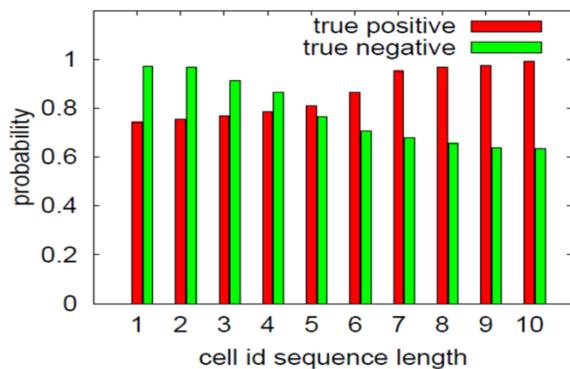
Study with sensing glove

6-degree IMU Sensor Board
(accelerometer and gyro)

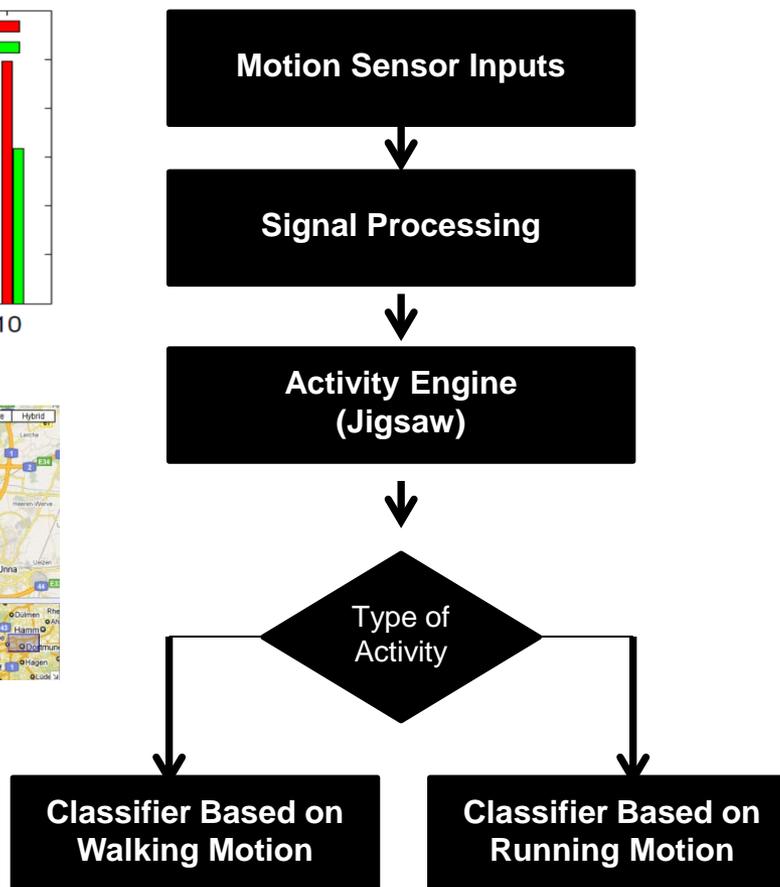


Multiple modalities

Cell ID/GPS locations



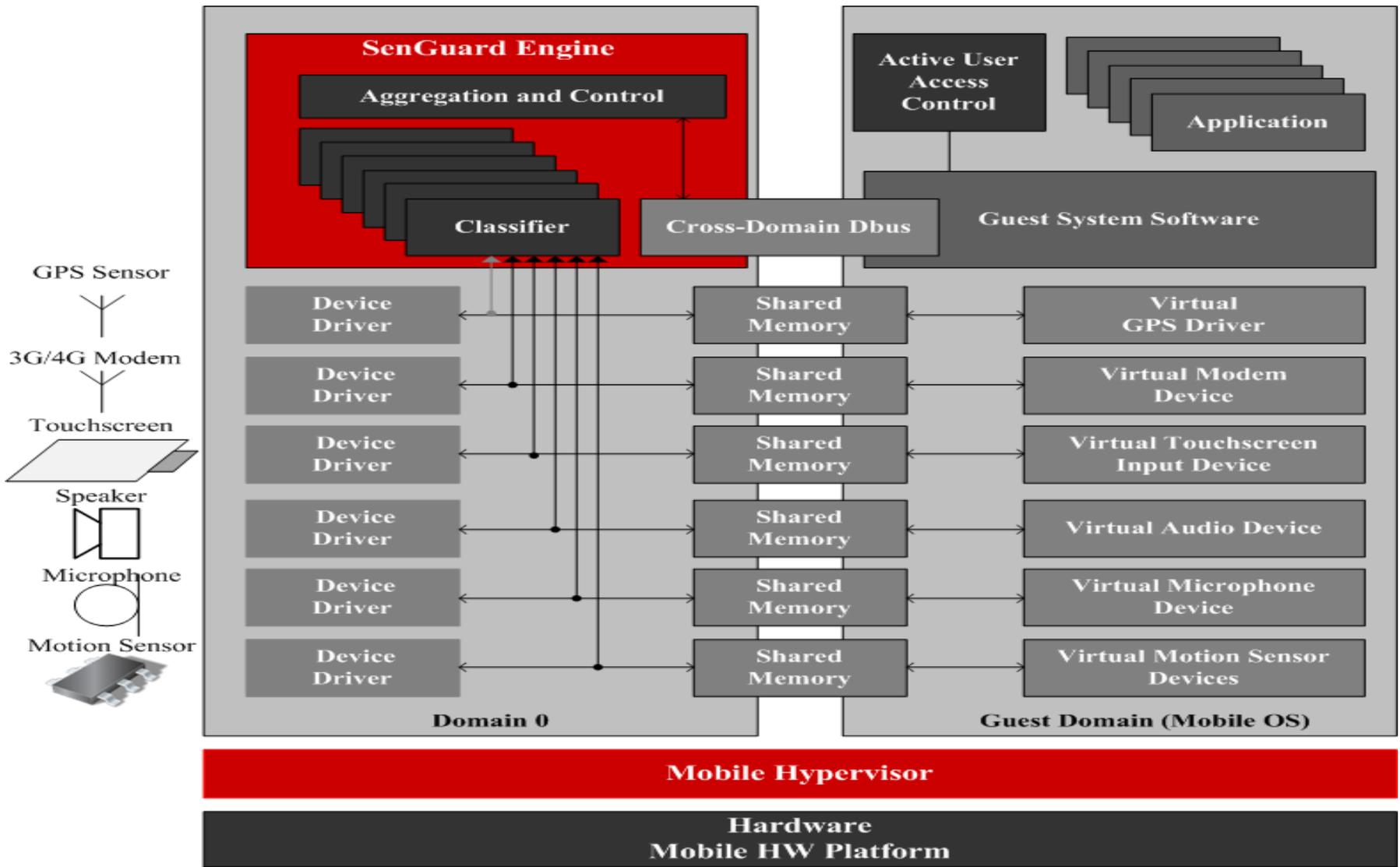
Locomotion



Voices



Port to smartphones with virtualization support



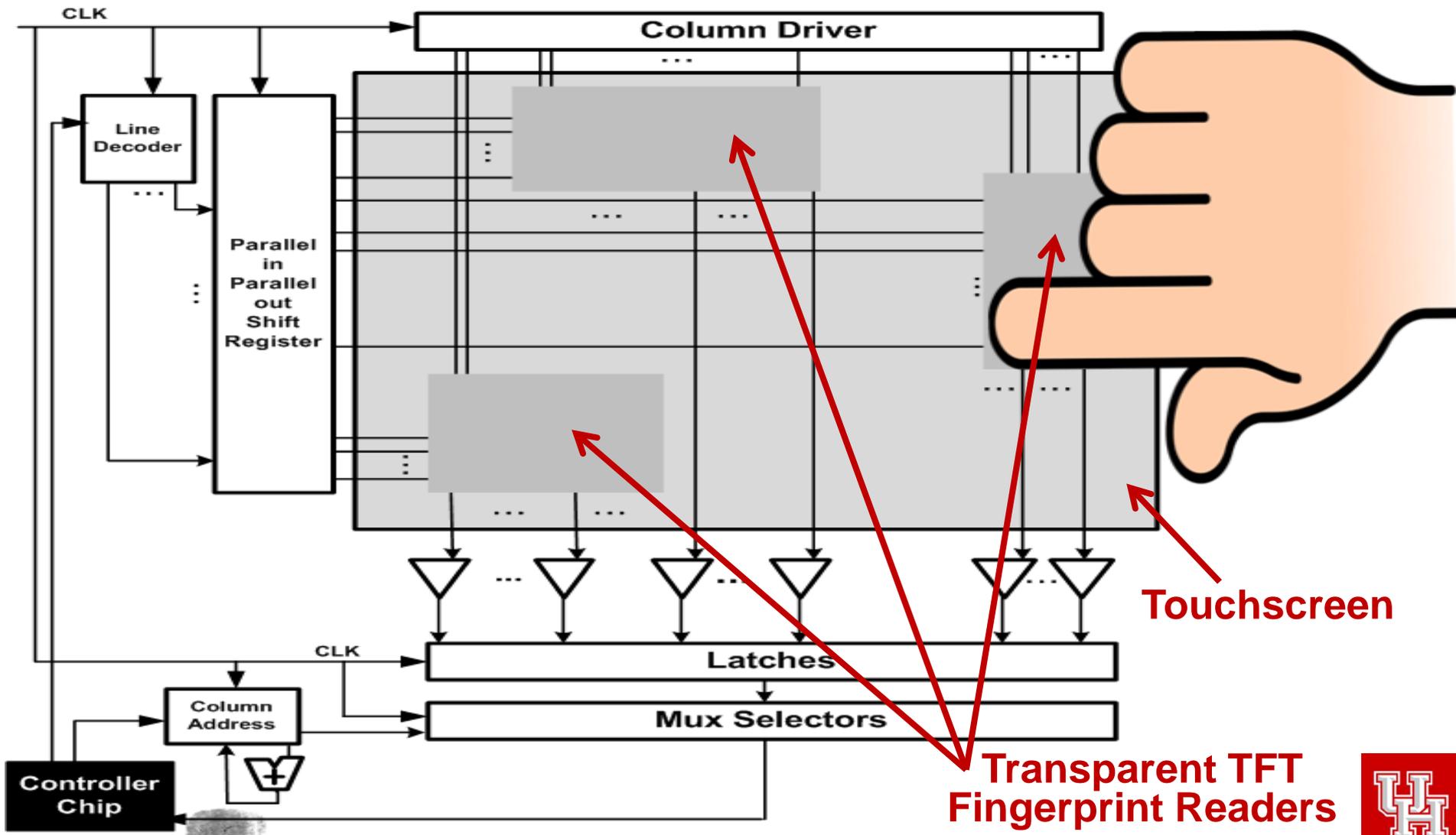


Security HCI Device Research at University of Houston

Biometric integrated touchscreen

	One-shot Access Control	Separate Fingerprint Reader	Unified with Touchscreen
Continuous User Verification	No	No	Yes
User Burden	Memorization, extra step	Extra login step (rub/swipe)	No
Login Speed	Typing, drawing speed	Few seconds	Instant
Transparent to User	No	No	Yes

A new unified approach: integrating biometric with touchscreens



Touchscreen

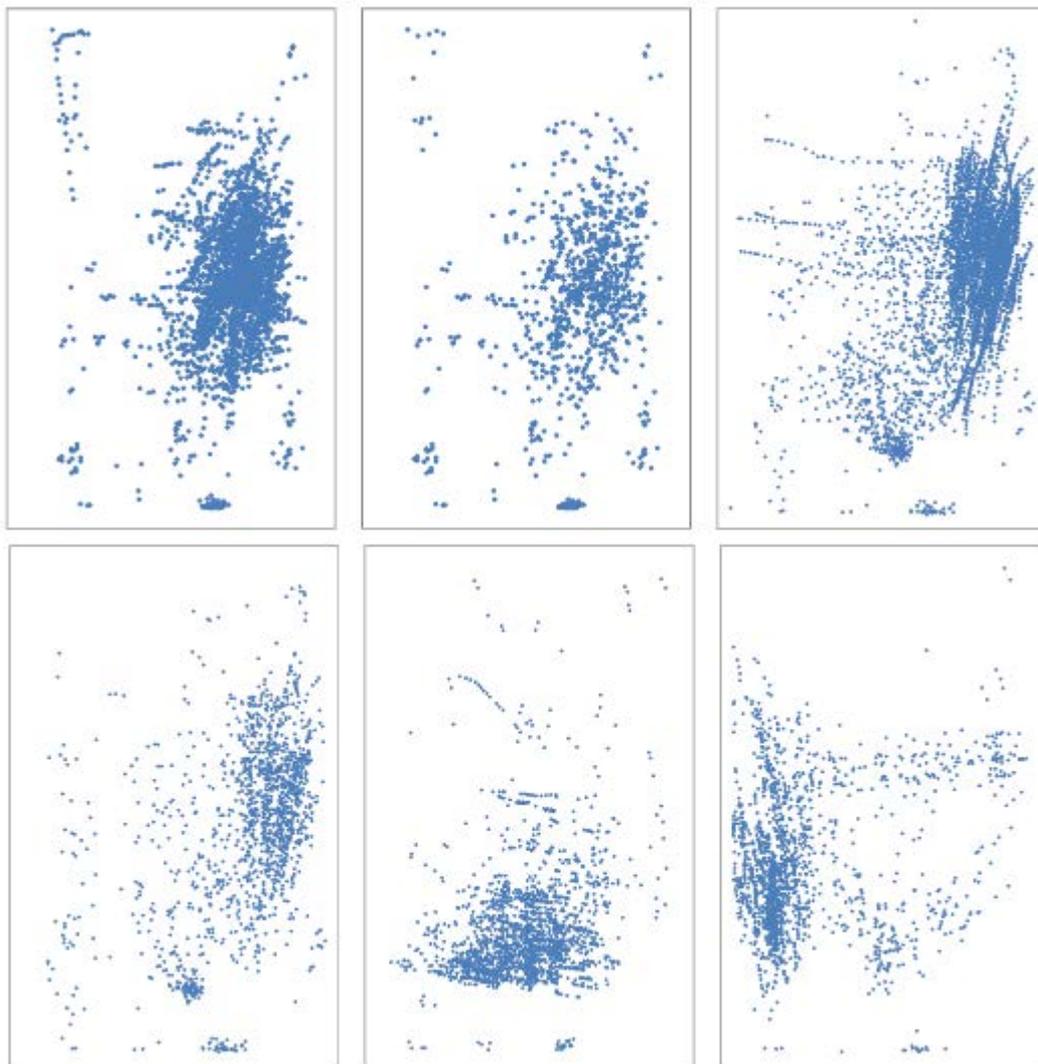
Transparent TFT
Fingerprint Readers



Challenges

Speed	Must be done < 7 – 10 ms
Transparent	Must use transparent TFT electronics
Cost	Cost prohibitive to make the entire screen a reader
Privacy	Avoid storing raw fingerprints
Power overhead	Must be energy efficient
Performance	Incomplete data, low quality data (e.g., fingers move too fast, light touch)

Distributions of touches



- **Observational data**
 - 6 participants
- **Insight**
 - no need to cover the entire screen

Sensor areas and touch point coverage

Area Percentage	HTC 110mm*60mm	HTC 85mm*55mm
15%	25.18%	18.29%
20%	35.92%	33.52%
25%	45.62%	39.12%

Performance

Area Percentage	Average # of Touches Needed to Detect Unauthorized Users	FAR in 10 Touches	FRR in 10 Touches
15%	3.67	0.01%	3%
20%	2.46	0.01%	0.13%
25%	2.18	0.01%	0.12%

- Sensing time: 7ms
- Take into account of
 - data completion, data quality, directions and angles of touches, touch speed, time interval fingers staying on the touchscreen

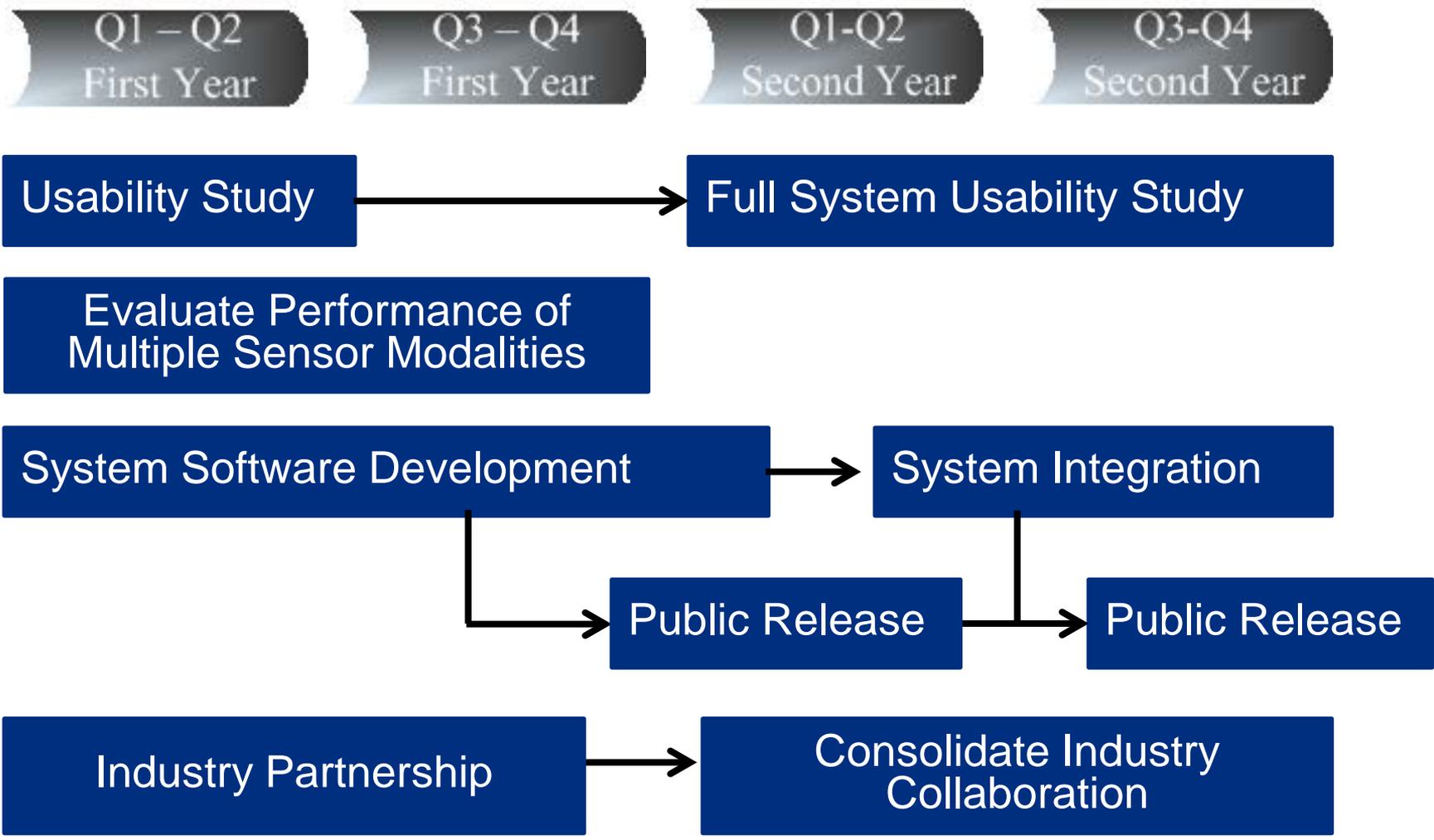
Deliverables

Design Documents	
Design Requirements Specification	Documents
System Architecture Design Specification	Documents
Technical Design Specification	Documents
Quality Assurance Plan	Documents
User Study and Usability Evaluation Plan	Documents
Software and Prototype	
Software	
• Android, iPhone, Windows Phone	Software
Source Code Release	Software
Software Ported to Platform with Mobile Virtualization	Software
Reports and Publications	
Evaluation Report	Report
Usability Study Results/Reports	Report
Publications	Report

Milestones and schedule

Research and Development

Technology Transition

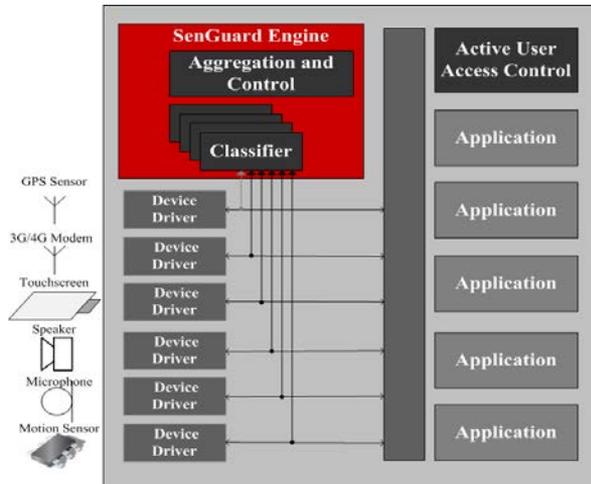


Technology transition plan

- Apps release by the PI and research team
 - Android, iPhone, and Windows Phone
- Open source release (GPL)
- Collaboration with industries

Title: Implicit and Continuous Mobile User Identification/Authentication Using Smartphone Sensors

Project Objective and Approach:



Proposed Technical Approach:

Tasks

- Usability and security evaluation;
- In-depth evaluation of classifier for each mobile sensor; and
- Software development.

Status

- Conducted initial evaluation of four sensors (touchscreen, accelerometer, cellid, mobile voice) for user identification;
- Developed initial SenGuard software;

Ongoing Effort.

- Ongoing user study and in-depth sensor property research; and
- Ongoing software development and system integration.

Operational Capability:

Targets

- Software supporting implicit and continuous mobile user identification/authentication;
- No significant power and performance overhead; and
- Can be accepted by mobile users and applied as real mobile security policy.

Cost of Ownership

- Low

BAA Relevance

- Mobile security is one of the most important security concerns at the age of smartphones and tablets;
- Few people use access control on mobile handheld devices; and
- Proper balance between security and usability more difficult to attain for mobile handheld devices;

Schedule, Deliverables, & Contact Info:

Milestone:

- Year 1: usability study; system software development.
- Year 2: system software development; and system integration.

Deliverables:

- Software integrated with Android, iOS, and Windows Phone
- User study results/reports
- Virtualization based prototype

Corporate Information:

- Weidong Shi (Larry),
- Department of Computer Science,
- University of Houston, Email: larryshi@cs.uh.edu



