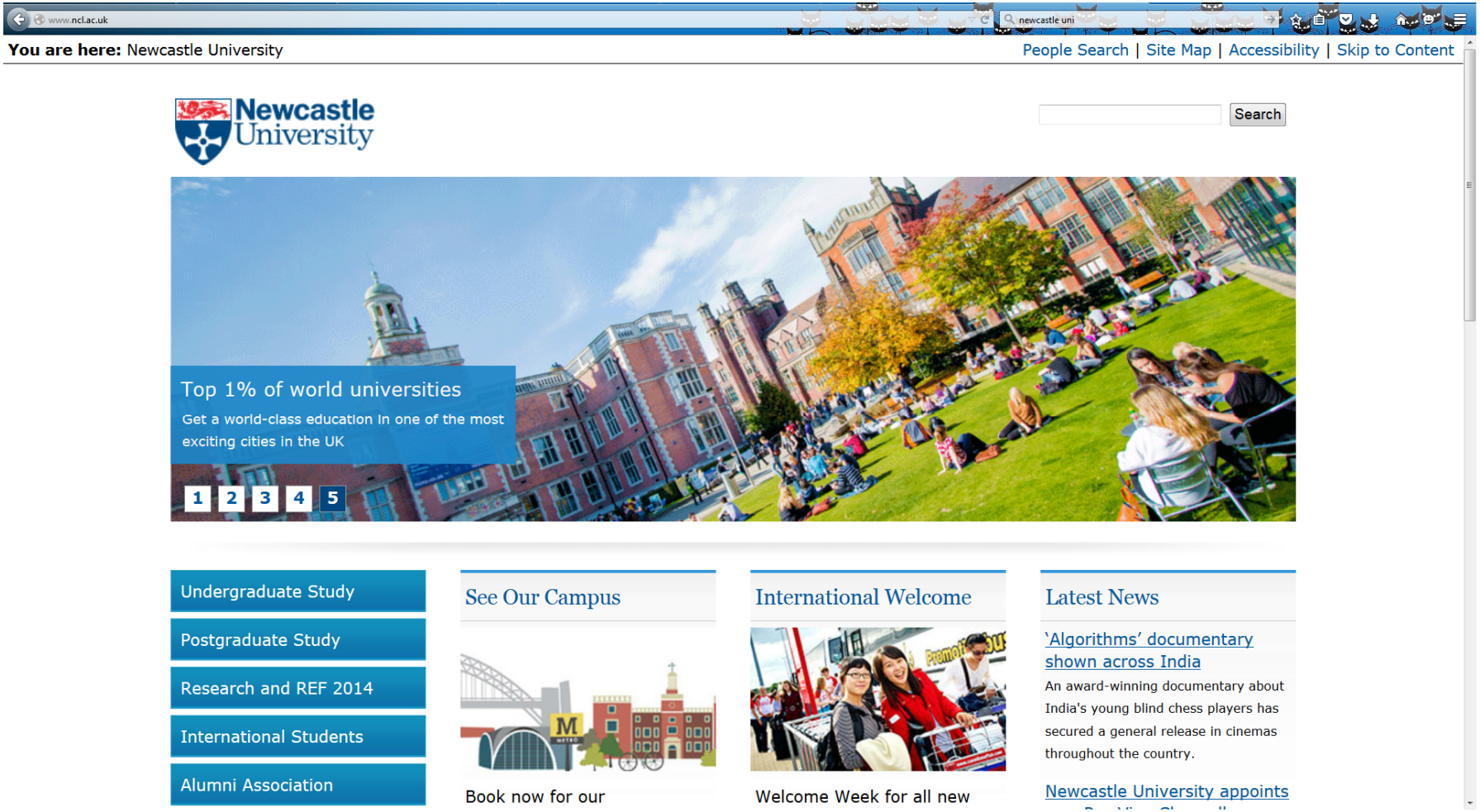
Attacks on User Privacy and Security Based on Mobile Motion and Orientation via JavaScript

M. Mehrnezhad, E. Toreini, S. Shahandashti, F. Hao

Newcastle University, UK

A picture from NCL in summer



Reality …

Mobile Sensors

- Touchscreen
- Geolocation
- Ambient light
- **Orientation and motion**
- ….

Access to mobile sensors by developers

- Writing native codes by using mobile OS APIs
- Recompiling HTML5 codes into native apps
- Using standard APIs provided by the W3C which are accessible through JavaScript codes within mobile browser

JavaScript codes

- Advantages
  - No app-store approval for the app/ update/ fix
  - Platform-free (Android, iOs, Windows, …)
  - No manual update by users after each release
- Disadvantages
  - Less accurate
  - Privacy and security issues
    - No installation
    - No permission
    - No notification

Sampling rates

Device/mOS	Accelerometer Freq. (Hz)	Gyroscope Freq. (Hz)
Nexus 5/Android 5.0.1	200	200
iPhone 5/iOS 8.2	100	100

Table 2: Maximum in-app sampling frequencies on different mobile OSs

Device OS	Browser	Motion Freq. (Hz)	Orientation Freq. (Hz)
Nexus 5/Android 5.0.1	Chrome	60	44
	Opera	60	52
	Firefox	50	50
	Dolphin	NA	151
	UC Browser	NA	15
iPhone 5/iOS 8.2	Safari	20	20
	Chrome	20	20
	Dolphin	20	20
	UC Browser	20	20

Table 3: Maximum in-browser sampling frequencies on different mobile OSs and browsers

In-browser access details

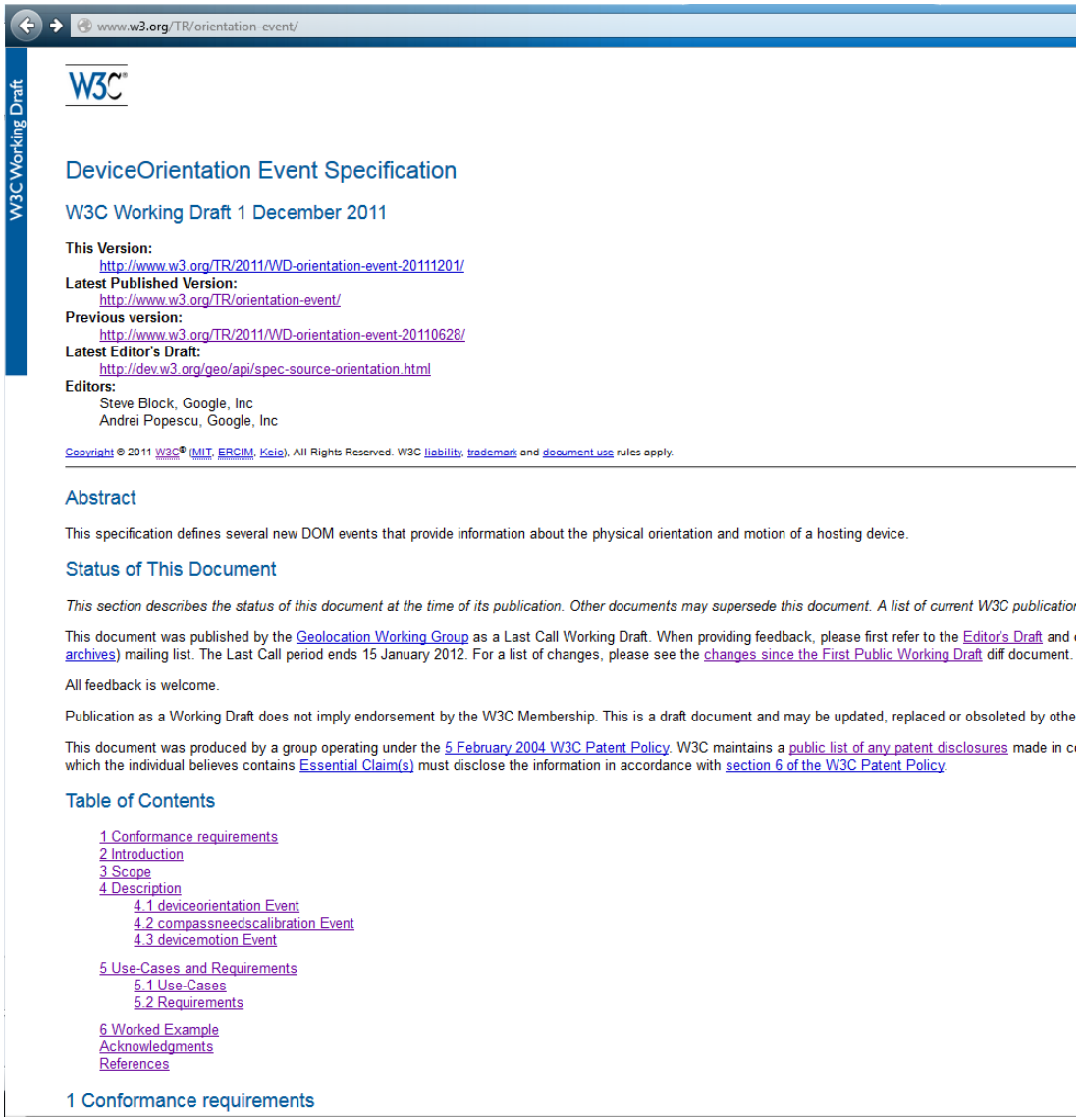
http://www.w3.org/TR/orientation-event/

- Orientation
  - the physical orientation of the device
- Motion:
  - Acceleration: the physical acceleration of the device
  - Acceleration including gravity
  - Rotation rate: rotation rate of the device
  - Interval: constant rate

Research questions

- What is the **W3C specification** for motion and orientation sensor data for mobile devices?
- How different mobile **browsers** have **implemented** this feature?
- What are potential privacy and security **attack vectors**?
- Is it actually possible to perform a **successful attack** in order to reveal users sensitive information such as their PINs and passwords?
- What are the possible **solutions** to fix this vulnerability?

W3C specification



www.w3.org/TR/orientation-event/

W3C Working Draft

W3C

DeviceOrientation Event Specification

W3C Working Draft 1 December 2011

This Version:
http://www.w3.org/TR/2011/WD-orientation-event-20111201/
Latest Published Version:
http://www.w3.org/TR/orientation-event/
Previous version:
http://www.w3.org/TR/2011/WD-orientation-event-20110628/
Latest Editor's Draft:
http://dev.w3.org/geo/api/spec-source-orientation.html
Editors:
Steve Block, Google, Inc
Andrei Popescu, Google, Inc

Abstract

This specification defines several new DOM events that provide information about the physical orientation and motion of a hosting device.

Status of This Document

This section describes the status of this document at the time of its publication. Other documents may supersede this document. A list of current W3C publicatio

This document was published by the Geolocation Working Group as a Last Call Working Draft. When providing feedback, please first refer to the Editor's Draft and archives) mailing list. The Last Call period ends 15 January 2012. For a list of changes, please see the changes since the First Public Working Draft diff document.

All feedback is welcome.

Publication as a Working Draft does not imply endorsement by the W3C Membership. This is a draft document and may be updated, replaced or obsoleted by othe

This document was produced by a group operating under the 5 February 2004 W3C Patent Policy. W3C maintains a public list of any patent disclosures made in c which the individual believes contains Essential Claim(s) must disclose the information in accordance with section 6 of the W3C Patent Policy.

Table of Contents

1 Conformance requirements
2 Introduction
3 Scope
4 Description
- 4.1 deviceorientation Event
- 4.2 compassneedscalibration Event
- 4.3 devicemotion Event

5 Use-Cases and Requirements
- 5.1 Use-Cases
- 5.2 Requirements

6 Worked Example
Acknowledgments
References

1 Conformance requirements

Ambient Light Events

W3C Last Call Working Draft 19 June 2014

.....

Table of Contents

1. Introduction
2. Conformance
3. Terminology
4. Security and privacy considerations
5. Device Light
    - 5.1 Extensions to `Window` Interface
    - 5.2 `DeviceLightEvent` Interface
        - 5.2.1 Event handlers

A. Acknowledgements

B. References
    - B.1 Normative references
    - B.2 Informative references

Geolocation API Specification

W3C Editors Draft 11 July 2014

.....

Table of Contents

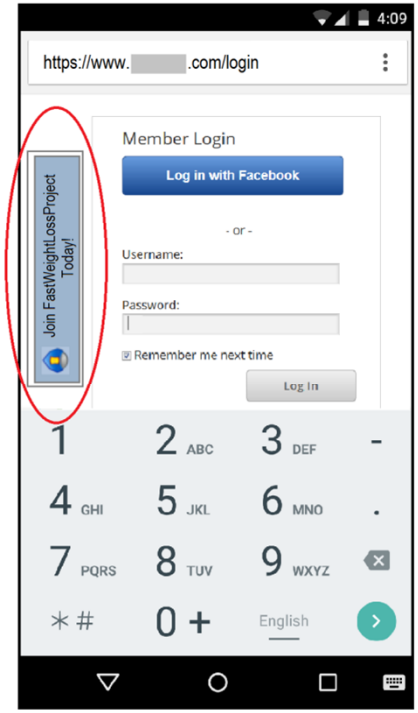
1 Conformance requirements
2 Introduction
3 Scope
4 Security and privacy considerations
    - 4.1 Privacy considerations for implementers of the Geolocation API
    - 4.2 Privacy considerations for recipients of location information
    - 4.3 Additional implementation considerations

5 API Description
    - 5.1 Geolocation interface
    - 5.2 PositionOptions interface
    - 5.3 Position interface
    - 5.4 Coordinates interface
    - 5.5 PositionError interface

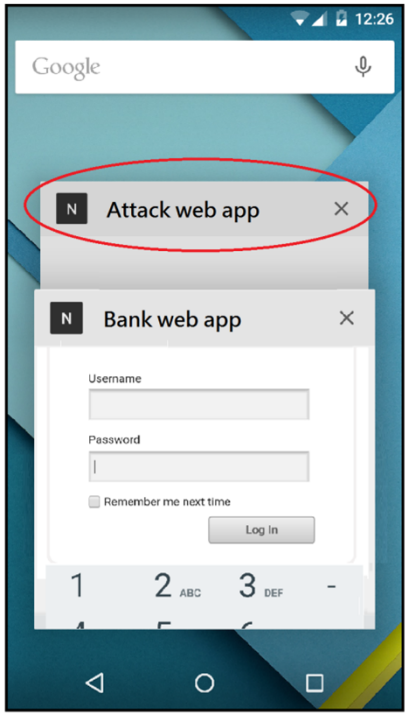
6 Use-Cases and Requirements
    - 6.1 Use-Cases
    - 6.2 Requirements

Acknowledgments
References

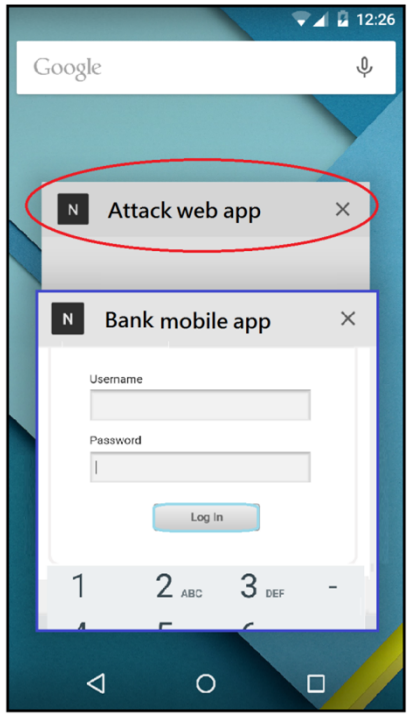
Attack Scenarios



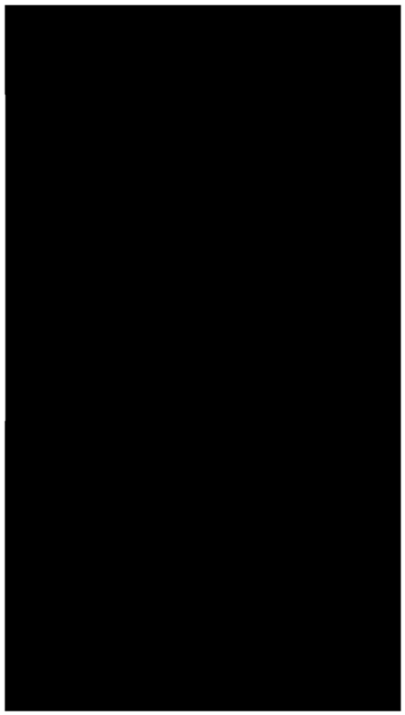
a



b



c



d

Browsers behaviour

Device/mOS/Browser		Active			Background		Locked	
		same	iframe	other	same	other	same	other
Nexus 5/Android 5.0.1	Chrome	yes	*yes*	—	—	—	—	—
	Opera †	yes	*yes*	—	—	—	—	—
	Firefox	yes	*yes*	—	—	—	—	—
	Dolphin	yes	*yes*	—	—	—	—	—
	UC Browser †	yes	*yes*	*yes*	—	—	—	—
	Baidu	yes	*yes*	*yes*	*yes*	*yes*	*yes*	*yes*
	CM Browser	yes	*yes*	*yes*	*yes*	*yes*	*yes*	*yes*
	Photon	yes	*yes*	*yes*	*yes*	—	*yes*	*yes*
	Maxthon	yes	*yes*	*yes*	*yes*	*yes*	*yes*	*yes*
	Boat	yes	*yes*	*yes*	*yes*	*yes*	*yes*	*yes*
	Next	yes	*yes*	*yes*	*yes*	*yes*	*yes*	*yes*
	Yandex	yes	*yes*	—	*yes*	—	*yes*	—
iPhone 5/iOS 8.2	Safari	yes	*yes*	—	—	—	*yes*	—
	Chrome	yes	*yes*	*yes*	—	—	—	—
	Dolphin	yes	*yes*	*yes*	—	—	—	—
	UC Browser	yes	*yes*	—	*yes*	—	*yes*	—
	Baidu Browser	yes	*yes*	*yes*	*yes*	*yes*	*yes*	*yes*
	Maxthon	yes	*yes*	*yes*				
	Yandex	yes	*yes*	*yes*	—	—	—	—
	Mercury	yes	*yes*	*yes*	—	—	—	—

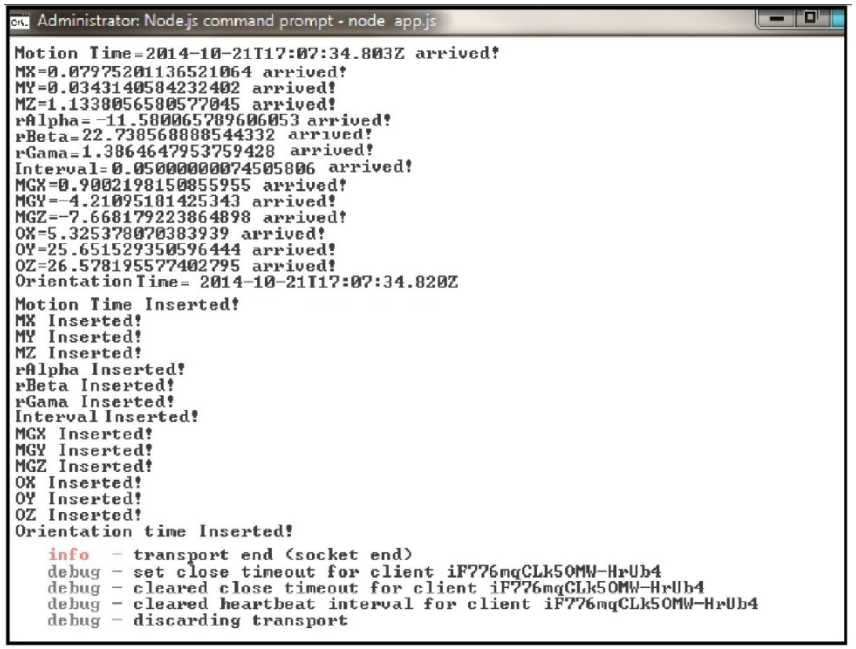
Table 4: Mobile browser access to the orientation and motion sensor data on Android and iOS under different conditions. A † indicates a family of browsers (e.g., Opera and Opera Mini are considered to be in the same Opera family). A *yes* (in italics) indicates a possible privacy/security leakage vector. A *yes* (in italics and underlined) indicates a possible privacy/security leakage vector only in the case when the browser was active before the screen is locked.

What the attack can reveal about the users?

- Phone call timing
- Physical activities
- Touch action types
- PINs/ Patterns/ Passwords
- Identity
- …

Our JavaScript code

- js code, register two listeners
- Client; GUI in html5
- Server; node.js, Mongolab db




```
function socketInit(){
//initial settings
socket= io.connect();
socket.on('connected', function(){
if (window.DeviceOrientationEvent){
window.addEventListener('deviceorientation',
function(event){
var gamma= event.gamma;
var beta= event.beta;
var alpha= event.alpha;
socket.emit('OX', gamma);
socket.emit('OY', beta);
socket.emit('OZ', alpha); }); }
if (window.DeviceMotionEvent){
window.addEventListener('devicemotion',
function(event){
var acceleration= event.acceleration;
var gacc= event.accelerationIncludingGravity;
var interval= event.interval;
var rotationRate= event.rotationRate;
var ax= acceleration.x;
var ay= acceleration.y;
var az= acceleration.z;
var ralpha= rotationRate.alpha;
var rbeta= rotationRate.beta;
var rgama= rotationRate.gamma;
var gx= gacc.x;
var gy= gacc.y;
var gz= gacc.z;
socket.emit('MX', ax);
socket.emit('MY', ay);
socket.emit('MZ', az);
socket.emit('rAlpha', ralpha);
socket.emit('rBeta', rbeta);
socket.emit('rGama', rgama);
socket.emit('MGX', gx);
socket.emit('MGY', gy);
socket.emit('MGZ', gz);
socket.emit('interval', interval); }); }
socket.on('disconnect', function(){
alert("Disconnected!"); }); }
```

Phone call timing

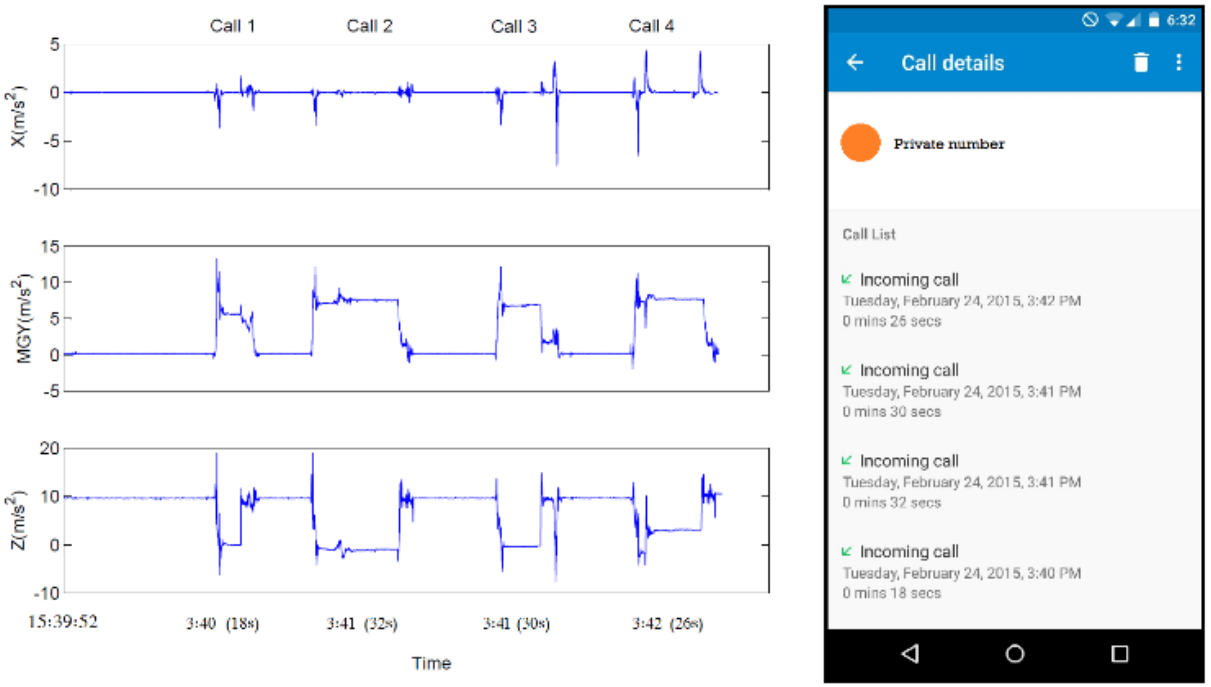


Figure 2: Left: Three dimensions (x, y, and z) of acceleration data including gravity from the device motion sensor. The start time, duration, and end time of four phone calls are easily recognisable from these measurements. Right: The screenshot of the call history of the phone during the experiment for comparison.

Physical activities

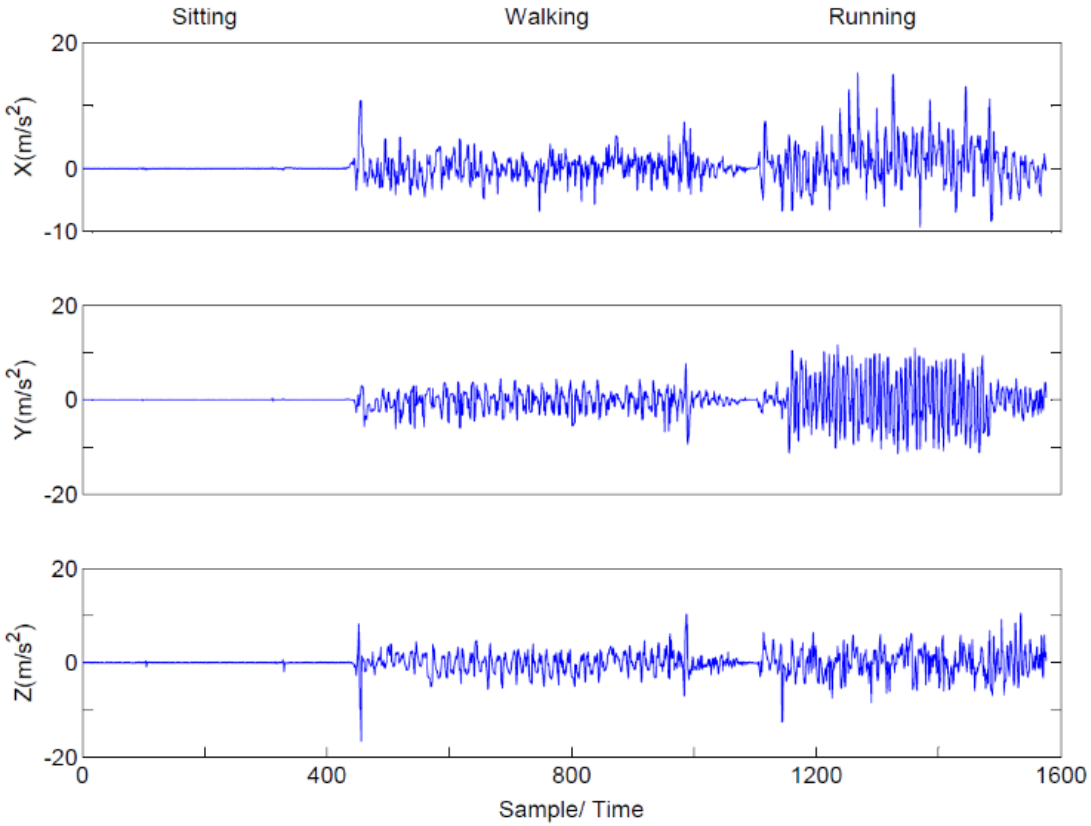


Figure 3: Three dimensions (x, y, and z) of acceleration data (from the device motion sensor) during 22 seconds of sitting, 34 seconds of walking and 25 seconds of slow running. The three activities have visible distinctive measurements.

Touch Action Types

- Classification techniques
- Wider experiments (11 users using Chrome on iPhone)
- Extracting 164 features in the time/frequency domain
- Using k-nearest neighbour (k-NN)

Touch Action	Description
Click	Touching an item momentarily with one finger
Scroll – up, down, right, left	Touching continuously and simultaneously sliding in the corresponding direction
Zoom – in, out	Placing 2 fingers on the screen and sliding them apart or toward each other, respectively
Hold	Touching continuously for a while with one finger

Table 5: The description of different touch actions users perform on the touch screen of a mobile device.

Results

Touch action	Click	Hold	Scroll	Zoom in	Zoom out
Click	**78.18%**	5.45%	2.73%	0%	0%
Hold	10.9%	**88.18%**	0.68%	1.81%	1.82%
Scroll	7.27%	2.72%	**95.91%**	0.90%	0.90%
Zoom in	0%	1.82%	0.23%	**71.82%**	20.9%
Zoom out	3.64%	1.82%	0.45%	25.45%	**76.36%**
Total	100%	100%	100%	100%	100%

Table 6: Confusion matrix for the first classifier for different touch actions

Touch action	Scroll down	Scroll up	Scroll right	Scroll left
Scroll down	**57.27%**	19.09%	12.73%	4.55%
Scroll up	26.36%	**69.09%**	16.36%	6.36%
Scroll right	9.09%	4.55%	**48.18%**	17.27%
Scroll left	7.27%	7.27%	22.73%	**71.82%**
Total	100%	100%	100%	100%

Table 7: Confusion matrix for the second classifier for different scroll types

PINs

- More advanced classification techniques
- Even wider experiments (12 users, using Chrome on Android and iOs)
- Extracting 150 features in the time/frequency domain
- Using Artificial Neural Network (ANN)

1 (54%)	2 (64%)	3 (63%)	-
4 (81%)	5 (67%)	6 (73%)	.
7 (57%)	8 (74%)	9 (79%)	x
*#	0 (73%)	English	>

Nexus 5 (Ave. iden. rate: 70%)

1 (70%)	2 (50%)	3 (59%)
4 (70%)	5 (46%)	6 (56%)
7 (53%)	8 (48%)	9 (67%)
+ * #	0 (41%)	>

iPhone 5 (Ave. iden. rate: 56%)

Table 8: Identification rates of numbers in Nexus 5 and iPhone 5.

More attacks…

Solutions in the standards level

- Security and privacy considerations for ambient light in W3C specification:
  - “The event defined in this specification is only fired in the top-level browsing context to avoid the privacy risk of sharing the information defined in this specification with contexts unfamiliar to the user. For example, a mobile device will only fire the event on the **active tab**, and **not** on the **background tabs** or within **iframes**”

Solutions in the implementation level

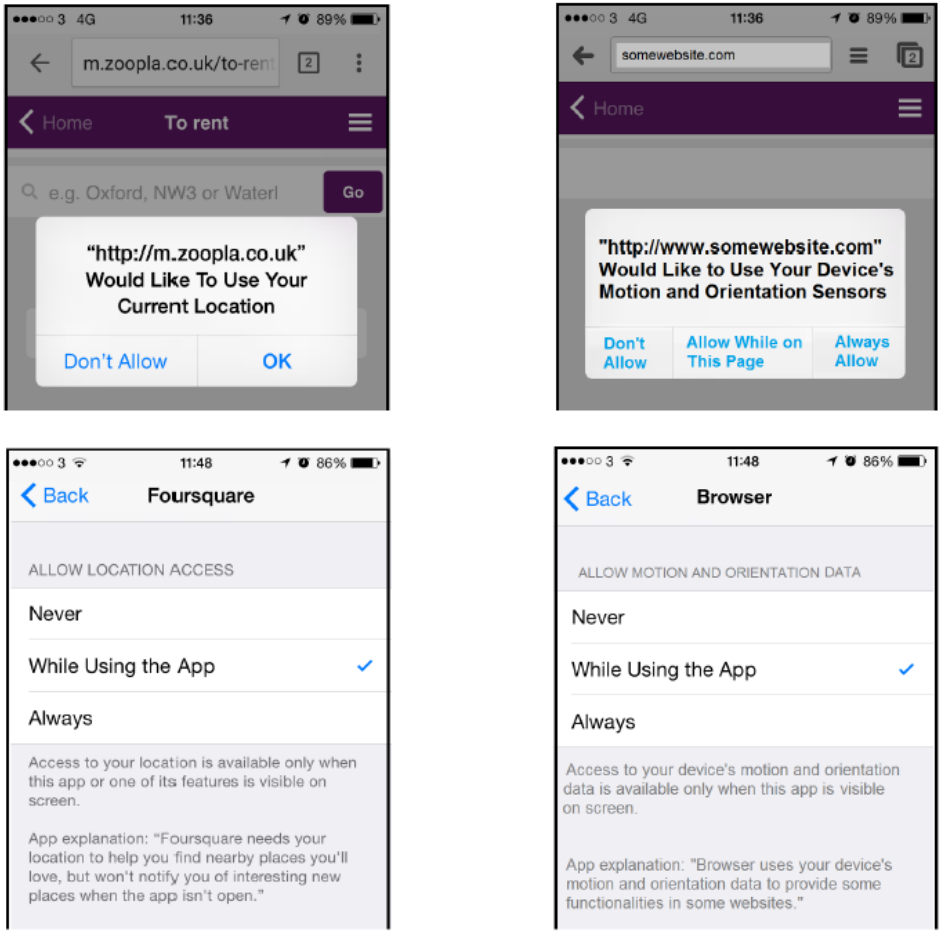


Figure 5: Left: The existing interfaces to allow the web page to access Geolocation in browser (top) and in mobile OS (down). Right: Our suggested mock-up interfaces to allow web page (top) and OS setting (down) to access Motion and Orientation data in browser.

Informing W3C and browsers vendors

- Informed vendors
  - W3C, Chromium, Firefox, Safari, Opera, Dolphin
- Feedback
  - …

Publications

- TouchSignatures: Identification of User Touch Actions based on Mobile Sensors via JavaScript
  - ASIACCS'2015, Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security
- TouchSignatures: Identification of User Touch Actions and PINs based on Mobile Sensors via JavaScript
  - Journal of Information Security and Applications
- More available at: http://homepages.cs.ncl.ac.uk/m.mehrnezhad/

- Thanks
- Q&A