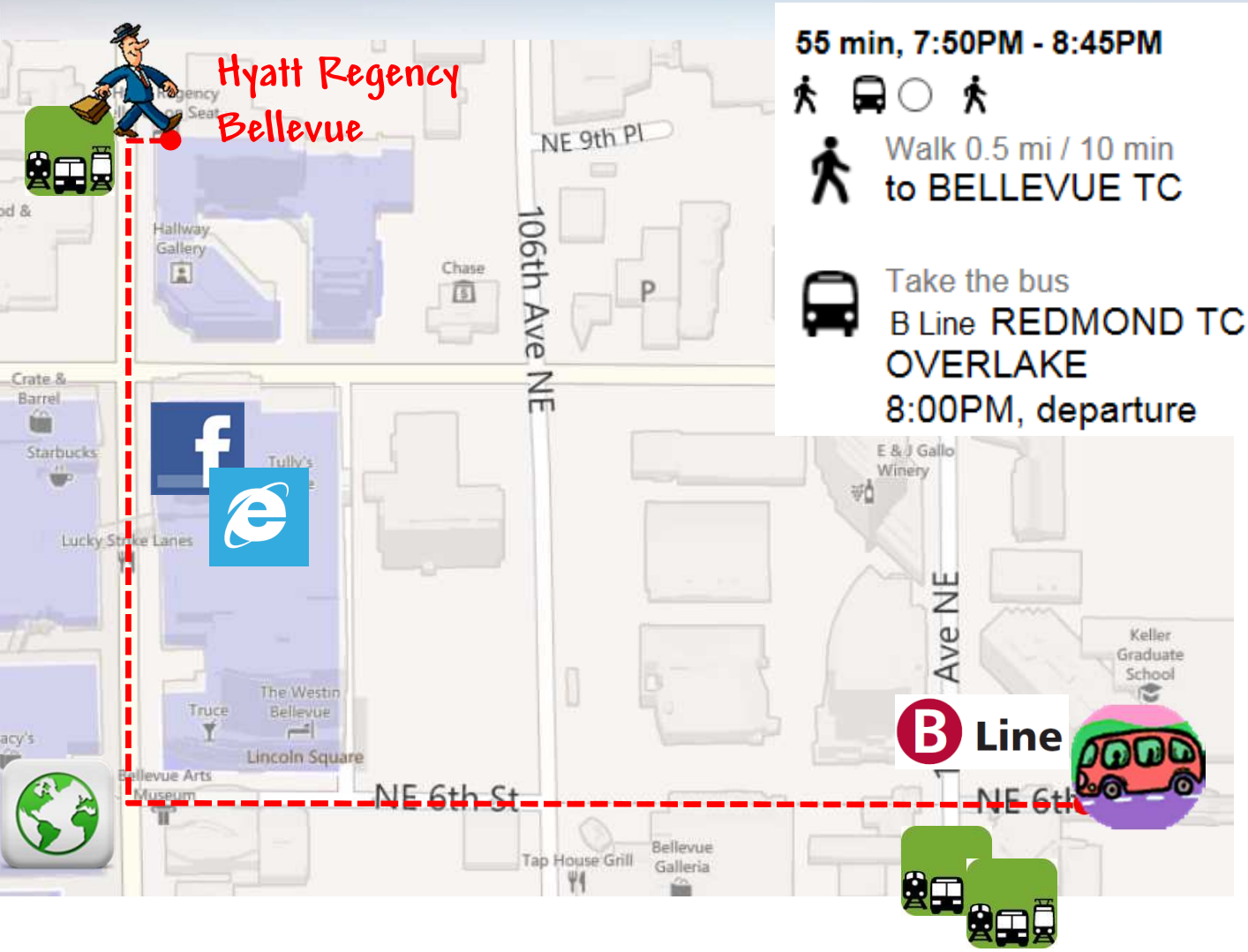
Progressive Authentication: deciding when to authenticate on mobile phones

Oriana Riva (Microsoft Research)
Chuan Qin (University of South Carolina)
Karin Strauss (Microsoft Research)
Dimitrios Lymberopoulos (Microsoft Research)

Joe on his way to the bus…



1 out 6 has private info

Where?: pocket, hands
Who?: face, voice

1 PIN every 2 min

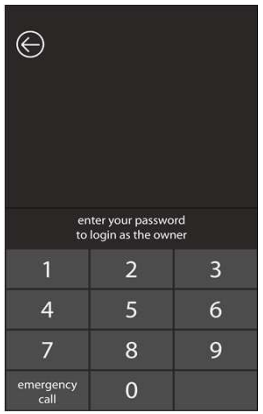
5 PIN requests

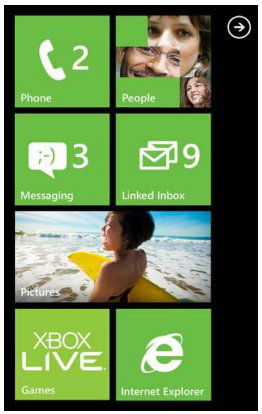
6 app invocations

Security vs. usability

- More than 60% of users do not use a PIN on their mobile phone (*)

- All-or-nothing access control model does not meet mobile users' requirements
  - See our user study results:
    "*Goldilocks and the Two Mobile Devices*" (**)





(*) http://www.bullguard.com/news/latest-press-releases/press-release-archive/2011-06-21.aspx

(**) E. Hayashi et al., *Goldilocks and the Two Mobile Devices: Going Beyond All-Or-Nothing Access to a Device's Applications*. SOUPS 2012

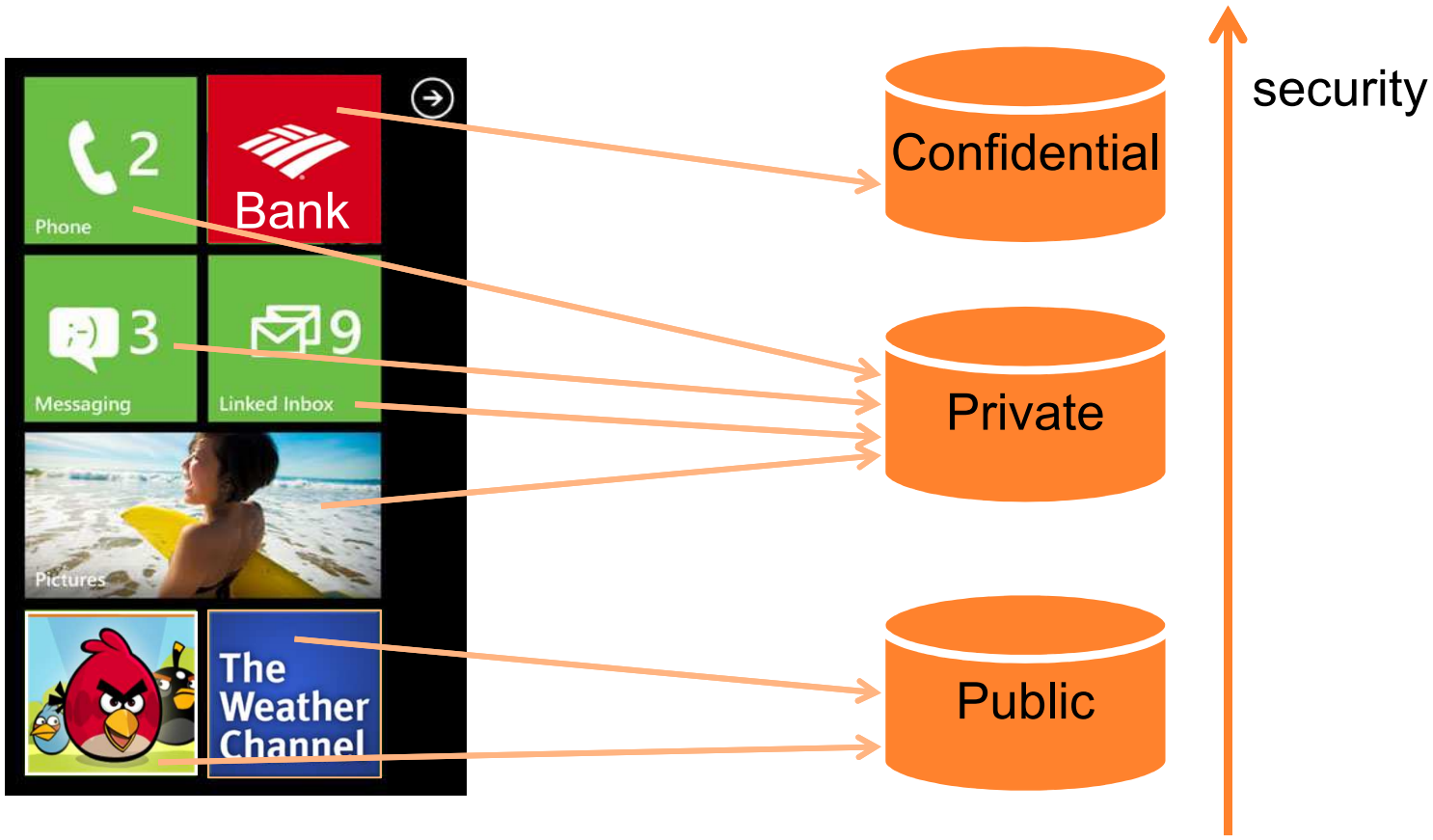
Progressive authentication

… is not about a new authentication mechanism for mobile devices.

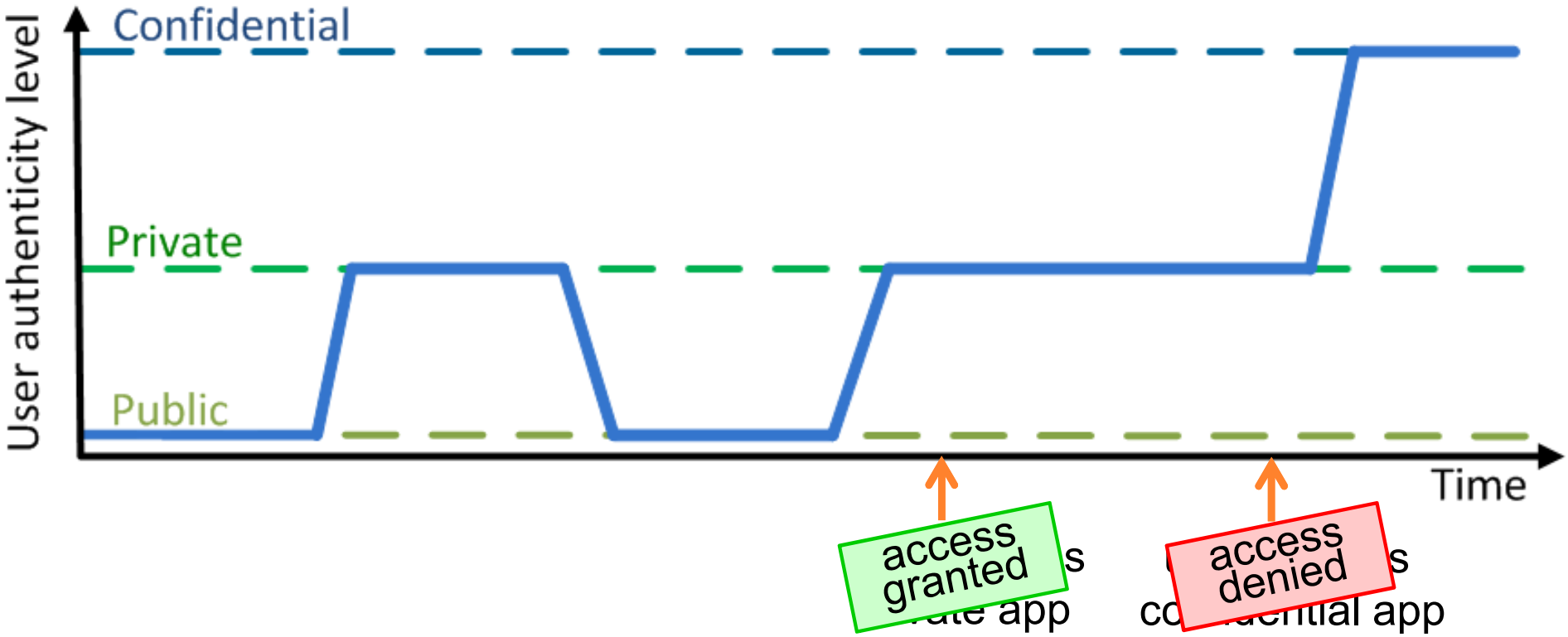
… is about deciding when to surface authentication and for which applications.

Beyond all-or-nothing

- Different protection levels for different applications
  - Our user study indicates 3 levels are desirable



Multi-level authentication




```
if (authenticity_level < app_security_threshold)
   request_credentials
else
   grant_access
```

How is the authenticity level computed?

Sensors are here and more are coming!

Which sensor to use for authentication?

Little Rock: Enabling Energy Efficient Continuous Sensing on Mobile Phones

Bodhi Priyantha, Dimitrios Lymberopoulos, and Jie Liu
Networked Embedded Computing Group
Microsoft Research
Redmond, WA
{bodhip, dlymper, liuj}@microsoft.com

and a powerful processor for information processing. This allows phones to *continuously sense* their users and they interact with, *understand* this environment to *provide* meaningful services, such as

Mobile 3.0 arrives: How Qualcomm just showed us the phone (and why iPhone sucks for this new contextual

JULY 11, 2012 BY ROBERT SCOBLE • 2 COMMENTS

Like Send 580 likes. Sign Up to see what your friends like.

The world just changed yesterday. You probably didn't notice. But I gu at Apple, Facebook, Amazon, Microsoft, and Google did.

What happened? Qualcomm shipped a new contextual awareness pla phones.

Yesterday the Mobile 3.0 world arrived. First mobile was the standard talked into it. The second mobile era was brought to us by the iPhone. screen. The third era will bring us a mobile that

The New York Times Technology | Personal Tech | Business Day

Bits

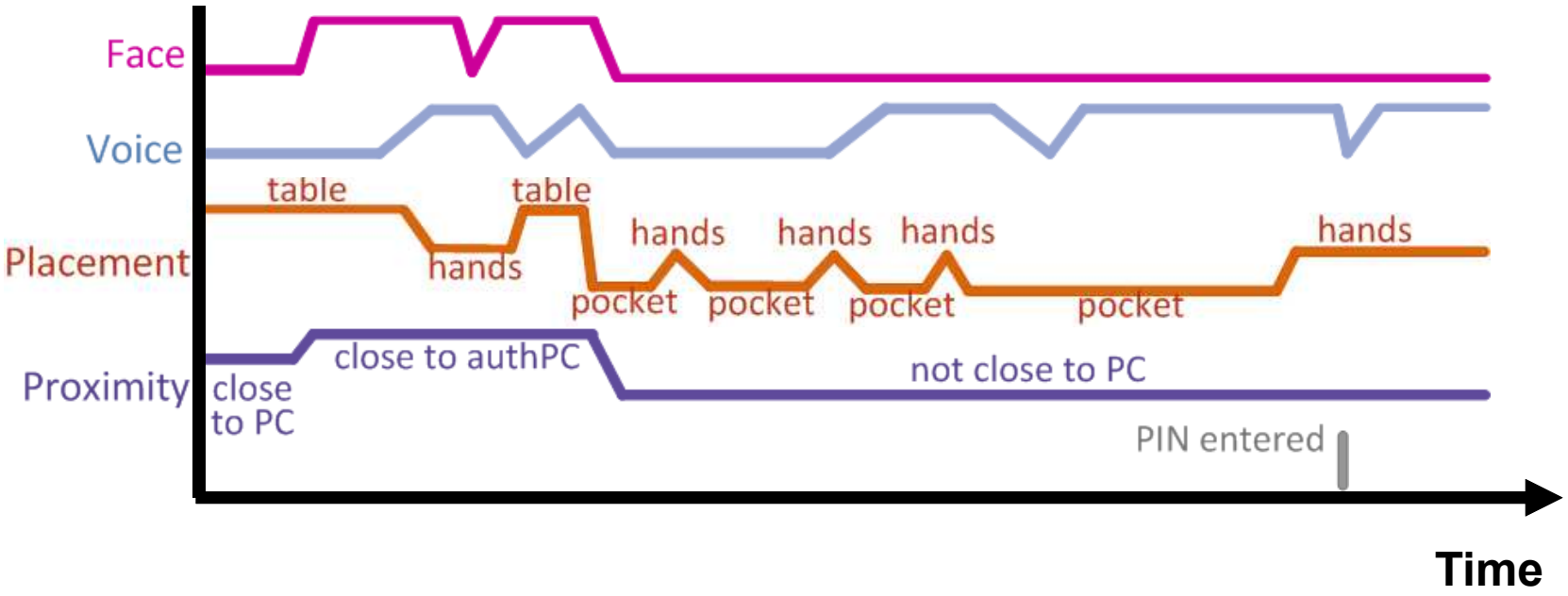
BITS; Sensors for Smarter Smartphones

By NICK BILTON
Published: May 23, 2011

If you own a smartphone, you probably know just how smart those little gadgets are. They know where you're standing, the direction you're moving in and if you're holding the phone vertically or

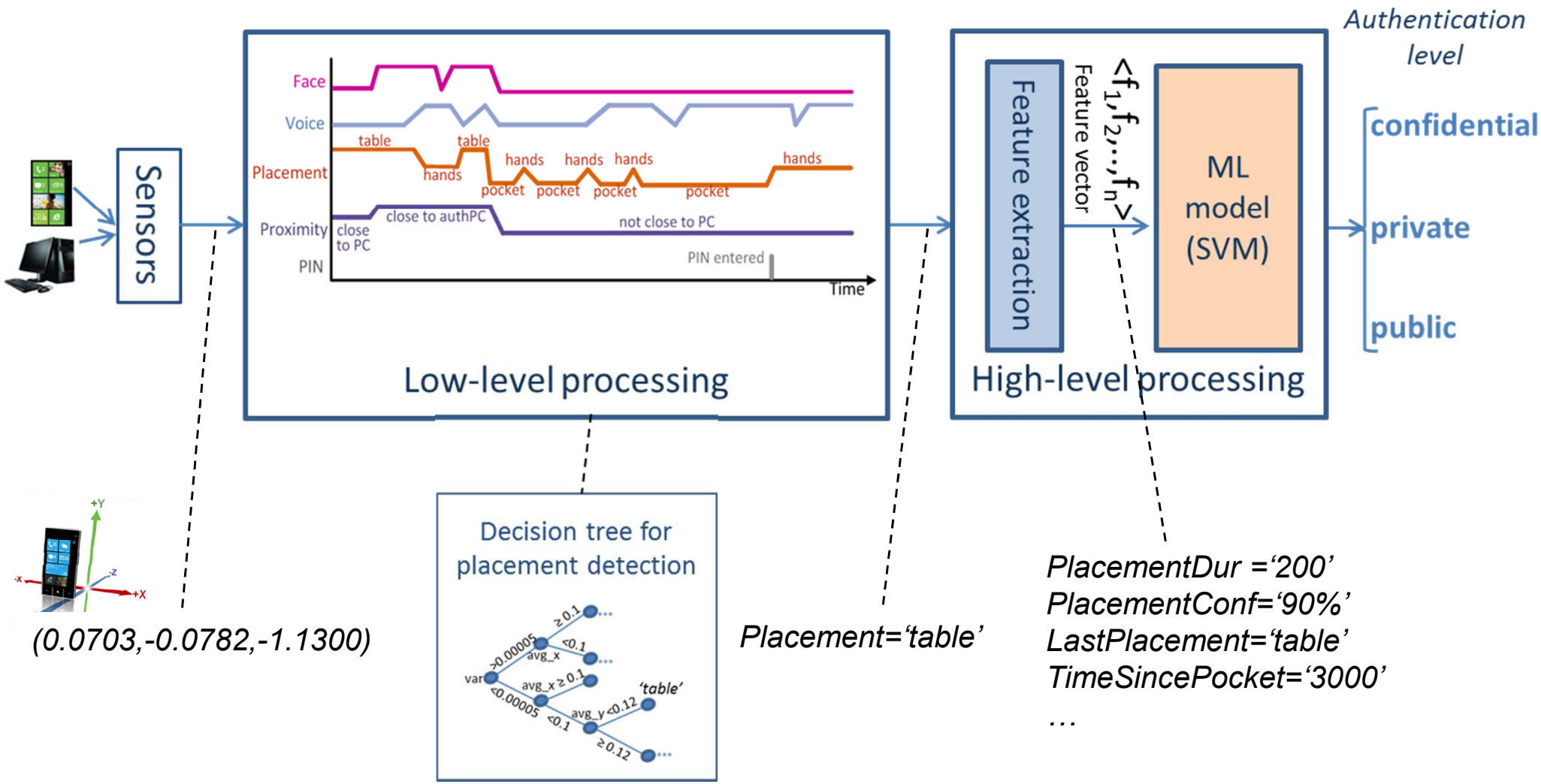
Multi-modal, multi-device model

- Identity: face and voice recognition (camera, audio)
- Continuity: when has the user let go off the phone? (acc., touch, light...)
- Proximity to other known devices (Bluetooth, activity detection sensors)
- Secrets: PIN, passwords
- … and many more: behavioral signals, possession signals, etc.

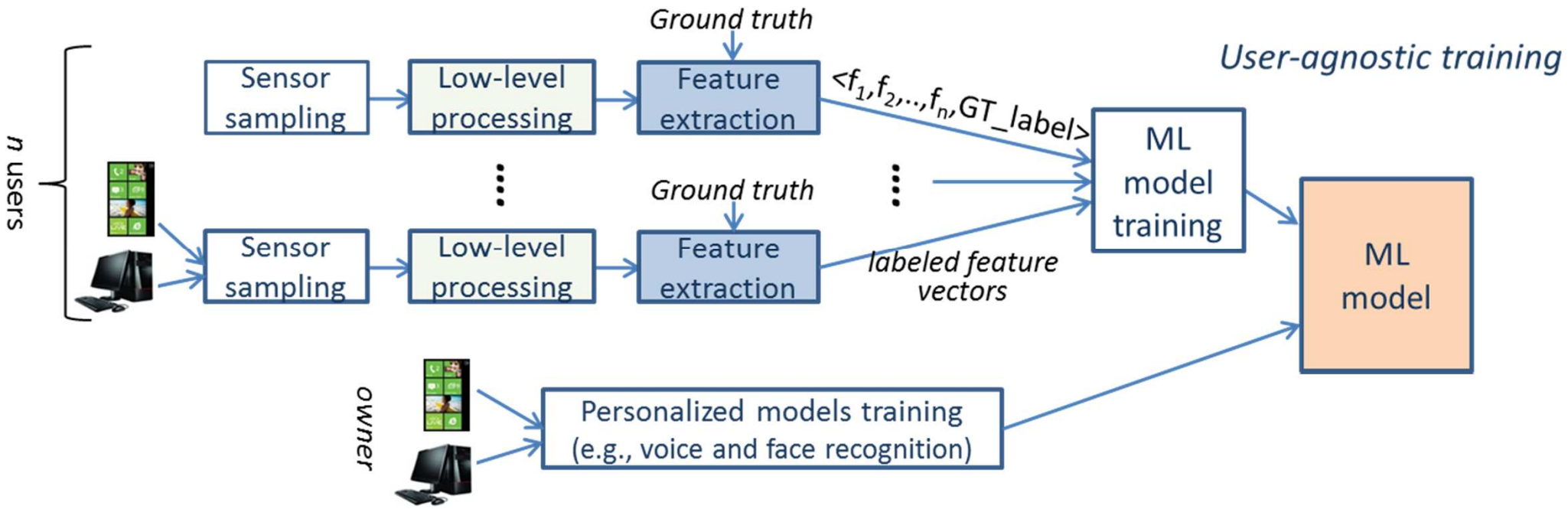


Dealing with noisy, unreliable signals

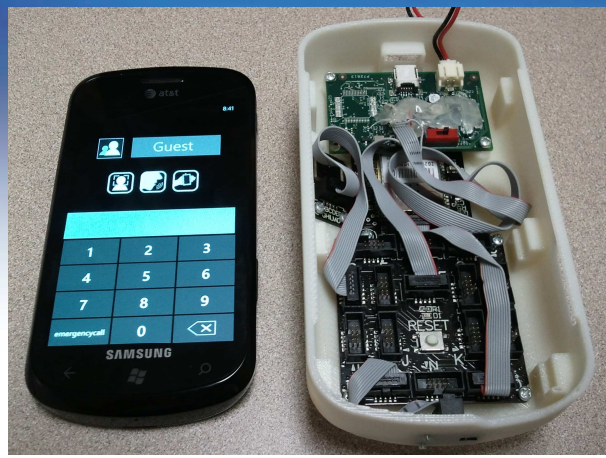
- Not robust in isolation, combined using machine learning models



Training machine learning models



Implementation



- Implemented on WP7.5 + Gadgeteer sensors
- Data collection and offline training
  - Office scenarios: 9 users for 1.5 h, 5 apps, phone-PC setup
- Attack scenarios
  - Attackers: strangers or known non-owners
  - May or may not know which sensor signals the system relies on
  - No attacks to passwords or biometrics
  - No attacks on wireless link, trusted OS
  - If owner present, implicit authorization
- 3 machine learning models
  - SVM (support vector machine), Decision Tree, Linear Regression

System evaluation

- Goals
  - Authentication overhead
  - Convenience and security trade-offs
  - High and low-level processing models' accuracy
  - Power consumption

Authentication overhead reduction

- Overhead reduction of 42% and no unauthorized accesses

	Phone w/o PIN	Phone w/ PIN	ProgAuth
PIN entries	0	19.2	11.2
Unauthorized accesses	100%	0%	0%

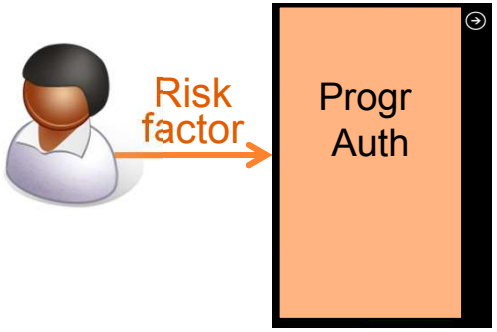
Convenience and security trade-offs

- False Rejection (FR): Incorrectly require a PIN from a legitimate user
- False Authentication (FA): Incorrectly authenticate a non-legitimate user

R low → **R high**

Security
(More FRs)

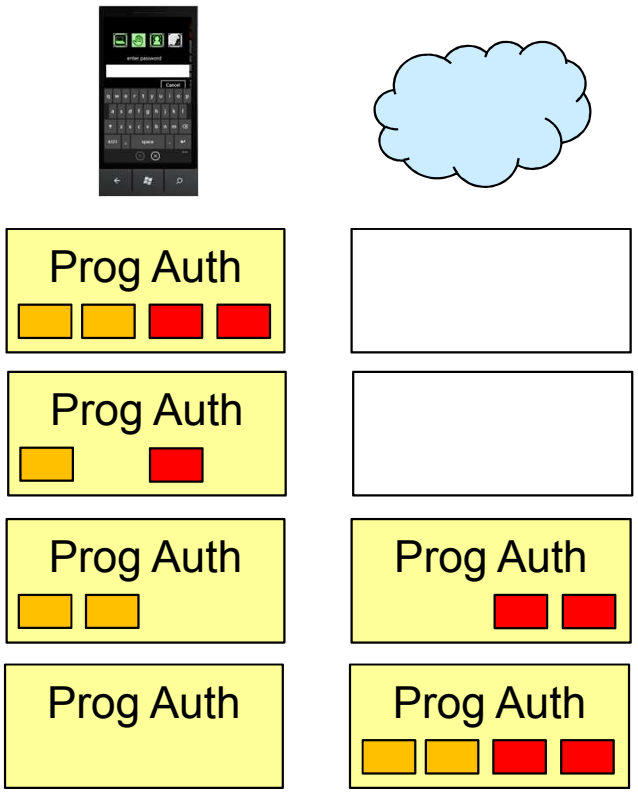
Convenience
(More FAs)



Risk factor	%FR Priv	%FR Conf	%FA Priv	%FA Conf
0.05	57.7	100.0	3.3	0.0
1	53.5	98.4	4.9	0.0
20	34.4	96.8	16.1	0.0

Power consumption

- Low-energy continuous sensing architecture (e.g., LittleRock)
- Disable/enable costly signals
- Offload computation to cloud



Config.	Avg power (mW)	Exec time (sec)
Local	651	0.23

(*) reduced model accuracy

Conclusions

- Benefits
  - Smaller authentication overhead
  - Multi-level protection for valuable data
- Prototyped for mobile phones
  - But extensible to desktop PCs, tablets, etc.
- With a few unreliable signals promising accuracy
- Power consumption and execution overhead acceptable

Thanks and see me for a demo