CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS'

Usable Multi-Factor Authentication and Risk-Based Authorization

IBM T. J. Watson Research Center

Larry Koved, Research Staff Member

17 September 2013

Homeland Security

Science and Technology

We gratefully acknowledge the UK for supporting this project

Team Profile

- **IBM Research, T.J. Watson Research Center, Yorktown Heights, NY**
  - A multi-disciplinary research facility
  - Security research on a broad range of topics, including hardware, information, operating systems, cryptography and network security
- World wide research team on security and privacy topics

- **Interdisciplinary Team – HCI, Security, Biometrics, Systems**
  - *Larry Koved*, Information Security, mobile security, HCI, middleware
  - Dr. Rachel Bellamy, User Experience Design and Engineering, HCI, psychometrics
  - Dr. Pau-Chen Cheng, Information Security, risk analysis
  - Dr. Nalini Ratha, Exploratory Computer Vision, biometrics
  - Dr. Kapil Singh, Information Security, web and mobile security
  - Calvin Swart, User Experience Design and Engineering, mobile and web HCI
  - Dr. Shari Trewin , User Experience Design and Engineering, HCI, accessibility

Customer Need

Who is using this mobile device?

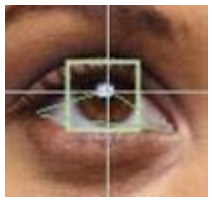
Valuable information and assets are at risk!

- **Mobile device interaction is brief (< 1 minute)**
  - Often interrupt driven
  - Authentication is a *secondary* task
- **Secure passwords are very hard to enter on these devices**
  - High dissatisfaction with strong password entry
  - *Security credentials are cached by mobile apps*
- **Mobile device unlock is predominantly:**
  - Weak credentials: PIN / SWYPE
  - No authentication
- ***We are authenticating devices!***
  - Mobile devices are more likely to be lost / stolen / shared / borrowed

Security versus usability – asking too much or too little.

Approach: Human Interaction Paradigm Shift

Interaction being driven by mobile multi-modal features



Eye tracking

Camera

Touch / Haptics

Speech recognition

Text spoken

Context

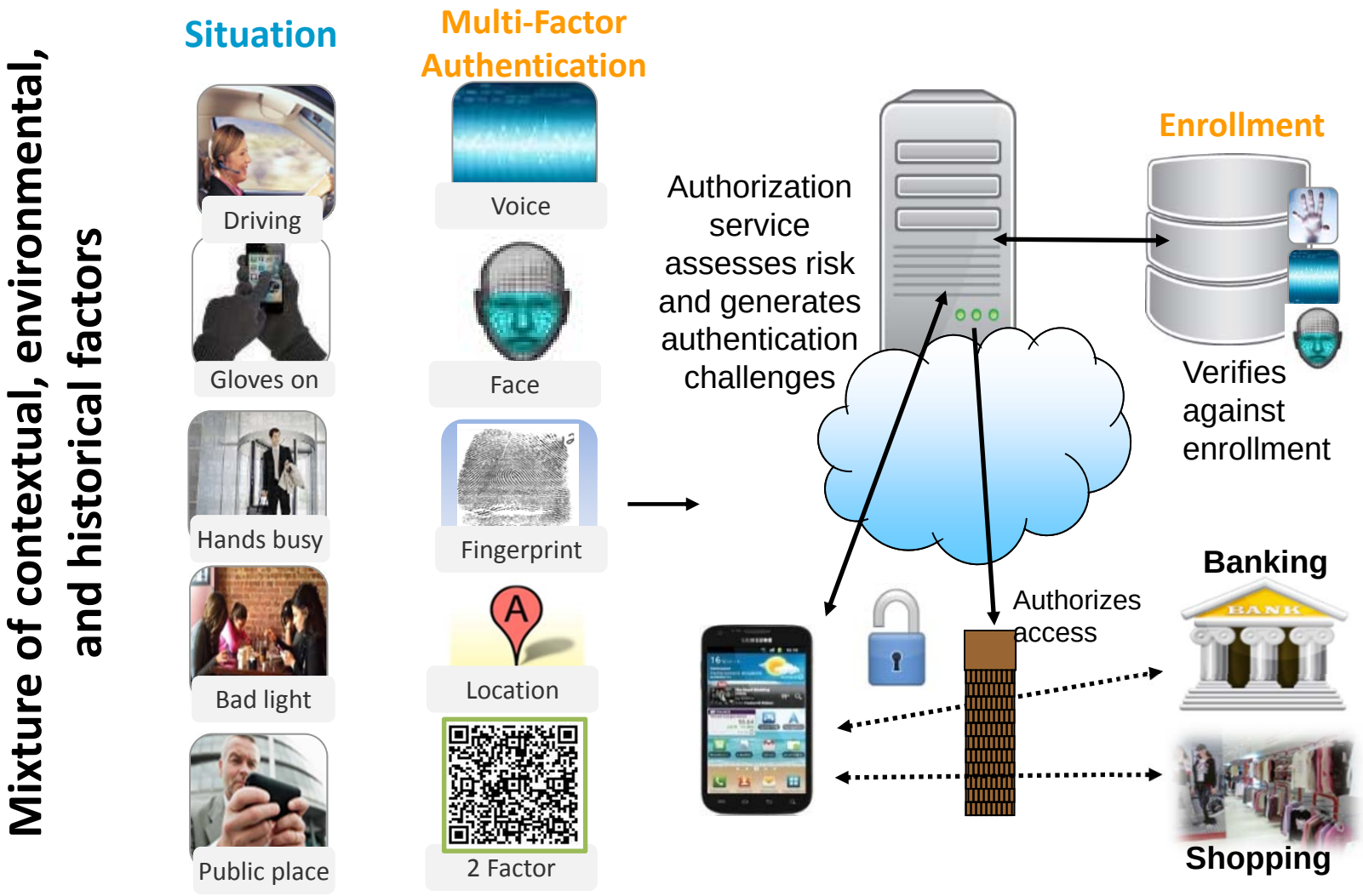
Location

No wires

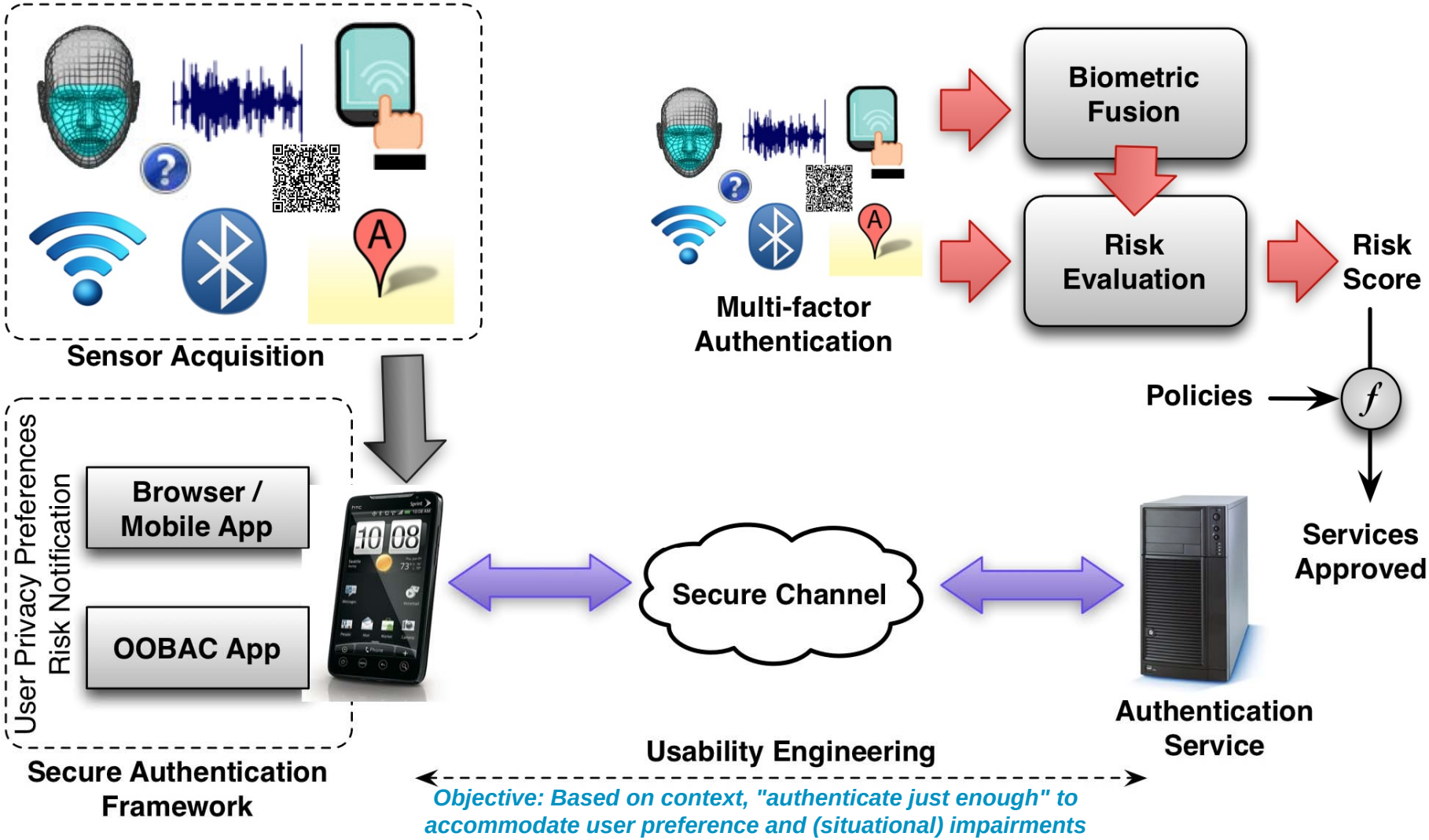
Transactions

Motion

Approach: Balancing Usability and Security



Approach



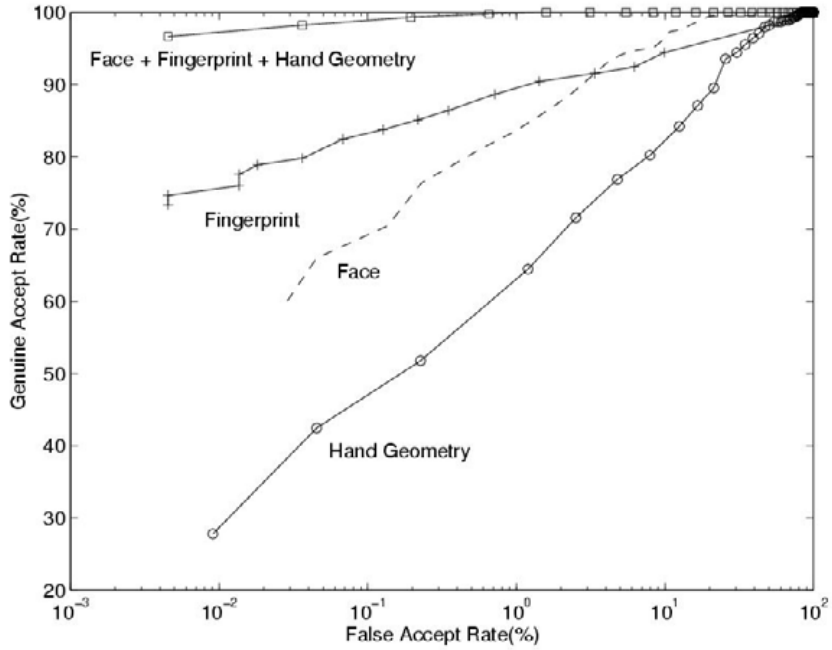
Approach

Strong Authentication Through Fusion

Property	Fingerprint	Face	Iris	Voice
Distinctiveness	High	Low	High	Low
Permanence	High	Medium	High	Low
How well trait can be sensed	Medium	High	Medium	Medium
Speed and cost efficiency of system	High	Low	High	Low
Willingness of people to have trait used	Medium	High	Low	High
Difficulty of spoofing the trait	High	Low	High	Low
False reject rate*	0.4 percent	1.0–2.5 percent	1.1–1.4 percent	5–10 percent
False accept rate*	0.1 percent	0.1 percent	0.1 percent	2–5 percent

Biometric Traits

*Error rates depend on testing environment, sensors used and composition of users in the population.

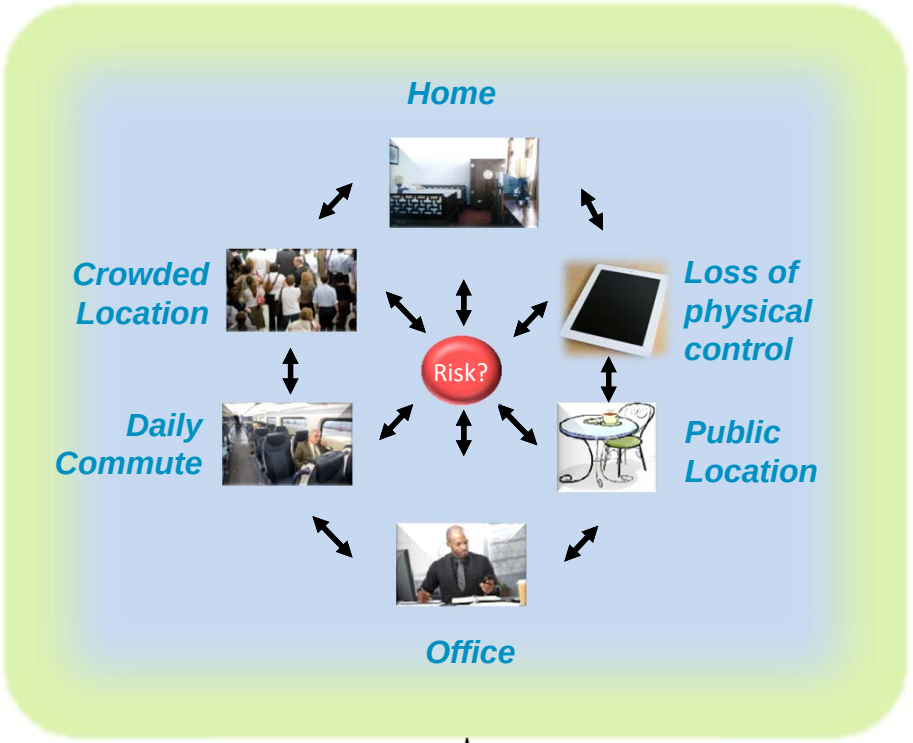


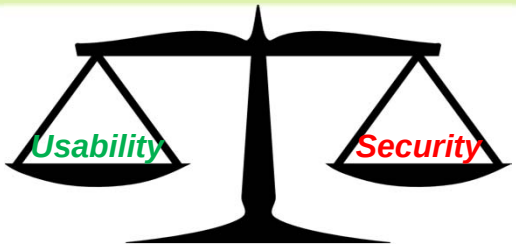
- **Fusion always gets better accuracy when the underlying modalities (biometrics) are uncorrelated.**
- **Table shows 2008 state of the art.**

Benefits

Usable Security: Authenticate *if and when* needed, *to the extent* needed.

- Eliminate insecure passwords on mobile devices
  - Eliminate on-device password caching risks
  - Eliminate forgotten passwords
- Strong usable multi-factor authentication
  - Simple user interaction
  - Minimize authentication challenges
  - Multi-factor biometric (who you are)
  - Non-biometric authentication
  - "Continuous" authentication
  - Extensible framework
- Estimates change in possession of the device
  - "Lock out" to prevent misuse by a 3rd party
- Risk-based authorization
  - Model user/device context and behaviors
  - Authentication commensurate with value at risk
  - Risk communication
- Integrate with existing apps with no app code changes





Competition

- Passwords
  - Hard to remember
  - Insecurely stored
  - Very hard to enter compliant passwords
  - Disruptive to *short term* memory
- 2-factor tokens
  - Separate item to lose
  - Dreaded token “necklace”
  - Subject to social engineering
- 2-factor SMS – insecure (eavesdropping apps risk)
- Single factor biometrics
  - Relatively weak
  - Ignores situational impairments
  - Niche vendors
  - Increases risk due to non-trivial false accept rate
  - Device-centric
- Traditional authentication flows
  - Ignores context and history
  - Does not reduce security challenges based on context

Current Status

Accomplishments so far

- **Operational demo system**
  - Negotiating the commercialization of the system (see *Next Steps)*
- **Security software frameworks**
  - System architecture & communication protocol
  - Cross-platform client-side framework & UI
  - Server-side frameworks with bio & context plug-ins
  - Out-Of-Band Authentication Client (OOBAC)
    - Including unattended device detection
  - User interface for multi-factor authentication
- **Risk Perception**
  - 2 psychometric studies on perceived risk in mobile transactions
  - Taxonomy of perceived risk
  - Risk communication design
- **Risk-based authorization**
  - Offline modeling of risk factors, focusing on time & location; features beyond GPS to model location
  - Risk-based access control policy
- ***Risk Perception in Information Technology workshop***
  - Started and co-chaired with L. Jean Camp (U Indiana)
  - 53+ attendees, most popular workshop at the *Symposium on Usable Privacy and Security,* http://cups.cs.cmu.edu/soups/2013/risk.html
- ***MObile Security Workshop (MoST 2013)***
  - Started and co-chaired with Hao Chen (U.C. Davis)
  - Popular workshop for mobile security topics
  - 60+ attendees, most popular workshop at the *IEEE CS S&P Workshops,* http://mostconf.org/2013/
- **Patents**: two filings in progress, one filed.

  Papers: *Perceived Security Risks in Mobile Interaction.* Koved, Trewin, Swart, Singh, Cheng, Chari. Risk Perception in Info. Tech. workshop. One in submission (Singh & Koved), two in preparation. Two related papers: RAID 2013 and one in submission (Singh).
- **University collaborations** being explored:
  - University College London, Carlton University, and Helsinki Institute for Information Technology

Deliverables so far

- Risk Perception reports
  1. *Design of Psychometric Studies on Security Risk Perception for Mobile Authentication and Authorization*
  2. *Taxonomy of Perceived Risk in Mobile Authentication and Interaction*
  3. *Perceived Risk in Mobile Authentication and Interaction*
  4. *Heuristic Evaluation of Mobile Authentication & Risk Communication Design*

Next Steps

- **Upcoming deliverables:**
  4Q2013: Biometric fusion
  1Q2013: User preference specification & enforcement
  3Q2014: Full system demo and evaluation, online modeling of risk

- **Technology Transition Activities**

  – Ongoing meetings with customers in multiple industries
    - Assess needs / requirements / use cases / scenarios / validation
    - Understand their security and integration concerns
    - Integration scenarios with existing mobile applications

  – Negotiations with potential distribution channels
    - Application development / deployment environments
    - Mobile application gateways

  – Software technology to transfer:
    - Software security frameworks, risk-based authorization technology, risk communication, User Interface, biometric fusion

Contact Information

Larry Koved
koved at us.ibm.com

IBM T. J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598

http://researcher.watson.ibm.com/researcher/view.php?person=us-koved

