Usable Multi-Factor Authentication and Risk-Based Authorization

IBM T.J. Watson Research Center
Larry Koved

December 18, 2014
Team Profile

IBM 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, cloud, cryptography and network

IBM has a world wide research team on security and privacy topics

Dr. Pau-Chen Cheng
Risk Based Access Control

Larry Koved
Identity & Data Security

Dr. Nalini Ratha
Multi-Factor Biometrics

Dr. Kapil Singh
Mobile & Web Security

Cal Swart
HCI & Risk Perception

Dr. Shari Trewin
HCI & Risk Perception

Diogo Marques
Intern, Risk Perception
Customer Need: Mobile Authentication

Who is stealing your $$ and data?

Valuable information and assets are at risk!

- IDC: Tablet purchases to exceed total PC purchases by YE 2015
- User interaction time < 1 minute
  - 15%+ time spent on authentication
- User frustration with strong passwords
- Mobile devices == identity?
  - App caches user credentials
- eWeek: 40% of organizations lost critical business data from mobile devices!
- AlixPartners: Mobile banking adoption to reach 50% in 2016. Is a key factor when switching banks.
Approach: Mobile Context Awareness, Risk Assessment and Multi-Factor Authentication

Expected Time & Location: customized to your schedule

Context aware – in your car

Recognize unfamiliar environment ➔ other people present

Senses loss of device control ➔ session lockout
Objective: Based on context, "authenticate just enough" to accommodate user preference and (situational) impairments.
Benefits

- Authenticate the user, not the device
- Authenticate just enough, based on context and risk, to accommodate situational impairments and user preferences
- Use what you are (biometrics), what you know, and what you have (mobile device)
- Estimate loss of possession / device control
  - “log out” the user / device
  - Force re-authentication to reduce risk and increase security
- Reduce authentication burden when behavior is “normal”
  - More authentication when risk is higher, including under “abnormal” conditions
Competition: Current Mobile Authentication

- **Passwords & PINs**
  - Memory recall
  - Entry on small / tiny keyboards, weaker password rules
  - Interrupts short term memory

- **Contextual factors are ignored**
  - The environment in which the activity is taking place
  - Unattended device can be misused

- **Mobile device centric solutions**
  - Built-in fingerprint / face / voice
  - Network-based authenticators

- **Biometrics – single / multi modal**
  - Single factor can be relatively weak
  - Non-zero false accept rate
  - Situational impairments
  - Niche vendors
  - Usually device-centric
    - Complete trust in the device
    - Ignores the location of the sensitive assets – the cloud!

- **2-Factor authentication**
  - Entry on small / tiny keyboards
  - Subject to social engineering
  - Another object to lose
  - SMS eavesdropping
Status: System Proof of Concept

Mobile Device
- Mobile Apps
  - Customizable User Interfaces
  - Client Authentication Services
    - Client Framework
      - Security Lib
      - Bio Lib
      - Context Lib
      - OOBAC Lib
      - Presence Lib
- Mobile Authentication Services
  - Reverse Proxy
  - Mobile Services
  - Mobile Apps
  - Mobile Authentication Services
    - Multi-User / Multi-Device Coordination Services and Administration
    - Risk-Based Authorization
    - Risk Assessment
      - Content Sensitivity/Value
      - Context Evaluation
      - User Presence Detection
    - Biometric Services – Enrollment & Verification and Fusion
      - Biometric Fusion
      - User Presence Detection
Status: Risk-Based Authorization

Incremental learning based
Time & Location Anomaly Scoring

Framework for fuzzy composition of anomaly scores and risk assessment
Status: Mobile Security Risk Perception and Communication

- Anti-phishing: User-selected image
- Insider threat awareness
- Prompt with risk communication
- Risk indicator. Tap for explanation

- Risk-based Authentication
- IT Company Employee
- Personal Financial

- Information Loss
- Observation
- Device Loss/Theft/Attack
- Network

- Situation

- Graph showing percentage of risk levels at different locations:
  -在北京
  -餐厅
  -繁忙
  -街头
  -一个人
  -自己的办公室
  -安静

12/12/2014
CYBER SECURITY DIVISION 2014 R&D SHOWCASE AND TECHNICAL WORKSHOP
Status: Multi-Factor Biometrics

- Commercial Biometric Engines
- Enrollment & Verification

Strong Biometric Authentication

- Face
- Voice
- Fingerprint

Biometric Fusion Scoring

Identity Confidence Score

Preventing Replay Attacks Through Information Hiding

Mobile Client

1. Resource Request
2. Biometric Authentication Challenge with Random Token
3. Biometric signal with hidden Random Token
4. Return requested resource if Random Token successfully extracted. Otherwise flag as replay or impersonation attack.

Authentication & Authorization

Face Voice Fingerprint

Biometric Fusion Scoring

Identity Confidence Score

Strong Biometric Authentication
Status: Academic Activities, Patents

- Workshops organized
  - RP-IT 2013 – Risk Perception in Information Technology at the Symposium On Usable Privacy and Security

- Invited Talks and Panels
  - University College London – Risk Perception
  - Cornell Tech – Risk Perception
  - Global Identity Summit – Biometric Fusion
  - Voice Biometrics Conference SF – multi-factor authentication

- Papers
  - Practical Context-Aware Permission Control for Hybrid Mobile Applications, RAID 2013
  - Perceived Security Risks in Mobile Interaction, RP-IT 2013
  - Practical Out-of-Band Authentication for Mobile Applications, Middleware 2013
  - Improving Usability of Complex Authentication Schemes Via Queue Management and Load Shedding, WAY 2013
  - Cui Bono? An Experiment in Re-Framing Authentication Decisions. In submission.

- Patents and Inventions
  - 3 patents applications filed
  - 6 invention disclosures filed
Transition Activities

• Collaborating with IBM Software Group to bring a commercial offering to market

• Four use cases targeted:
  – Single mobile app bundled with integrated multi-factor authentication, allowing the adopter to fully control the user experience
  – Separate authentication app, allowing the adopter to secure both mobile & non-mobile apps without or minimal app mods (security unaware)
    • Authentication app launched via PushNotification (unaware)
    • Web and Internet of Things (IoT) authentication (unaware)
    • Authentication app launched by the business app (minimal mods)

• Ongoing discussion with customers in multiple business sectors
  – Strong interest in all of the above use cases

• Currently validating through two customer proof of concepts engagements
Lessons Learned

• Integration with existing authentication services:

  • Three constituencies: End Users, Programmers, Administrators
    – Ease of use for all three are critical success factors

    – Four use cases of importance supporting mobile, web and Internet of Things

    – Real network security services have very complex integration requirements
      • Substantial legacy systems support requirements

• Communication of the benefits of authentication did not increase user acceptance

• Business development personnel essential for identifying and working with prospective customers.
Contact Information

Larry Koved

koved at us.ibm.com

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