Usable Multi-Factor Authentication and Risk-Based Authorization

Cyber Security Division
2012 Principal Investigators’ Meeting

October 11, 2012

Larry Koved, Principal Investigator
Research Staff Member
IBM T. J. Watson Research Center
koved@us.ibm.com
914-945-1745

This work is supported by a grant from the Department of Homeland Security under contract FA8750-12-C-0265

© 2012 IBM Corp.
Introduction

- TTA #3 Usable Security

- Interdisciplinary Team – HCI, Security, Biometrics, Systems
  - Larry Koved, Information Security, authorization, HCI, middleware
  - Dr. Rachel Bellamy, Software Productivity, 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, Software Productivity, mobile and web HCI
  - Dr. Shari Trewin, Software Productivity, HCI, accessibility
Emerging Security Environment

Mobile smartphones are increasingly used as authentication devices

Payments and micro-payments through mobile devices is an emergent phenomenon

Personal = Business
BYOD

• Enterprise enablement of mobile devices requires “strong passwords”
• Enterprise passwords are
  • Hard to enter on mobile devices
  • Disruptive to short term memory
• Strong dissatisfaction with enterprise authentication requirement for mobile
Current Mobile Authentication and Authorization Environment

Two factor security tokens are under attack; not an integral part of the mobile environment

Mobile smartphones are increasingly used as authentication devices and payment devices
- Retailer, banks, lock companies, etc.
- In use around the world

(examples omitted)

**Increased loss potential of mobile devices enhances need for strong authentication**

**Key issues with Mobile Authentication**
- **Weak Single Factor Authentication**
  - Strong passwords hard to enter

- **Weak Protection of Credentials**
  - Smartphones unlockable in < 2 minutes
  - Credentials in the clear / decrypted

- **Contextual Risk not considered**
  - Location, environment
  - Device and configuration

**Emergent Mobile Biometrics Market**
- **Apple**: Acquired AuthenTec
  - rumored biometric API

- **Android**: Ice Cream Sandwich
  - face recognition engine

- **Assorted Small Biometrics Vendors**
Representative Usage Context

Enterprise Identity and Access Management (IAM) Lifecycle*

**Enrollment**
- Reputation, portability
- Biometrics
- Drivers license, passports, etc.

**Proofing**
- Background identity and reputation checks
- Document security
- Identity analytics
- Biometrics

**Credentialing**
- Logical credentials (e.g., OTP, public certificates)
- Physical tokens (e.g., id cards w/chip)
- Smartcards

**Usage**
- Authentication
- Trust and reputation
- Logical access control
- Physical access control
- Enterprise identity mgmt
- Identity federation & delegation
- Usage monitoring

* A simplified view
Representative Target Integration Points

- Firewall
- Reverse Proxy
- Mobile Application Servers
- Authentication and Authorization Services
- Web Applications
- Network Admission Control
- 802.11
- BT
- 2/3/4G

© 2012 IBM Corp.
Usable mobile authentication & authorization
Three Legged Approach

Risk-Based Authorization

Authentication Context

Environmental Situation

Trust Centric

Behavior History

Security Responses / Authentication Confidence

Multi-Factor Biometric Fusion

Authentication Challenges and Policies

Environmental Constraints

Limited Working Memory

Usable Security

© 2012 IBM Corp.
Proposed Solution

Sensor Acquisition

User Privacy Preferences
- Web Browser
- Mobile Application

Secure Authentication Framework

Secure Channel

Usability Requirements

Biometric Fusion
Risk Authorization Evaluation
Multi-factor Authentication

Risk Score
Policies
Services Approved

Server
<table>
<thead>
<tr>
<th>Topic</th>
<th>Problem</th>
<th>Challenge</th>
<th>Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Perception</td>
<td>People's perception of risk does not match system risk</td>
<td>How do we align user perception of risk with system risk?</td>
<td>Taxonomy of perceived risk and validation studies</td>
</tr>
<tr>
<td>Reducing Authentication Friction</td>
<td>Authentication interrupts task flow and is slow</td>
<td>How do we reduce / eliminate challenges requiring explicit user action?</td>
<td>Predictive modeling and acquisition scheduling of authentication challenges</td>
</tr>
<tr>
<td>Strong Authentication</td>
<td>Creating strong identity from weak signals</td>
<td>How can poor quality biometric samples be used to get strong identity?</td>
<td>Robust policy-driven fusion based on weak mobile device biometric signals</td>
</tr>
<tr>
<td>Secure Client-side Frameworks</td>
<td>Secure and reliable interaction on the client side</td>
<td>Can we protect the security and integrity of user inputs for untrusted application?</td>
<td>Secure system and application design patterns and implementation</td>
</tr>
<tr>
<td>Risk-based Authorization</td>
<td>Authentication and authorization are not binary decisions</td>
<td>Can we provide access control that maximizes information sharing while keeping risk in check?</td>
<td>Need vs. risk tradeoff “learning” analytics based on history, situation and context</td>
</tr>
</tbody>
</table>
## Schedule and Milestones

<table>
<thead>
<tr>
<th>Topic</th>
<th>1Q / 2Q</th>
<th>3Q / 4Q</th>
<th>5Q / 6Q</th>
<th>7Q / 8Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Perception</td>
<td>Psychometric study design</td>
<td>Study report &amp; recommend</td>
<td>Report on eval. of system</td>
<td>Report on eval of system</td>
</tr>
<tr>
<td></td>
<td>Perceived risk taxonomy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reducing Authentication Friction</td>
<td>User modeling</td>
<td>Usable interface</td>
<td>Predictive analytics</td>
<td>Fusion Policy</td>
</tr>
<tr>
<td>System integration and validation</td>
<td>System design</td>
<td></td>
<td>Integrate with application(s)</td>
<td>Demonstrate full system</td>
</tr>
<tr>
<td></td>
<td>Initial system prototype</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Deliverables

- Demonstrate usable mobile authentication and authorization system comprised of:
  - User interface components that effectively communicate authorization risk
  - “Low friction” authentication components minimizing disruptive authentication challenges
  - Secure client-side components for secure biometric and non-biometric authentication
  - Client-side multi-sensor data acquisition (camera, microphone, location, …), with user preference specification, organization policies, and enforcement
  - Anti-phishing framework
  - Risk-based authorization learning-based analytic algorithms
  - Environment sensing and biometric quality assessment
  - Biometric fusion and policy algorithms

- Technical reports:
  - User perception of authentication / authorization risk
  - Heuristic evaluation of early mockups with design recommendations
  - Summative evaluation of running system
  - Offline evaluation of the use of context, history and situation to identify risk factors and assess transaction risk
  - Online effectiveness of authentication challenge generation when performed in consultation with the multi-factor fusion algorithm
Targeted Publication Areas

- HCI / UX
  - Mobile authentication and authorization
  - Low friction authentication
- Risk perception
  - Psychometrics of mobile IT security risk perception
  - IT risk communication
- Risk-based authorization
  - Historical, Contextual and Situational risk authorization
  - Mobile risk-based authorization
- Mobile security
  - Secure mobile frameworks
  - Security risk indicators
- Biometrics
  - Multi-factor biometrics for mobile devices
  - Biometric fusion
  - Biometric fusion policies

- ACSAC 2012 paper:
  - Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption
Technology Transition Plan

- Target integration points:
  - Web-based, application independent, authentication and authorization for mobile device endpoints
  - Network access control (NAC)
  - Application-specific authentication and authorization

- Potential commercial entry points into the market:
  - IBM’s web (reverse) proxy – authentication & authorization
  - Addition or substitute for existing token-based authentication and authorization
  - Application-specific integration (e.g., toolkit)

- Potential open source contributions:
  - Mobile application development frameworks (e.g., PhoneGap)
  - Server-side authentication and authorization frameworks (e.g., Apache Geronimo)
Technology Transition Plan

- Use DETER?
  - To run usability experiments with *face validity*, we will be using corporate applications on corporate and public networks to enable larger numbers of mobile devices to have access to the sensitive applications and data. This project does not need the services and capabilities offered by DETER.

- Use PREDICT?
  - We will investigate whether PREDICT datasets are useful for modeling some aspects of user and/or device behavior.
BAA Number: Cyber Security BAA 11-02
Title: Usable Multi-Factor Authentication & Risk-Based Authorization

Offeror Name: IBM Research

Operational Capability
- Performance targets: Usable security, specifically easy to use adaptive strong user identification through multi-factor biometrics. Advances in biometrics on commodity devices, well integrated into well designed interaction with mobile devices.
- BAA goals: Address usable security through interface design and evaluation meeting strong authentication objective.

Proposed Technical Approach:
- Addresses usable strong identity of people using mobile devices for high value and/or high risk transactions.
- Design and implement multi-factor biometrics, risk-based authorization and usability evaluation.
- Build on existing biometric algorithms and Risk-based authorization research.
- Other elements of proposal are new.
- Extends existing enterprise-grade identity and access control offerings.

Milestone Decision Point: UI design, multifactor biometrics, mobile & server integration

Deliverables: (1) Usability design & evaluation (2) Biometric fusion (3) Multi-factor authentication (4) Risk-based Authorization (5) Mobile & server middleware

Period of Performance: 2 years

Offeror: IBM Research
Point of Contact: Larry Koved, Yorktown Heights, NY 10598. Phone: (914) 945-1745 Email: koved@us.ibm.com