Keystroke Authentication

It's All in How You Type

John C. Checco, CISSP

Overview

What is Keystroke Biometrics

How Effective is Keystroke Biometrics

Advantages of Keystroke Biometrics

Markets for Keystroke Biometrics

Future for Keystroke Biometrics

$$\frac{1}{\sqrt{(\ell+m)(\ell-m+1)}}\frac{1}{\sin^{m-1}\theta}\frac{\partial}{\partial(\cos\theta)}\sin^{m}\theta e^{-i\varphi}Y_{\ell}^{m}$$

What is Keystroke Biometrics

Biological Measurements

- Physical aspects of a person that determine identity
- Static measurement
  - Absolute match
- Quality of measurement is only variable by the quality of the capture device
- Examples:
  - DNA
  - Iris/Retina Scan
  - Fingerprint
  - Hand Geometry / Vein Structure
  - Facial Recognition

$$Y_\ell^{-\ell}(\theta,\varphi), Y_\ell^{-\ell+1}(\theta,\varphi), \cdots, Y_\ell^{-1}(\theta,\varphi), Y_\ell^{0}(\theta,\varphi), Y_\ell^{1}(\theta,\varphi), \cdots, Y_\ell^{\ell-1}(\vartheta,\varphi), Y_\ell^{\ell}(\theta,\varphi)$$

What is Keystroke Biometrics

Behavioral Measurements

- Characteristic traits exhibited by a person that can determine identity
- Dynamic measurement
  - Confidence match
- Quality of measurement varies by behavioral and other external factors
- Examples:
  - Keystroke Heuristics
  - Handwriting Analysis
  - Voice Verification
  - Language Removal Identification

$$\langle L_{\pm}^{k} Y_{\chi}^{m}, L_{\pm}^{k} Y_{\chi}^{m} \rangle = [\lambda - (m \pm (k-1))\,(m \pm k)] \cdots [\lambda - m(m \pm 1)] \langle Y_{\chi}^{m}, Y_{\chi}^{m} \rangle$$

What is Keystroke Biometrics

Pattern exhibited by an individual using an input device in a consistent manner

- Input Device
  - Keyboard, Keypad, Stylus, …
- Raw measurements available by the input device
  - Dwell time
  - Flight time
  - Absolute versus Relative timing
- Factors
  - Timing / Cadence
  - Content
  - Spatial Configuration
  - Consistency (as well as consistent inconsistencies)
- Signature Processing
  - Deduction of key factors from an arbitrary data stream
  - Robotic vision, Economic trending, Quantum physics

$$L_{\pm}Y_{\ell}^{\pm\ell} \equiv \pm e^{i\phi}\left(\frac{\partial}{\partial\theta} \pm i\frac{\cos\theta}{\sin\theta}\frac{\partial}{\partial\varphi}\right)P_{\ell}^{\pm\ell}(\theta)e^{\pm i\ell\varphi} = 0$$

What is Keystroke Biometrics

History of the World, Part I

- **1979**:
  - Technology originally developed by SRI International.
- **1984**:
  - National Bureau of Standards (NBS) study concluded that computer keystroke authentication of 98% accuracy.
- **1988**:
  - Keystroke authentication hardware device passes NIST Computer Security Act of 1987.
- **2000**:
  - Keystroke authentication passes the Financial Services Technology Consortium (FSTC) / International Biometric Group (IBG) Comparative Testing program.
- Patents (partial list):
  - 4621344, 5557686, 4805222, 4962530, 4998279, 5056141

$$\sum_{\ell=0}^{\infty}\sum_{m=-\ell}^{\ell} Y_\ell^m(\theta,\varphi)\overline{Y_\ell^m(\theta',\varphi')} = \frac{\delta(\theta-\theta')}{\sin\theta}\delta(\varphi-\varphi')$$

How Effective is Keystroke Biometrics

- Fingerprint
  - FAR= ~0%
  - FRR= ~1%

- **Keystroke Biometrics**
  - FAR= ~0.01%
  - FRR= ~3.0%
    - Manufacturer recommended settings
    - Variable (application-defined)

- Facial Recognition
  - FAR/FRR vary according to: compression, distance, illumination, media, pose, resolution, and other temporal factors.

- Voice Recognition
  - FAR= ~1.6%
  - FRR= ~8.1%

$$H_\nu(kR)e^{i\nu(\Omega-\theta_0)} = \sum_{m=-\infty}^{\infty} J_m(kr_0)H_{\nu+m}(kr)e^{i(\nu+m)(\theta-\theta_0)}$$

How Effective is Keystroke Biometrics

What If ….

- *I injure my hand?*
  - How many people have you met that have had hand injuries?
  - How many people have you met that forgot their password?
- *I enrolled on one keyboard and want to login on another?*
  - Tactile versus membrane
  - Full-size versus compact
  - Key-character layout
- *My connection is hijacked and someone replays my keystrokes?*
  - Fraud detection methods vary by manufacturer
- *I have a bad day?*

$$0 \leq \int_0^{\pi} \int_0^{2\pi} |L_{\pm} Y_{\lambda}^{m}(\theta,\varphi)|^2 \sin\theta d\theta d\varphi$$

Advantages of Keystroke Biometrics

Technology Advantages

- Performance:
  - Inherently narrows the identification pool to achieve lower FAR/FRR
- Portability:
  - Users are not limited to individual or specific workstations
- Flexibility:
  - Dynamically managed threshold for acceptance
- Security:
  - Constant biometric refinement of templates over time
- User Acceptance:
  - Non-invasive capture
  - Support for invisible (background) enrollment
  - Works better with pass phrases familiar to the user
    - translation: passwords *can* be easy to remember
- Paradigm:
  - Only solution that provides for limited liability risk mitigation.
  - Capabilities based policies, not simply role based

$$[\nabla^2 + \ell(\ell+1)]Y_\ell^m(\theta,\varphi) = 0$$

Advantages of Keystroke Biometrics

Implementation Advantages

- Deployment / Maintenance:
  - No physical hardware to install or maintain
  - No manpower needed on client-side deployment for installations or upgrades
- Coverage:
  - Support for remote access and telecommuting
  - Software-only components allow integration into any software solution
- Policy Management:
  - Secondary authorization does not change current policies
  - Application and/or user managed levels of security
- Audit Control:
  - Promote proper use of existing licensing
  - Logging of biometric access creates better forensic evidence
- Exit / Override Strategies
  - No additional resources needed to override or temporarily disable biometric.
  - No invasive exit strategy …. Just turn off server-side secondary authentication process.

$$\|L_+ Y_\ell^\ell\|^2 = [\ell(\ell+1) - \ell(\ell+1)]\|Y_\ell^\ell\|^2$$

Markets for Keystroke Biometrics

Network / Intranet Security:

- Single Sign-on Solutions
- RADIUS
- Corporate Application Access
- xFS Volume Protection
- Document Control Management
- Corporate Internet Access

$$\frac{\partial^2}{\partial\theta^2}+\frac{\cos\theta}{\sin\theta}\frac{\partial}{\partial\theta}+\frac{1}{\sin^2\theta}\frac{\partial^2}{\partial\varphi^2} \stackrel{?}{=} e^{i\phi}\left(\frac{\partial}{\partial\theta}+\frac{i}{\sin\theta}\frac{\partial}{\partial\varphi}\right)e^{-i\phi}\left(\frac{\partial}{\partial\theta}-\frac{i}{\sin\theta}\frac{\partial}{\partial\varphi}\right)$$

Markets for Keystroke Biometrics

Asset Identification:

- Online Training / Testing
- Document Signing
- Software Licensing and Registration

Personal Information Security:

- Primary Authorization for individual document encryption
- Secondary Authorization mechanism for online purchases
- Secure Laptop Access

$$\nabla^2\psi = \frac{1}{r^2}\,\frac{\partial}{\partial r}r^2\frac{\partial\psi}{\partial r} + \frac{1}{r^2}\left[\frac{1}{\sin\theta}\,\frac{\partial}{\sin\theta}\sin\theta\frac{\partial}{\partial\theta} + \frac{1}{\sin^2\theta}\,\frac{\partial^2}{\partial\varphi^2}\right]\psi .$$

Future for Keystroke Biometrics

Consumer Market:

- PDA / Tablet / Stylus Input
- RIM
- ATM
- Cell phones
- Home Security Access Pads

$$\int_R \int \left[\psi(\vec{x})(-)\delta^2(\vec{x}-\vec{x}_0) + G(\vec{x};\vec{x}_0)f(\vec{x})\right] d^2x = \oint_{\partial R} (\psi\vec{\nabla}G - G\vec{\nabla}\psi)\cdot\vec{n}\, ds\ .$$

Questions and Comments

Commonly Asked Questions:

- Can keystroke biometrics determine if an employee is incapacitated due to inebriation or drug abuse?
- How does keystroke biometrics protect against “Cyrano de Bergerac” breaches?

$$\sum_m \int_0^\infty k\,dk \int_0^{2\pi} d\alpha J_m(kr) i^m \frac{e^{im(\theta-\alpha)}}{2\pi} \sum_{m'} J_{m'}(kr_0) \frac{e^{-im'(\theta_0-\alpha)}}{2\pi} (-i)^{m'}$$

Q.E.D.

John C. Checco
President, bioChec™
Checco Services, Inc.

John.Checco@bioChec.com
http://www.bioChec.com

Stony Point, New York
1-845-942-4246

$$\sum_{m=-\infty}^{\infty} \frac{1}{2\pi} \int_0^{\infty} k dk J_m(kr) J_m(kr_0) e^{im(\theta-\theta_0)} .$$