ARGHHH!!

Understanding frustration with biometric authentication

Michael Brooks[1], Michael Toomim[2], Cecilia Aragon[1]

University of Washington HCDE[1], CSE[2]

What is biometric authentication?

Identity verification from physical or behavioral markers.

Fingerprints, irises, voice, faces, ears, hand veins, gait, keystrokes, and signatures

Growing popularity: high security, workplaces, computers, homes, laptops with fingerprint readers or face recognition, large-scale deployments like US-VISIT and Aadhaar

Advantages of Biometrics

More directly identifies people

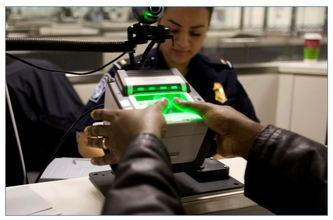
Doesn't use secret knowledge (passwords) or tokens (keys)

Sometimes more difficult to steal than passwords

*Biometrics are error-prone and **annoying***

Systems sometimes fail to recognize people:

- Sensor errors
- Marker presence varies between people
- Individuals vary over time



Several biometric systems: a fingerprint reader (top left); an iris scanner (top right); a person's biometric data being recorded as part of the US-VISIT program (bottom left); a laptop fitted with a fingerprint reader (bottom right).

Two key performance metrics

False Acceptance Rate

How often individuals are admitted by the security system when they actually should not be

High FAR indicates security vulnerability

False Rejection Rate

How often the system wrongfully denies access to legitimate users

The higher the FRR, the more annoying

New metrics are needed

What is the user's experience?

Too annoying: people often give up on biometrics

Impact of errors on UX still poorly understood

Environmental factors

Testing done in carefully controlled settings

In reality, many factors reduce system performance:

- Humidity, temperature, lighting, background activity

Performance varies by individual

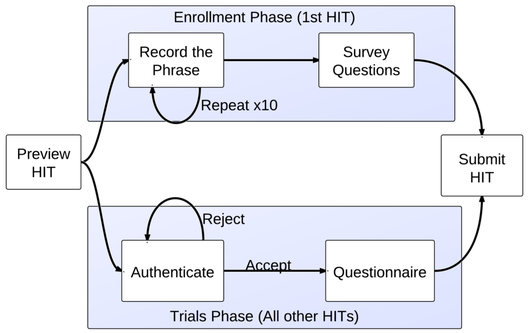
A vendor might advertise an FRR of 5%, but errors are not evenly distributed over users.

Work in progress: Mechanical Turk study

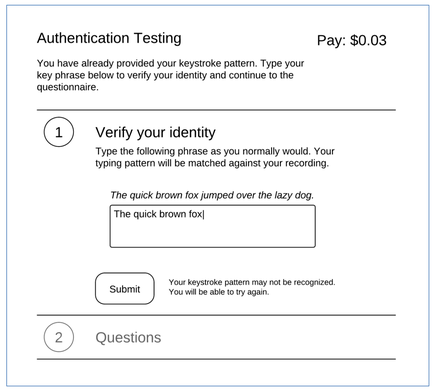
Developing a Mechanical Turk task that simulates biometric authentication

Uses keystroke biometrics

People will eventually decide that the payment is not enough, and stop completing tasks



This diagram shows the process that Mechanical Turk workers will go through in our planned experiment.



A mockup of a human-intelligence-task (HIT) that will be posted to MTurk. The turker must type the phrase in order to continue and receive the reward.

When will people stop putting up with it?

Key experiment design questions:

- Choice of "primary task"
- Time between tasks
- Amount of pay
- How to control rejection and acceptance

Research Goals

Clarify relationships between failures and user acceptance/satisfaction.

Find out how people react to authentication errors

Develop new experience-based performance metrics for biometric authentication systems.

Acknowledgments and Contact Information

This research is supported by the National Institute of Standards and Technology.
For more information, contact Michael Brooks at mjbrooks@uw.edu or visit http://depts.washington.edu/sccl

Scientific Collaboration & Creativity Lab

HCDE Human Centered Design & Engineering

dub

University of Washington