Speaker Authentication: Biometrics & Security

Mobile Authentication Ecosystem

- **FIDO Alliance**
  - Server
  - Client—Mobile Devices
    - Risks of Mobile Device
      - Rooted? Jail-broken?
      - Key Characteristics of Mobile Device
      - Location
  - Authenticator
    - User Name, Password, Knowledge Qs
    - Biometrics: voice, vision, finger print, pattern, PIN, key stroke, new technology
- **Reduces Cost & Risk**

Authentication Trends

- **Biometrics at Tipping Point**
  - Mobile Device Authentication
  - Moving into retail/consumer Password/PIN
  - Multifactor Biometric Authentication
  - Industry Specific Biometric Solutions
- **Two Factor Authentication**
  - Something User **HAS**
    - phone, token
  - Something User **KNOWS**
    - user name, password, knowledge Qs
  - Something User **IS**
    - biometric—voice, face, iris, fingerprint, EKG, etc.

Authentication

- **Industry Standards**
  - PIN / Passwords
- **Biometric Options**
  - Finger Print
  - Iris Recognition
  - Voice Recognition
  - Face Recognition
  - Keyboard Dynamics
  - Heart / EKG
  - Gesture Recognition
  - Gait Recognition
  - DNA
- **Non-Biometric Options**
  - Patterns
- **Each solution has issues when used in isolation**

sensory

Security

Requirements for Authentication Solutions

- **Frictionless**
- **Secure**
- **Integrate with Security Ecosystem**
- **Must Work Reliably in Real World**
- **Maximize Adoption**
  - Broadest Device Base
  - Fast & Easy to Enroll / Setup / Use
    - Large percentage users don't lock their mobile devices. Why? Hassle.
    - If authentication is slow or challenging to use, people won't use
- **Affordable**

Authentication
PINS & Passwords

- **PINS & Passwords**
  - Ubiquitous
  - The 'Problem'
- **Challenges**
  - Single Point of Failure if PIN/Password is compromised
  - Difficult to remember
  - Re-Used
  - Infrequently changed
  - Susceptible to phishing

1. **123456** (Unchanged)
2. **password** (Unchanged)
3. **12345678** (Up 1)
4. **qwerty** (Up 1)
5. **12345** (Down 2)
6. **123456789** (Unchanged)
7. **football** (Up 3)
8. **1234** (Down 1)
9. **1234567** (Up 2)
10. **baseball** (Down 2)

Authentication Iris

- **Challenges w/ Iris**
  - Intrusive
  - Long enrollment
  - Challenging
    - poor lighting
    - Glasses / Sunglasses
  - If copied, hard to change
    - you only have two eyes
  - Difficult to use while moving (walking, riding, running, etc.)

Authentication Finger Print

- **Challenges with Finger Print**
  - Hardware Availability on Mobile devices
  - Expensive, requires additional hardware
  - High rate of false rejects – frustrating to user
    - Sweat, dirt, grease, cuts, etc.
    - If copied, hard to change
  - Breakable
    - Mythbusters

Voice and Face

- **Challenges with either as solo solution**
  - Voice
    - doesn't work in high noise
    - User may not want to use in public
    - Voice changes over time or with colds, etc.
  - Face
    - Challenging in low light conditions
    - Angle between face - device all can effect
- **Together Voice and Face can solve these issues**

Voice and Face for Authentication

- **Hardware**
  - Microphone + Selfie Cam
- **Face**
  - Something the user 'IS'
- **Voice**
  - Something the user 'KNOWS' + 'IS'

Voice and Face for Authentication

- **Fusion of Voice and/or Vision**
  - Two complimentary biometrics
    - More environmentally robust
    - More accurate across all conditions
    - Improve convenience
  - Match Security Level With Use Case
    - Voice
    - Face
    - Either / Or
    - Both for highest security
- **Highly Secure + Frictionless**
- **Multifactor Biometric Authentication**

TrulySecure

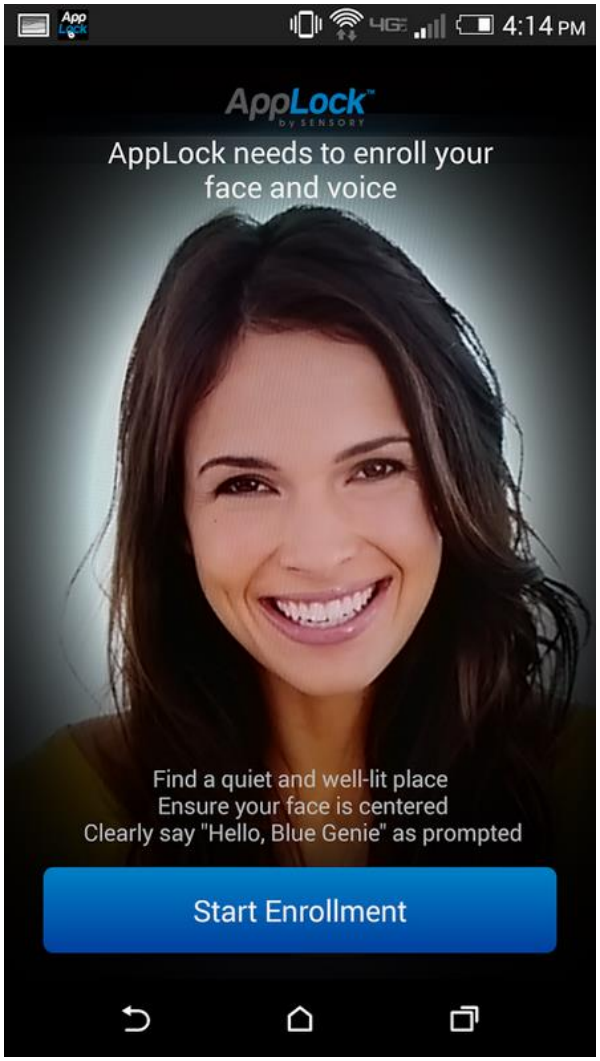
- **Easy to Use and Enroll**
  - Face & Voice Enrolled Simultaneously
    - ~ 10 seconds
  - Fast authentication <2 seconds
  - NO need to roll eyes, move your face around from side to side, up and down
  - On mobile device, one hand ultra convenient enroll and use

TrulySecure

- **Adaptability**
  - Adaptive learning with face recognition
    - Glasses, sunglasses, strange angles, etc.
    - With each adapt, overall use improves and FR's reduce
- **Changeability**
  - Voice password easily changed
- **100% On-Device Solution**
  - FAST
  - No biometric information stored on device
    - Mathematical Abstracted Templates
  - No information sent to cloud
- **Works In Real World**
  - See for yourself – search AppLock by Sensory on Google Playstore
- **Works with Security Architecture**
  - FIDO Certified Authenticator (UAF)

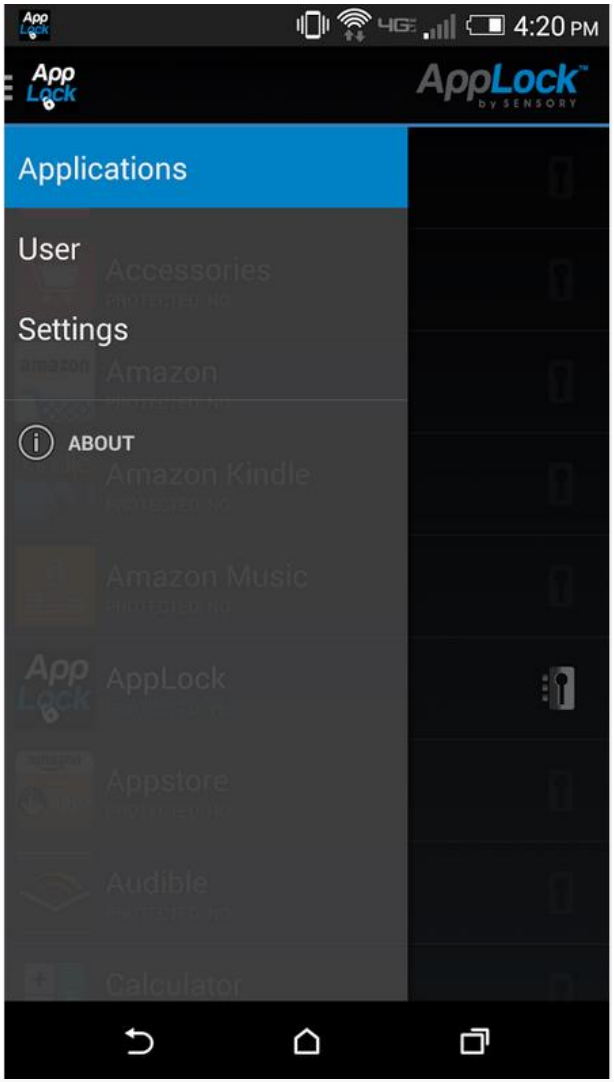
Truly Secure™ Authentication

AppLock
Example of TrulySecure

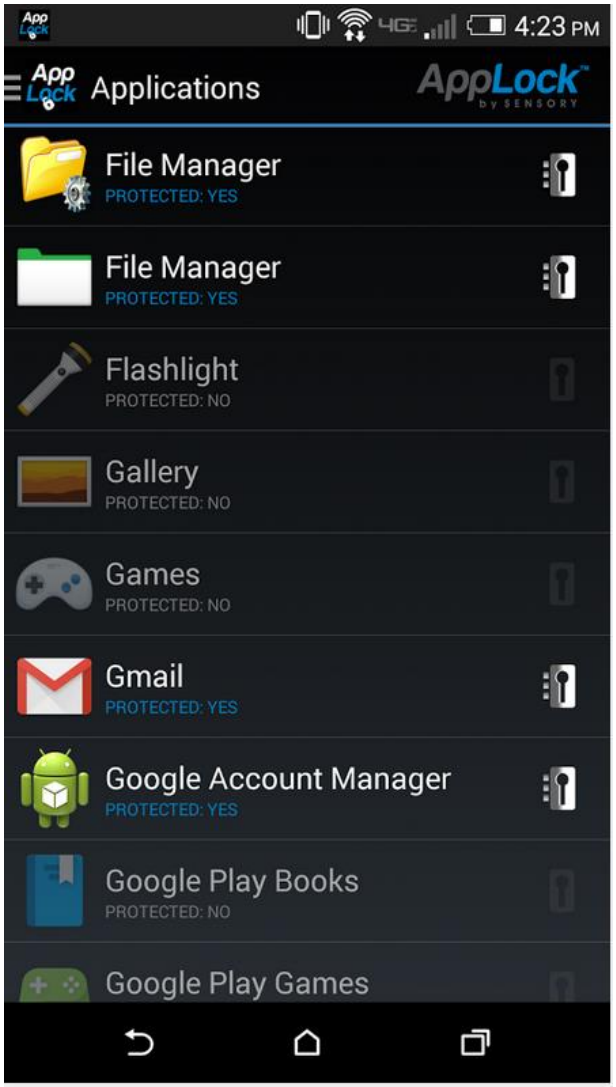


- **Enroll face and voice at the same time**
- **User can enroll with a fixed passphrase or user defined passphrase**

AppLock

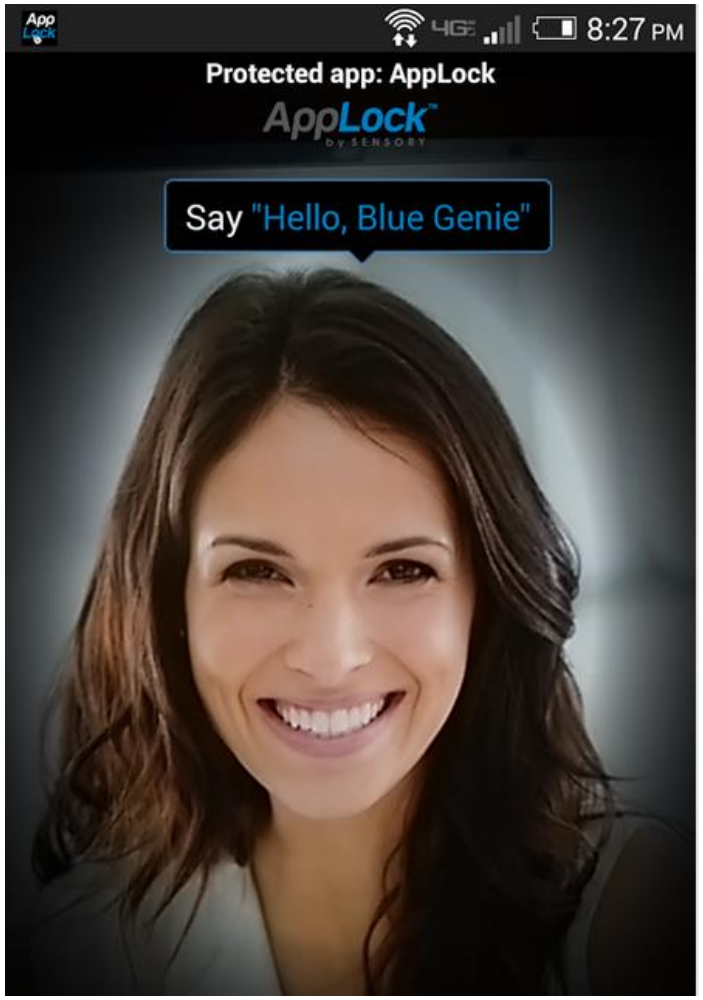


User selects apps and sets security level



Applock

- Voice password
- Facial recognition
- Either / Or
- Both



TrulySecure DEMO


Спасибо
Gracias
شكرا
Obrigado
Спасибо
Dank U
Grazie
Ευχαριστώ
Danke
Merci
Obrigado
Diolch
Thank You
Ngiyabonga
Dank U
Thank
You
Merci
Ευχαριστώ
Tack
Dziękuję
Dziękuję
Danke
Grazie
תודה
Dank U
Diolch
Grazie
Tack
Ευχαριστώ
Terima Kasih
Diolch
Gracias
Merci
תודה