

Factoring User Experience into Mobile Application Security

Sean C. Mitchem
Principal Analyst
210-522-2698
smitchem@swri.org
www.swri.org

March 27, 2012





Outline of Presentation

- ◆ Why factor in the user?
- ◆ Current User Authentication Schemes
- ◆ Mobile Device Functionality
- ◆ Concepts for New Authentication Schemes
- ◆ Final Thoughts



What's the user got to do with security?

- The purpose of securing information is to protect from access by unauthorized parties
- Information must be accessible by authorized parties or it serves no use
- Mobile devices facilitate the sharing of information between authorized parties on the go
- Mobile applications ease user access to distinct types of data
- Make user authorization too difficult and users will try to not use the application, hindering communication and productivity
- Make authorization too lax and security will be comprised





A (Frustrating) User Authentication Example

- 1st step: Access the device
 - 14+ character password
 - Pseudo-random combination
- 2nd step: Access the secure container
 - Another password
 - Can't be same as device password
- 3rd step: Utilize a user-carried token
 - Connect Bluetooth token reader
 - Select an application certificate
 - Enter a user pin (6-8 digits)
 - Pair to device by manually entering a randomly generated number from the reader



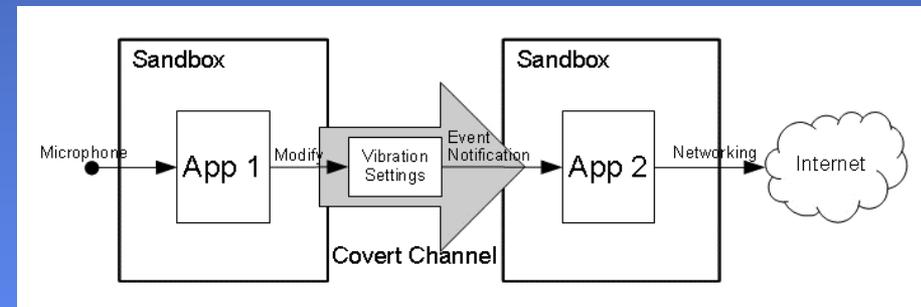
Army 04-IA-O-001 compliant passwords

tU3s*nK9qp@M4o

O4\$E^zi5L%wP9v

Mobile Applications Security

- SwRI is conducting original research into securing mobile device applications
 - Identifying the threats
 - Analyzing the OS and development models
 - Analyzing application-level process and data sharing security
 - Developing unique authentication and authorization techniques
 - Examining balance between user experience and level of security





CURRENT USER AUTHENTICATION SCHEMES



Current Methodology

- User Passwords
 - Legacy from desktop computing
 - Utilized as "seeds" for personal encryption schemes
 - Proven "uncrackable" given:
 - *Sufficient length*
 - *Use of entire character set*
 - *Separation from standard dictionary words*
- User Pins
 - Primary access method to access a general information component
 - Secondary access method for an authenticated user to access additional sensitive information
 - Numeric
 - Based on single digit combinations
 - Easily "crackable" in an off-line attack mode
- Problem with passwords on mobile devices
 - Keyboard is graphical, not physical
 - Muscle memory not usable
 - Limited display space requires keyboard switching



Keyboarding on Mobile Devices

- The Problem

- Multiple keyboard layouts required on mobile devices
- No tactile feedback to the user
- Visual cues differ between keyboards
- Easy to lose place in long, complicated passwords
- Password masking exacerbates the problem

- Result

- User frustration
- Look for “work arounds”
- Find different way to access information (desktop computer)

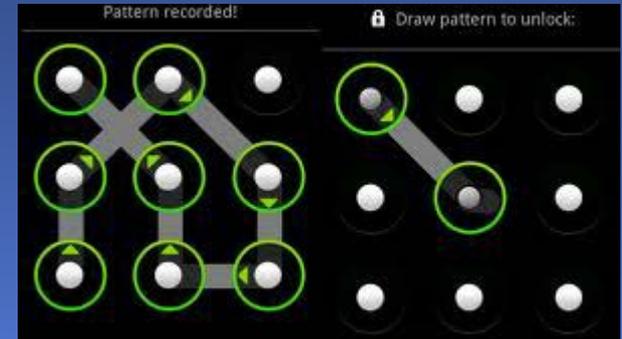
tU3s*nK9qp@M4o



Current Methodologies

- Patterns

- Underlying implementation is the same as the pin
- Easier to crack than pins
 - *The next number has to be a neighbor*
- Subject to user cognitive analysis
- Designed for "quick" access
 - *Addresses a user interface weakness*



- Picture Selection

- Recognition-based rather than recall-based
- Picture placement is randomized
- User selects their picture out of group
- Requires cognitive focus
- Equates to a 1-digit pin for the group displayed





MOBILE DEVICE FUNCTIONALITY

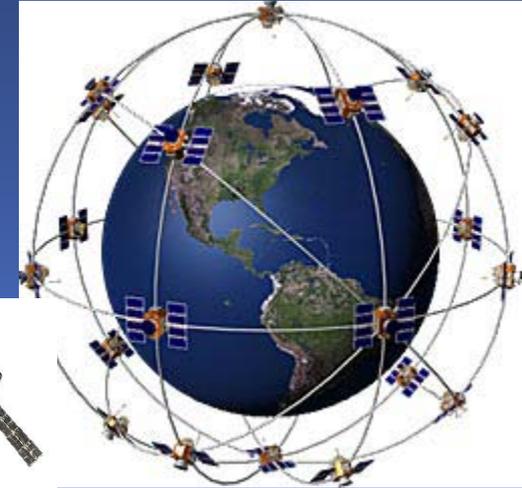
Camera and Microphone

- Many new phones now come with front and back cameras
- Several possibilities for camera recognition exist
 - Facial recognition of the user
 - *Android Face Unlock*
 - Image recognition of a token
 - QR code scanning of a token
- Voice recognition
- "Verbal" codeword
- Can be biometric or not



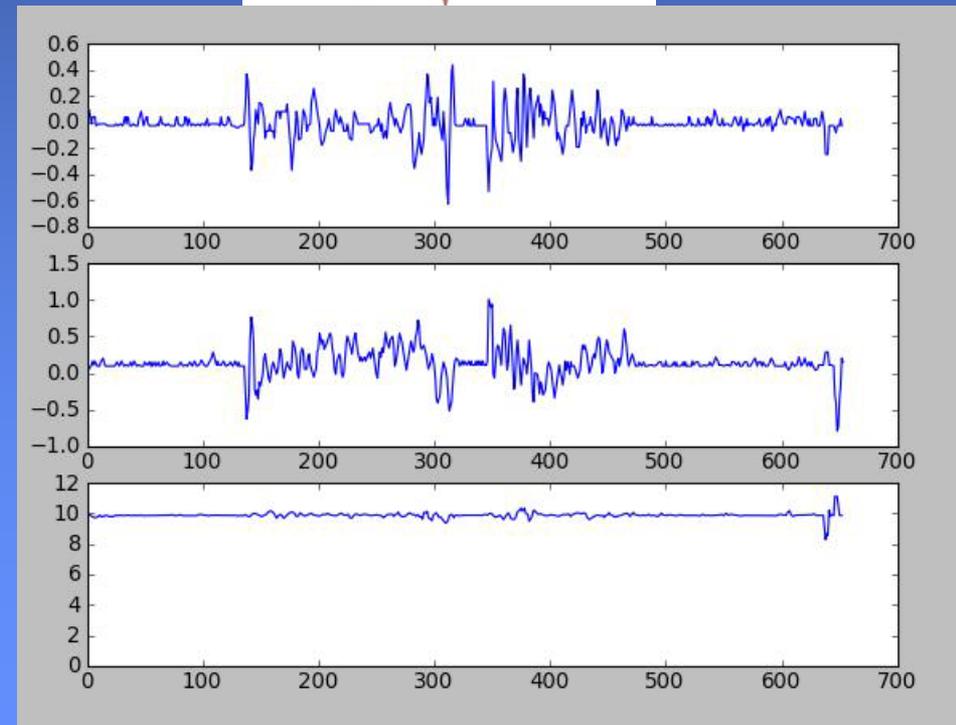
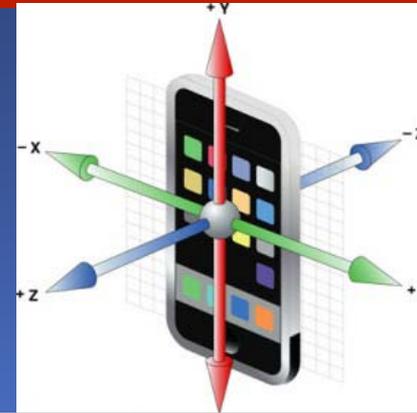
GPS

- Determination of location can be very useful in authentication
- Can automatically restrict access if access to GPS is unavailable
- Doesn't require user input to validate



Accelerometer and Gyroscope

- Accelerometer allows for determination of movement
 - Is the device traveling at odd speeds?
 - Has the device not moved for an inordinate amount of time?
 - Has the device moved since its last location was authenticated?
- Gyroscope can determine orientation
 - Left hand or right hand use?
 - Wide view or narrow view?





CONCEPTS FOR NEW AUTHENTICATION SCHEMES



Graduated Authentication Levels

Can be defined two ways:

- Requiring increasingly complex authentication as the user progresses towards more sensitive information (typical implementation)
- Providing less complex authentication based on a confidence factor that the current user is the authorized user

Pin to access device

Password to access application

Token to access sensitive content within application

User is in authorized location

Access time is in normal working hours

Workflow is appropriate for user

Require pin instead of password



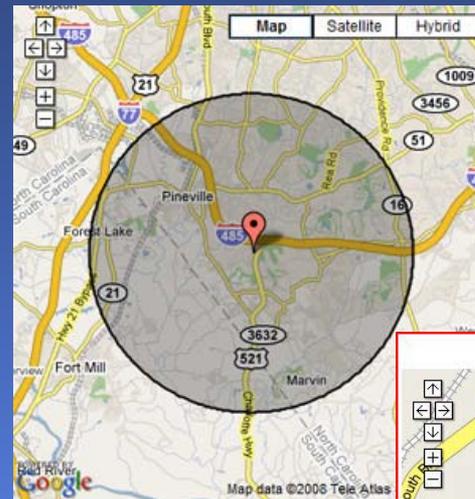
Combinations

- Multi-factor authentication
- Utilize mobile device sensors such as GPS, accelerometer, gyroscope as an authentication factor
- When confidence level drops require more complex authentication
- More combinations are possible given the devices that are a part of today's mobile devices
- For example:
 - If user enters correct 4-digit pin AND they are located within the grounds of the hospital
 - Then allow access to medical records application
 - Else If they are outside the grounds
 - Then require full strength password



Geolocation/Geofencing

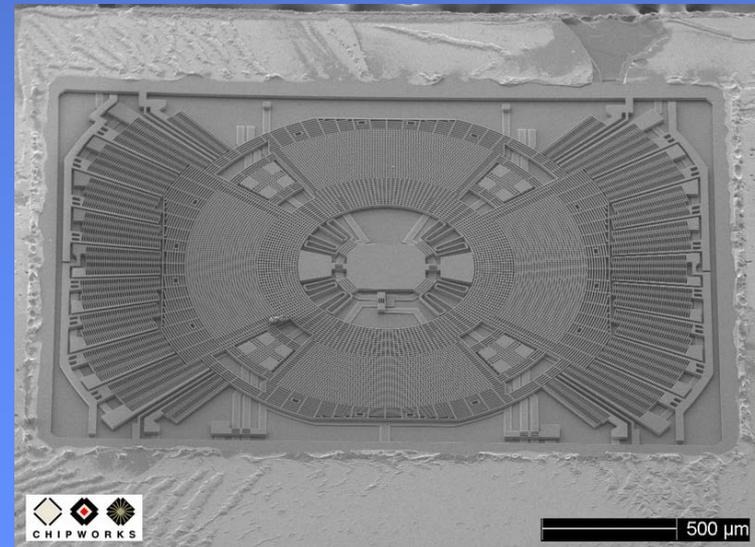
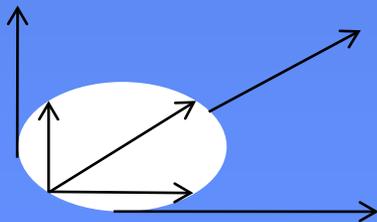
- Drawing a virtual fence around an intended use area
- Utilizing GPS to determine position in relation to the fence
- Increase authentication complexity when outside the fence
- Used in targeted advertising to mobile users





Orientation in Space

- Using the gyroscope to determine use orientation
- For example, if our user is left handed but the phone is being held in the right hand...
- Another example, if the tablet is typically used in a holder but now is being used while laying flat...
- By combining gyroscope and accelerometer you can get 6-axis movement in space
 - Angular acceleration X, Y, Z
 - Device acceleration X, Y, Z



Cognitive Behavior

- What hand do they predominately use?
- What is their swipe pattern like?
- What's their keystroke behavior like?
- What's their normal workflow?
- Develop cognitive patterns to use as a continuous authentication scheme





FINAL THOUGHTS



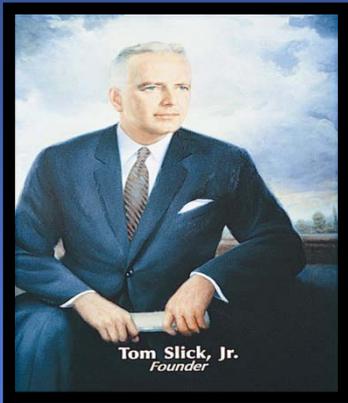
Summary

- ◆ Mobile devices provide greater ability to determine the authentication of a user
- ◆ Use case scenarios based on location, orientation, behavior can be factors for user authentication
- ◆ Mobile devices provide sensors that allow for a greater combination of authentication factors
- ◆ While there is no real “balance” that can be achieved between user experience and information protection needs, mobile devices provide tools that can ease the burden of authentication on the user
- ◆ As the technology for information processing changes, so should our thoughts in authentication and security.



Southwest Research Institute

1947



- 63 years, 4 presidents
- 3200 employees
- \$500M+ Revenue
 - 1200 Acres
 - 170 Buildings
- 2.1 million square feet
- Non Profit Applied R&D

2010

