Authentication

with

Minimal User Interaction

Authentication

- Authentication - Verification of a user, usually through the use of private credentials.
- What you know - Username/Password combination
- What you have - Card
- Who you are – Face, Fingerprint, Voice, etc.
Physical Security

- Protecting access to physical resources
  - Locked rooms
  - Physical machines
  - Cars

- Old methods relied on physical locks
  - Security of standard tumbler lock

- Digital protection of physical resources now more common

- Challenges of physical access security devices
  - Keys
  - cards

http://upload.wikimedia.org/wikipedia/commons/thumb/5/54/Pin_tumbler_bad_key.svg/1228px-Pin_tumbler_bad_key.svg.png

http://upload.wikimedia.org/wikipedia/commons/thumb/5/54/Pin_tumbler_bad_key.svg/1228px-Pin_tumbler_bad_key.svg.png
Physical Security

- Physical realms now more commonly secured with digital resources
  - RFID access cards
  - NFC technology
  - Car Key Fobs
- Most examples rely on wireless technologies.
- Problems?
  - Security of wireless?
  - Physical attacks?

Zero-Interaction Authentication & Relay Attack Resistance
Zero-interaction (de)authentication

PKES – Passive Keyless entry and start

Easy-to-use security

BlueProximity project in SourceForge
Corner and Noble, MobiCom '02
Ghost-and-leech relay attack

Kfir and Wool, SecureComm ’05
Francillon et al., NDSS ’11

Reader-and-ghost relay attack

Drimer and Murdoch, USENIX Security Symposium ’07
Defenses to Relay Attacks

- Distance Bounding
- Contextual Co-presence

Existing Solution

Brands and Chaum, EUROCRYPT ‘93

- Distance bounding

*1 light microsecond = 300m

Prior security association (e.g., shared key)

Verifier

Prover

challenge

minimize

response

Measure RTT
Context – Verbal Meaning

Definition of context in English:
noun
1. The circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood and assessed:
   ‘the decision was taken within the context of planned cuts in spending’

1.1 The parts of something written or spoken that immediately precede and follow a word or passage and clarify its meaning:
   ‘word processing is affected by the context in which words appear’

Contextual Co-Presence Detection (Benign Case)
Contextual Co-Presence Detection (Relay Attack)

Environmental Context Examples

- Acoustic & electromagnetic environment
  - Audio (Au)  [T. Halevi et al., ESORICS 2012]
  - WiFi (W)  [J. Krumm and K. Hinckley, UbiComp 2004]
  - Bluetooth (B)  [A. Varshavsky et al., UbiComp 2007]
  - GPS  [D. Ma et al., IEEE TDSC 2013]
- Natural – physical ambient environment
  - Temperature (T)
  - Humidity (H)
  - Gas Ratio (G)
  - Altitude (Al)
Environmental Context Detection

- Acoustic and RF environment
  - Sensors already available in current smartphones
- Physical ambient environment
  - Off-the-shelf ambient sensing device -- Sensordrone

Acoustic & RF Context – Data Collection
Natural Context – Data Collection

Co-Presence Detection Design

• Machine learning approach
• Multiboost algorithm
  • pruned J48 Graft/Random Forest as weak learner algorithm
  • ten-fold cross validation
• Evaluation metrics
  • False Positive Rate (FPR): measure of security
  • False Negative Rate (FNR): measure of usability
• Performance
  • FNR, FPR, F-measure, and Matthew’s correlation coefficient (MCC)
Environmental Context Features

- WiFi, Bluetooth, GPS
  - Jaccard distance
  - Mean of Hamming distance
  - Euclidian distance
  - Mean of exponential of difference
  - Sum of square of ranks
  - Subset count
- Audio
  - Max cross validation
  - Time frequency distance
- Temperature, humidity, gas, altitude
  - Hamming distance

Acoustic & RF Context Detection – Results

For all audio-RF combined

<table>
<thead>
<tr>
<th>Time Budget</th>
<th>F-Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>5s</td>
<td>0.9</td>
</tr>
<tr>
<td>8s</td>
<td>0.95</td>
</tr>
<tr>
<td>10s</td>
<td>0.95</td>
</tr>
<tr>
<td>12s</td>
<td>1.0</td>
</tr>
<tr>
<td>15s</td>
<td>1.0</td>
</tr>
</tbody>
</table>
Natural Context Detection – Results

Discussion

• How do Physical Ambient Modalities compare with other commonly available sensor modalities?
  • Temperature, Humidity, Gas, Pressure/Altitude vs
  • RF Sensors (WIFI, Bluetooth, GPS), Audio
Discussion

• Availability of sensors

Discussion

• Response Time
  • Sensors for physical parameters are typically faster than common RF sensors
Discussion

• Battery Power Consumption
  • Low power consumption compared to common RF sensors
  • Minimal influence on the power consumption than RF sensors

Discussion

• Adversarial Settings
  • Changing multiple physical ambient modalities simultaneously
    • will be harder
    • increases the likelihood of being noticed
Discussion

• Privacy
  • (Location) Privacy
  • Modalities keep on changing

Discussion

• Other Sensors?
Conclusion

Co-presence detection based on information collected from multiple different **physical ambient sensors**

- Approach for preventing relay attacks
- Improved security, efficiency & privacy

Two-Factor Authentication
Introduction

• Password only systems
• Two Factor Authentication TFA (Password + one-time code)
• Online guessing attack
• Offline dictionary attack
  • Many real-world instances
  • Password re-use

More than 200,000 of these passwords have reportedly been cracked so far.

Current State

|D| = 2^d = Size of a password dictionary

|z| = bandwidth of Device to Client channel

x = time
Adoption

- Small user adoption (if TFA optional)
  - Only 25% of Americans use TFA
  - Only 6% of 100k Gmail accounts have TFA enabled
- So Let’s Minimize user-phone interaction
  - QR/Blutooth/Wifi (Shirvanian et al., NDSS ’14)
  - USB/NFC Dongles (U2F — FIDO Universal 2nd Factor)
  - Sense the environment (Karapanos et al., Usenix’15)

LBD/MBD/FBD TFA (Shirvanian et al., NDSS ’14)
Main Idea

- Server stores a hash of the password and a secret \( s \), \( h=H(p,s) \)
- Device stores the secret \( s \)
- Authentication decision based on whether user provides the correct password and owns the device which stores \( s \)

Protocols

- Time-based TFA protocol
  - Applicable to all device types (Low, Mid, High Bandwidth)
  - Rely on a clock synchronized with the server
- Challenge-Response TFA Protocols
  - Symmetric-key and public-key TFA protocols
  - Applicable for devices that receive a challenge and show PIN
Time-Based TFA Protocol

1. Copy PIN
   \[ z = s \oplus F_s(T_a) \]

2. (UN, p, z)

3. Accept if:
   \[ H(p, z \oplus F_s(T_s)) = h \]

Symmetric-Key TFA Protocol

1. x

2. x

3. z = s \oplus F_s(x)

4. (UN, p, z)

5. Accept if:
   \[ H(p, z \oplus F_s(x)) = h \]
Public-Key TFA Protocol

1. $s, K, S_k$
2. $c = 2 \cdot c = E_{c_{ik}}(r)$
3. $z = s \oplus D_{c_{ik}}(a)$
4. $(p, z)$
5. Accept if:
   $H(p, z \oplus r) = h$

LBD Authentication Phase

1. $s, K$
2. $z = s \oplus x_{r_{k}} F_{k}(T_d)$
3. Copy PIN
4. User
5. Device
6. $s, K$

Password:

Verification Code:

Account:

Example.com

PIN: 467173
MBD Authentication Phase

\[ z = s \text{ xor } F_k(x) \]

FBD Authentication Phase

\[ z = s \text{ xor } \text{Dec}_k(a) \]
Discussion and Conclusion

- **Security:**
  - All mechanism provide improved resilience to offline dictionary attacks and online attacks.
  - Challenge-Response protocols are secure against a lunch-time attacker.
  - FBD mechanisms are more secure against online attacks.

- **Usability:**
  - There is no time synchronization requirement in Challenge Response mechanisms.
  - In high bandwidth channels user does not need to manually transfer the PIN.

- **Deployability:**
  - Traditional and LBD work with a plain browser and no special hardware.

U2F — FIDO Universal 2nd Factor
About U2F

• U2F is an open authentication standard that enables internet users to securely access any number of online services, with one single device
• U2F was created by Google and Yubico, with contribution from NXP, and is today hosted by FIDO Alliance

Main Idea

• The YubiKey requires nothing more than a simple tap or touch:
The Protocol

Protocol Details

- **Challenge-response**
  - challenge-response authentication flow, based on public-key cryptography
  - The key pair is generated in the device’s tamper-resistant execution environment

- **Phishing and MitM protection**
  - the client compiles what it knows about the current HTTP connection
  - this information is then signed by the U2F device and sent to the server

- **Device cloning detection**
  - A counter, sent from the device to the server
Sound Proof (Karapanos et al., Usenix’15)

Main Idea

- Leverage the proximity between user’s phone and computer as the second factor
- Proximity can be verified by:
  - Using local communication channels (phone-computer communication)
  - Sense ambient audio to verify proximity
- Usable: No user-phone interaction
- Deployable: Compatible with smartphones and major browsers without plugins
- Sound-Proof works in a variety of environments, even if the phone is in a pocket or purse
Architecture overview

1. Username, password
2. Username, password
3. Record
4. Record
5. Calculate Similarity Score s
6. Login Authorization S>x?

The protocol

Browser
- username,password
  - record, phone's PK
    - record audio
      - encrypted audio
        - login accepted or rejected

Server
- record

Phone
- record audio
- encrypted audio
- compute similarity score
- login accepted or rejected
Remote Attacker

Silence can help the attacker. Silent samples are rejected.

Attacker wins if samples are similar.

Co-locator Attacker

Similar samples! Attack succeeds.

Attack trivial if no user-phone interaction.
Evaluations

- Environment: office, office-music, home-TV, lecture room, train station, café
- Laptop: MacBook Pro Mid 2012, Dell E6510 (using Google Chrome)
- Phone: iPhone 5, Google Nexus 4
- Phone position: outside, in pocket, in purse
- User activity: being silent, talking, coughing, whistling

Performance

- Total time: User clicks “login” —> browser refresh to log the user in
  - Recording time: 3 seconds
Results

- False Acceptance Rate when the adversary and the victim devices record the same broadcast media.
- SC-SP stands for “same city and same Internet/cable provider”, SCDP stands for “same city but different Internet/cable providers”.
- DC-SP stands for “different cities and different Internet/cable providers”.
- A dash in the table means that the TV channel was not available at the victim’s location.

<table>
<thead>
<tr>
<th>False Acceptance Rate</th>
<th>SC-SP</th>
<th>SC-SP</th>
<th>DC-SP</th>
</tr>
</thead>
<tbody>
<tr>
<td>TV channel 1</td>
<td>1</td>
<td>0.1</td>
<td>0.1</td>
</tr>
<tr>
<td>TV channel 2</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>TV channel 3</td>
<td>1</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>TV channel 4</td>
<td>1</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Web radio 1</td>
<td>1</td>
<td>0</td>
<td>0.4</td>
</tr>
<tr>
<td>Web radio 2</td>
<td>0.1</td>
<td>0.8</td>
<td>0.8</td>
</tr>
<tr>
<td>Web TV 1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Web TV 2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Discussion

[Graph showing comparison between Password only, Existing 2FA, and Sound-Proof]
Thank you!

Questions?