Proving co-location by context comparison

Xiang Gao

University of Helsinki
xzgao@cs.helsinki.fi

Mar 27, 2013
Outline

1. Background
2. Contextual Approach
3. Context tags
4. Discussion
5. Our Experiment
6. Conclusion
Background

- Security v.s. Usability? e.g. micro and macro payment
- Zero-Interaction Authentication: e.g. laptop lock, car key
ZIA model
Corner and Noble’s Token Authentication System [1]

- Attacks?
Attacks

- Mimicry attacks: not possible
- Relay attacks: Ghost-and-leech attack
Ghost-and-leeph

Example: Kfir and Wool’s ghost and leech demo using NFC devices [3]
Distance Bounding

- Challenge-response method, proving proximity

- Problems: sensitive to delay; distance can be forged in Distance Fraud attack.
Contextual Approach

- Co-location is tested by comparing context tags.
- Context tags are extracted and synthesized from the sensing data of related contextual attributes.
Example

- Scenario: NFC payment
- Third party involved to make comparison
- Data exchange in secure channels
- Defense against relay attacks
- Privacy preserved

Figure: NFC payment system with co-location comparison. [2]
Requirements

- **Unforgeability**: difficult to fake the context (attributes). Complexity, dynamics and noise
- **Efficiency**: computation, energy
- **Robustness**: the ability to tolerate errors in making co-location decisions. False positive errors and false negative errors
- **Usability**: ease-of-use considering environmental and hardware restrictions.
List of candidates

- Ambient Audio
- Ambient Light
- GPS
- Acceleration
- Wireless Broadcast Traffic
- Nearby Devices: WIFI, Cellular, Bluetooth
- ...

Correlation Approach [2]

- Record sample audio signals via microphone
- Technique selection: time-based, frequency-based, time-frequency-based correlation techniques.
- Classification formula: distinguish normal and attacked scenario by checking the confusion matrix of correlation distance. Classification formula chosen as threshold.
- Detection rate validation: test for FP and FN errors
Ambient Audio

Energy-based Fingerprinting [5]
- Divide the audio sequence into n frames, DFT
- Split each frame linearly into non-overlapping frequency bands
- Establish an energy matrix E with the sum of energy for each band as elements
- Translate differences of elements into bit sequence
- Use Hamming distance to set the threshold

Evaluation
- Correlation is stronger than fingerprinting approach
- Noise introduces error
- Better performance in scenarios with a higher ratio of featured signal and noise
Ambient Light

- Light illuminance
- Decision based on distance threshold
- Influenced by orientation of handsets
- High FN error
GPS

- Global Positioning System: satellites with standard atomic timer, calculate distance with RTT
- At least 4 satellites are needed to calculate accurate location
- NMEA sentences: satellite info from $GPGSV$, longitude and latitude info from $GPRMC$, 3D fix (altitude) from $GPGGA$
- Strategy 1: use location coordinates.
- Strategy 2: use raw data (mainly satellite info)
- Pros and Cons?
Acceleration

- CO2GO application: environmental acceleration traces for different transportation modes
- Limited; influenced by human actions
- Shaking in one hand: strong similarity for co-location, and unforgeability reported by Mayrhofer [4]
Wireless Broadcast Traffic

- Features from broadcast packets: IP addresses, packet sequence numbers
- High unforgeability according to experiment
- Influenced by density of APs
Nearby devices

- WIFI, Cellular, Bluetooth devices
- ID: MAC Address, combined with RSS
- Indoor positioning is overkill
- Moderate results for ID+RSS visible lists, high FN
- Influenced by density of APs
Comparison of context tags

<table>
<thead>
<tr>
<th>Context Tag</th>
<th>Evaluation</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ambient Audio</td>
<td>strong</td>
<td>scenarios with audio sources</td>
</tr>
<tr>
<td>Ambient Light</td>
<td>moderate</td>
<td>influenced by orientation of device hardware; high FN</td>
</tr>
<tr>
<td>GPS</td>
<td>strong</td>
<td></td>
</tr>
<tr>
<td>Acceleration</td>
<td>strong</td>
<td>need user interaction (shaking)</td>
</tr>
<tr>
<td>Wireless Broadcast Traffic</td>
<td>strong</td>
<td>density of access points</td>
</tr>
<tr>
<td>Nearby Device-IDs + RSSs</td>
<td>moderate</td>
<td>density of access points, high FN</td>
</tr>
</tbody>
</table>
Probable problems

- Replay attacks: timestamp or nounces
  
  \[(ID1, ID2, contextvector, timestamp)_K\]

  or

  \[Challenge : (ID2, ID1, N_1)_K\]

  \[Response : (ID1, ID2, contextvector, N_1)_K\]

- Faking context attack
- Spoofing: attacking infrastructures. WIFI v.s. GPS
- Granularity
- Location Privacy
BlueProximity and Experiment

- **BlueProximity**: an ubuntu application that enables automatic locking/unlocking of target laptop.
- **Principle**: the laptop periodically checks the received signal strength indicator (RSSI) of the handset, and estimates the distance.
- **No pairing** between the handset and the laptop, not a ZIA!
- **Scenario**: there is a queue from the intersection
Phase I

Faking ID attack

- Victim, Attacker, Token
- No pairing: unsecure channel
- Attack by faking Bluetooth MAC address
Phase II

Relay attack

- Victim, Ghost, Leech, Token
- Use pairing: secure channel, enhanced BlueProximity
- Relay attack instead of Faking-ID attack: motivation
Defend attacks

Contextual co-location authentication protocol

- Apply the context tag comparison model
- Use pairing: secure channel, enhanced BlueProximity
- To defend relay attacks
Conclusion

- Use context tag comparison model to solve problems in ZIA against relay attacks
- Surveyed and evaluated context tags categorized as audio, light, GPS, acceleration, wireless broadcast traffic, and nearby device-IDs+RSSs
- Our experiment on BlueProximity
References

M. D. Corner and B. D. Noble.
Zero-interaction authentication.

T. Halevi, D. Ma, N. Saxena, and T. Xiang.
Secure Proximity Detection for NFC Devices Based on Ambient Sensor Data.

Z. Kfir and A. Wool.
Picking Virtual Pockets using Relay Attacks on Contactless Smartcard.
In First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM’05), number c, pages 47–58. IEEE, 2005.