Context-based security
State of the art, open research topics and a case study

Stephan Sigg
The fifth International Workshop on Context-Awareness for Self-Managing Systems,
CASEMANS 2011, 18.09.2011, Beijing, China
Motivation

Security demands are omnipresent and increasing in number
Motivation

**Threats + requirements for security precautions increase simultaneously**

Have you ever...

- lost/forgot your password?
- wondered that the password has to be exchanged rather frequently
- utilised identical passwords for different accounts
- used weak passwords for convenience
- experienced security precautions as a hassle
- disabled password/pin? *(My phone was delivered with pin disabled by default)*
Motivation

We could use biometric data

- Fingerprints
- Iris scan
- DNA
- Face recognition
Motivation

We could use biometric data, BUT ...

Is this really more secure than the pin/password-based approaches?

- Or is it probably only more convenient?
  - Biometric data shall be easy to obtain/verify by legal authorities but difficult to forge/steal.
  - Commonly, this contradiction is solved in favour of the former aspect for convenience.
Motivation

What are the benefits of using context as a basis of security

- Context is very personalised information
- Context changes frequently with time and location
- We can adapt the security level of applications to their context
- Less obtrusive but at the same time more secure?
Aspects of security through context

Password-less authentication

- Context data is not forgotten like pins
- Enables new/intelligent, potentially intuitive security schemes
- High entropy has to be guaranteed
- Provide less-/un-obtrusive security schemes
- Prevent people from using weak passwords

Location is an important context

- Current applications location dependent

Privacy concerns

- People have grown sensitive to providing personal information
- Privacy threads are perceived differently

---

Outline

Motivation

Audio as a key

Case study

Conclusion
Audio as a key

Using audio for device authentication

- Can we use ambient audio from devices in proximity as a common secret for device pairing?
  - Establish trust-based perception of security among mobile devices \(^2\).
  - Establish ad-hoc secure channel among devices (non-interactive).
  - Establish a simplified and less-/un-obtrusive security mechanism.
  - Switch among several security levels-based on context.

\(^2\) C. Dupuy, A. Torre. Local clusters, trust, confidence and proximity, Clusters and Globalisation: The development of urban and regional economies, pp. 175–195, 2006.
Audio as a key

Audio fingerprints for device pairing

- Create audio fingerprints as features for ambient audio \(^3\)
- Utilise error correcting codes to account for differences in fingerprints

Audio as a key

Audio fingerprints for device pairing

- An audio fingerprint is-based on the fluctuation in energy differences in adjacent frequency bands over time
- Tolerant for low noise and changes in absolute energy

\[
f(i, j) = \begin{cases} 
1 & \text{if } E(i, j) - E(i, j + 1) - (E(i - 1, j) - E(i - 1, j + 1)) > 0, \\
0 & \text{otherwise.}
\end{cases}
\]
Audio as a key

Using audio for device authentication

<table>
<thead>
<tr>
<th>ID</th>
<th>Captured audio</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>1100101000101</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>1000101010001</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>0001000110011</td>
</tr>
</tbody>
</table>

- Issues
  - Context is a noisy source.
    - Measurement inaccuracies
    - Often strict time or location dependence
    - Classification inaccuracies
  - Accurate time synchronisation required
Audio as a key

Current approaches

- The Candidate key protocol\(^4\)
  - Acceleration data of shaking processes
  - Iterative key generation
- Hamming distance among binary keys \(^5\)


Audio as a key

Device pairing with fuzzy cryptography

- The received fingerprint at two devices is not identical due to
  - Recording errors
  - Timing errors
  - Noise

![Graph showing percentage of identical bits]
Outline

Motivation

Audio as a key

Case study

Conclusion
Case study
Case study

- We utilised Reed-Solomon error correcting codes in order to account for these bit errors ($RS(q, m, n)$)
  - $A = \mathbb{F}^m_q, C = \mathbb{F}^n_q : q \text{ prim.}$
- in conjunction with the Secure Hash Algorithm with 256 bit (SHA-256)

<table>
<thead>
<tr>
<th>Microphones</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Impedance</td>
<td>$\leq 22 \text{ kΩ}$</td>
</tr>
<tr>
<td>Current consumption</td>
<td>$\leq 0.5 \text{ mA}$</td>
</tr>
<tr>
<td>Frequency response</td>
<td>$100 \text{ Hz} \sim 16 \text{ KHz}$</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>$-38 \text{ dB} \pm 2 \text{ dB}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scenarios</th>
<th>Scenario 1</th>
<th>Scenario 2/3</th>
<th>Scenario 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microphone distance</td>
<td>$\approx 1 \text{ m}$</td>
<td>$\approx 4 \text{ m}$</td>
<td>$\approx 1 \text{ m}$</td>
</tr>
<tr>
<td>Distance to speaker</td>
<td>$0.8 \text{ m} - 3 \text{ m}$</td>
<td>$0.8 \text{ m} - 4 \text{ m}$</td>
<td>$0.5 \text{ m} - 3 \text{ m}$</td>
</tr>
</tbody>
</table>
Case study

<table>
<thead>
<tr>
<th>Scenarios</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful attempts</td>
<td>0.9</td>
<td>0.4</td>
<td>0.0</td>
<td>0.8</td>
</tr>
<tr>
<td>Bit errors corrected (∅)</td>
<td>179.6</td>
<td>170.75</td>
<td>–</td>
<td>173.75</td>
</tr>
</tbody>
</table>
Case study

Audio playback can improve success rate for low ambient audio

- Controlled Indoor environment
- Microphones attached to left and right ports of an audio card (1.5m, 3m, 4.5m, 6m)
- Audio source (music, clap, snap, speak, whistle)
- Loudness:
  - quiet (approx 10 – 23dB)
  - medium (approx 23 – 33dB)
  - loud (≈ 33 – 45dB)
- Pairwise comparison of hamming distance: 7500 comparisons; 300 comparisons for simultaneous recordings
Case study

Audio playback can improve success rate for low ambient audio

- $m=128$
- minimum overlap 62.5%

<table>
<thead>
<tr>
<th></th>
<th>clap</th>
<th>music</th>
<th>snap</th>
<th>speak</th>
<th>whistle</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>189</td>
<td>192</td>
<td>190</td>
<td>191</td>
<td>191</td>
</tr>
<tr>
<td>2</td>
<td>192</td>
<td>192</td>
<td>192</td>
<td>191</td>
<td>191</td>
</tr>
<tr>
<td>3</td>
<td>191</td>
<td>188</td>
<td>192</td>
<td>191</td>
<td>–</td>
</tr>
<tr>
<td>4</td>
<td>190</td>
<td>192</td>
<td>190</td>
<td>191</td>
<td>192</td>
</tr>
<tr>
<td>5</td>
<td>192</td>
<td>190</td>
<td>191</td>
<td>192</td>
<td>–</td>
</tr>
<tr>
<td>6</td>
<td>192</td>
<td>191</td>
<td>191</td>
<td>188</td>
<td>192</td>
</tr>
<tr>
<td>7</td>
<td>189</td>
<td>190</td>
<td>190</td>
<td>192</td>
<td>192</td>
</tr>
<tr>
<td>8</td>
<td>192</td>
<td>186</td>
<td>186</td>
<td>192</td>
<td>192</td>
</tr>
<tr>
<td>9</td>
<td>192</td>
<td>189</td>
<td>189</td>
<td>192</td>
<td>189</td>
</tr>
<tr>
<td>10</td>
<td>192</td>
<td>196</td>
<td>196</td>
<td>192</td>
<td>–</td>
</tr>
</tbody>
</table>
Case study

Audio playback can improve success rate for low ambient audio

- $m = 152$
- minimum overlap 65%

<table>
<thead>
<tr>
<th></th>
<th>clap</th>
<th>music</th>
<th>snap</th>
<th>speak</th>
<th>whistle</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>180</td>
<td>179</td>
<td>180</td>
<td>180</td>
<td>–</td>
</tr>
<tr>
<td>2</td>
<td>179</td>
<td>179</td>
<td>180</td>
<td>180</td>
<td>180</td>
</tr>
<tr>
<td>3</td>
<td>179</td>
<td>–</td>
<td>180</td>
<td>180</td>
<td>178</td>
</tr>
<tr>
<td>4</td>
<td>–</td>
<td>–</td>
<td>180</td>
<td>–</td>
<td>180</td>
</tr>
<tr>
<td>5</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>179</td>
</tr>
<tr>
<td>6</td>
<td>180</td>
<td>180</td>
<td>179</td>
<td>180</td>
<td>180</td>
</tr>
<tr>
<td>7</td>
<td>179</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>180</td>
</tr>
<tr>
<td>8</td>
<td>–</td>
<td>178</td>
<td>180</td>
<td>179</td>
<td>180</td>
</tr>
<tr>
<td>9</td>
<td>–</td>
<td>179</td>
<td>178</td>
<td>180</td>
<td>180</td>
</tr>
<tr>
<td>10</td>
<td>180</td>
<td>179</td>
<td>179</td>
<td>178</td>
<td>179</td>
</tr>
</tbody>
</table>
Case study

Audio playback can improve success rate for low ambient audio

- $m = 204$
- minimum overlap 70%

<table>
<thead>
<tr>
<th>Audio sample</th>
<th>clap</th>
<th>music</th>
<th>snap</th>
<th>speak</th>
<th>whistle</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>154</td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>153</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>-</td>
<td>-</td>
<td>154</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Conclusion

- We have demonstrated an unobtrusive mechanism for secure ad-hoc device pairing-based on ambient audio
  - Noise tolerant due to utilisation of error correcting codes
  - Error tolerance is a design parameter
- Audio fingerprint as feature
- Can be generalised to other context classes
- Instrumented and tested on laptop computers
- Entropy: No bias observed in dieHarder statistical tests
- Check our paper for open research issues and opportunities of context-based security
Questions?

Stephan Sigg
sigg@nii.ac.jp