Pattern based alignment of audio data for Ad-hoc secure device pairing
Zero-communication data synchronisation

Ngu Nguyen, Stephan Sigg, An Huynh and Yusheng Ji
ISWC 2012, 21.06.2012, Newcastle
Security from environmental stimuli

The number of communicating devices increasingly exceeds mobile users. Among all other tasks we have on our minds, how shall we also take care of these device’s security issues?
Security from environmental stimuli

The number of communicating devices increasingly exceeds mobile users. Among all other tasks we have on our minds, how shall we also take care of these device’s security issues?

- Security must become not only unobtrusive but unattended
- We need a more natural perception of security
Security from environmental stimuli

Audio-based ad-hoc secure pairing

- Audio as common context source
- Fuzzy cryptography

Hamming distance in created fingerprints (loud audio source in 1.5m and 3m)

<table>
<thead>
<tr>
<th>Audio sequence class</th>
<th>Median percentage of identical bits in fingerprints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clap</td>
<td>0.5</td>
</tr>
<tr>
<td>Music</td>
<td>0.55</td>
</tr>
<tr>
<td>Snap</td>
<td>0.6</td>
</tr>
<tr>
<td>Speak</td>
<td>0.65</td>
</tr>
<tr>
<td>Whistle</td>
<td>0.7</td>
</tr>
</tbody>
</table>

Percentage of tests in one test run that passed at >5% for Kuiper KS p-values

<table>
<thead>
<tr>
<th>Test run</th>
<th>Percentage of passed tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.91</td>
</tr>
<tr>
<td>2</td>
<td>0.93</td>
</tr>
<tr>
<td>4</td>
<td>0.95</td>
</tr>
<tr>
<td>6</td>
<td>0.97</td>
</tr>
<tr>
<td>8</td>
<td>0.99</td>
</tr>
<tr>
<td>10</td>
<td>1.01</td>
</tr>
</tbody>
</table>

Only music
Only whistle
Only snap
Only speak
Only clap
Security from environmental stimuli

Hardware-originated synchronisation offset

- We experience significant differences in audio samples from devices with differing hardware (Nexus One; Nexus S)
- How can we correct these without disclosing information on the channel?
Security from environmental stimuli

How to synchronise audio without disclosing information?
No data shall be transmitted among devices

Hardware-originated synchronisation offset

- Approximate pattern matching with arbitrary common sequence\(^a\)

Security from environmental stimuli

Hardware-originated synchronisation offset

- Synchronisation in the order of 3ms possible
- No additional data transmitted among devices
Unattended, spontaneous ad-hoc security scheme

Capable of rising the base-level for security on mobile devices
Conclusion

Unattended, spontaneous ad-hoc security scheme
Capable of rising the base-level for security on mobile devices

- Synchronisation of context data with zero data transmission
- Case study on audio-based secure pairing
Questions?

Stephan Sigg
sigg@nii.ac.jp
Security from environmental stimuli

- Generation of Audio fingerprints\(^1\)
- Utilise Fuzzy cryptography to obtain identical keys at devices\(^2\)

1. J. Haitsma and T. Kalker, A highly robust audio fingerprinting system, ISMIR 2002

\(X\) possible messages, \(C\) possible codewords.