0x1A Great Papers in Computer Security

Vitaly Shmatikov

http://www.cs.utexas.edu/~shmat/courses/cs380s/
L. Zhuang, F. Zhou, D. Tygar

Keyboard Acoustic Emanations Revisited

(CCS 2005)
Acoustic Information in Typing

- Different keystrokes make different sounds
  - Different locations on the supporting plate
  - Each key is slightly different

- Frequency information in the sound of the typed key can be used to learn which key it is
  - Observed by Asonov and Agrawal (2004)
“Key” Observation

◆ Build acoustic model for keyboard and typist
◆ Exploit the fact that typed text is non-random (for example, English)
  ● Limited number of words
  ● Limited letter sequences (spelling)
  ● Limited word sequences (grammar)
◆ This requires a language model
  ● Statistical learning theory
  ● Natural language processing
Sound of a Keystroke

- Each keystroke is represented as a vector of Cepstrum features
  - Fourier transform of the decibel spectrum
  - Standard technique from speech processing

[Zhuang, Zhou, Tygar]
Bi-Grams of Characters

- Group keystrokes into N clusters
- Find the best mapping from cluster labels to characters
- Unsupervised learning: exploit the fact that some 2-character combinations are more common
  - Example: “th” vs. “tj”
  - Hidden Markov Models (HMMs)

[Zhuang, Zhou, Tygar]
Add Spelling and Grammar

- Spelling correction
- Simple statistical model of English grammar
  - Tri-grams of words
- Use HMMs again to model

[Zhuang, Zhou, Tygar]
the big money fight has drawn the support of dozens of companies in the entertainment industry as well as attorneys generals in states, who fear the film-sharing software will encourage illegal activity, stem the growth of small artists and lead to lost jobs and diminished sales tax revenue.

---

Before spelling and grammar correction

After spelling and grammar correction

_____ = errors in recovery  □ = errors corrected by grammar
Feedback-based Training

- Recovered characters + language correction provide feedback for more rounds of training
- Output: keystroke classifier
  - Language-independent
  - Can be used to recognize random sequence of keys
    - For example, passwords
  - Representation of keystroke classifier
    - Neural networks, linear classification, Gaussian mixtures

[Zhuang, Zhou, Tygar]
Overview

Initial training

- wave signal (recorded sound)
  - Feature Extraction
  - Unsupervised Learning
  - Language Model Correction
  - Sample Collector
  - Classifier Builder

Keystroke classifier
recovered keystrokes

Subsequent recognition

- wave signal
  - Feature Extraction
  - Keystroke Classifier
  - Language Model Correction (optional)

recovered keystrokes

[Zhuang, Zhou, Tygar]
Experiment: Single Keyboard

- Logitech Elite Duo wireless keyboard
- 4 data sets recorded in two settings: quiet and noisy
  - Consecutive keystrokes are clearly separable
- Automatically extract keystroke positions in the signal with some manual error correction
Results for a Single Keyboard

[Datasets]

<table>
<thead>
<tr>
<th></th>
<th>Recording length</th>
<th>Number of words</th>
<th>Number of keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set 1</td>
<td>~12 min</td>
<td>~400</td>
<td>~2500</td>
</tr>
<tr>
<td>Set 2</td>
<td>~27 min</td>
<td>~1000</td>
<td>~5500</td>
</tr>
<tr>
<td>Set 3</td>
<td>~22 min</td>
<td>~800</td>
<td>~4200</td>
</tr>
<tr>
<td>Set 4</td>
<td>~24 min</td>
<td>~700</td>
<td>~4300</td>
</tr>
</tbody>
</table>

[Initial and final recognition rate]

<table>
<thead>
<tr>
<th></th>
<th>Set 1 (%)</th>
<th>Set 2 (%)</th>
<th>Set 3 (%)</th>
<th>Set 4 (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Word</td>
<td>Char</td>
<td>Word</td>
<td>Char</td>
<td>Word</td>
</tr>
<tr>
<td>Initial</td>
<td>35 76</td>
<td>39 80</td>
<td>32 73</td>
<td>23 68</td>
</tr>
<tr>
<td>Final</td>
<td>90 96</td>
<td>89 96</td>
<td>83 95</td>
<td>80 92</td>
</tr>
</tbody>
</table>
Experiment: Multiple Keyboards

- Keyboard 1: Dell QuietKey PS/2
  - In use for about 6 months

- Keyboard 2: Dell QuietKey PS/2
  - In use for more than 5 years

- Keyboard 3: Dell Wireless Keyboard
  - New
Results for Multiple Keyboards

12-minute recording with app. 2300 characters

<table>
<thead>
<tr>
<th></th>
<th>Keyboard 1 (%)</th>
<th>Keyboard 2 (%)</th>
<th>Keyboard 3 (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Word</td>
<td>Char</td>
<td>Word</td>
</tr>
<tr>
<td>Initial</td>
<td>31</td>
<td>72</td>
<td>20</td>
</tr>
<tr>
<td>Final</td>
<td>82</td>
<td>93</td>
<td>82</td>
</tr>
</tbody>
</table>
Defenses

- Physical security
- Two-factor authentication
- Masking noise
- Keyboards with uniform sound (?)