Side-Channel Attacks: Acoustics and Reflections

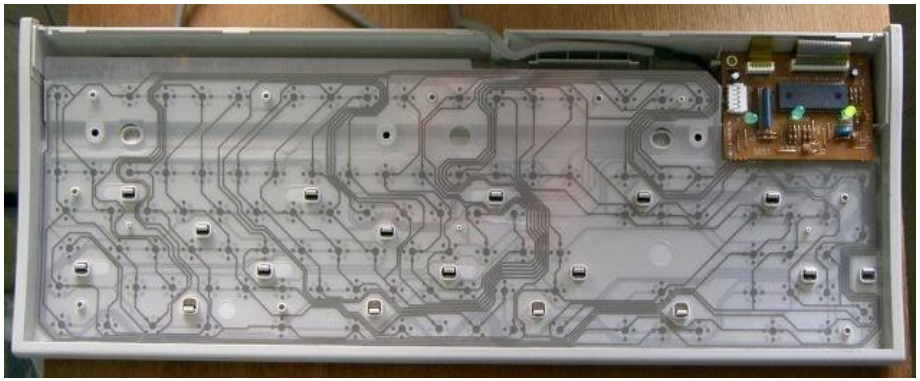
Vitaly Shmatikov

Reading

- "Keyboard Acoustic Emanations Revisited" by Zhuang, Zhou, and Tygar (CCS 2005)
- "Compromising Reflections: How to read Computer Monitors around a Corner" by Backes, Duermuth, and Unruh (S&P 2008)
  - Also "Tempest in a Teapot: Compromising Reflections Revisited" (S&P 2009)

Acoustic Information in Typing

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



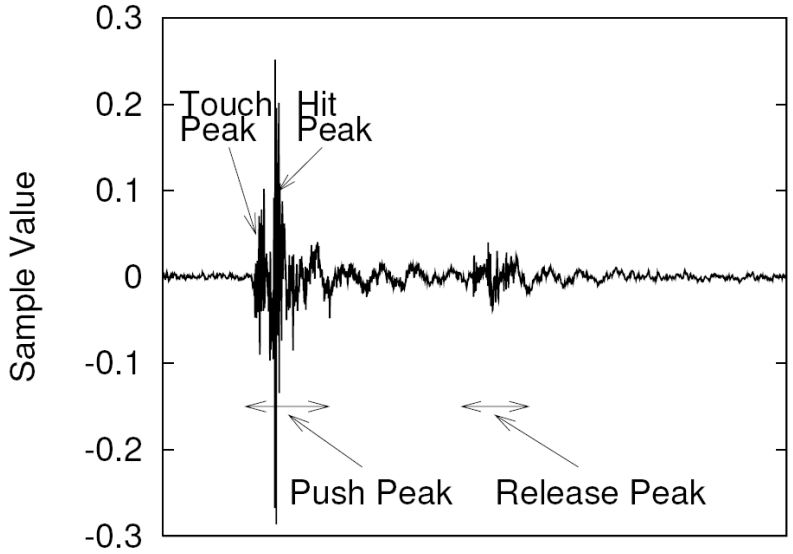
- Frequency information in the sound of typed key can be used to learn which key it is
  - Observed by Asonov and Agrawal (2004)

“Key” Observation

- Exploit the fact that typed text is non-random (for example, English)
  - Some letters occur more often than others
  - Limited number of valid letter sequences (spelling)
  - Limited number of valid word sequences (grammar)
- Build acoustic model for keyboard and typist

Sound of a Keystroke

[Zhuang, Zhou, Tygar]

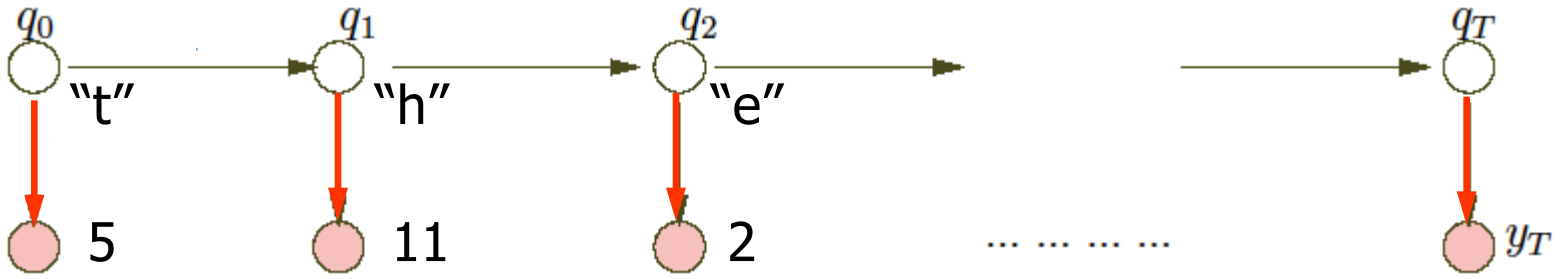


- Each keystroke is represented as a vector of Cepstrum features
  - Fourier transform of the decibel spectrum
  - Standard technique from speech processing

Bi-Grams of Characters

[Zhuang, Zhou, Tygar]

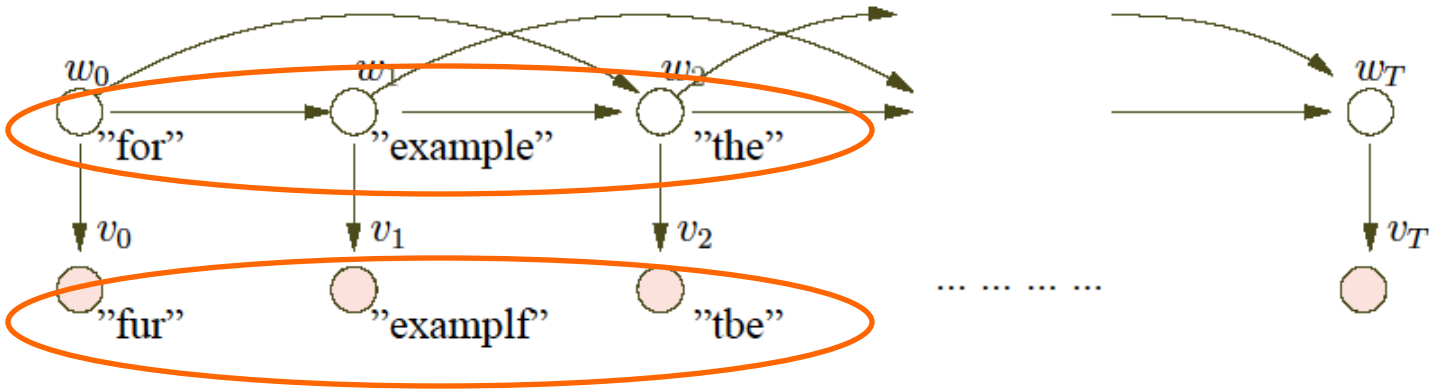
- Group keystrokes into N clusters
- Find the best mapping from cluster labels to characters
- Exploit the fact that some character combinations are more common than others
  - Example: "th" vs. "tj"
  - Unsupervised learning using Hidden Markov Models



Tri-grams of Words

[Zhuang, Zhou, Tygar]

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



Two Copies of Recovered Text

[Zhuang, Zhou, Tygar]

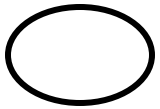
Before spelling and grammar correction

the big money fight has drawn the shoporo od dosens of companies in the entertainment industry as well as attorneys gnnerals on states, who fear the fild shading softwate will encourage illegal acyivitt, srem the grosth of small arrists and lead to lost cobs and dimished sales tas revenue.

After spelling and grammar correction

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 finished sales tax revenue.

_____ = errors in recovery

 = errors corrected by grammar

Feedback-based Training

[Zhuang, Zhou, Tygar]

- Language correction of recovered characters
- Feedback for more rounds of training
- Output: keystroke classifier
  - Language-independent
  - Can be used to recognize random sequence of keys
    - For example, passwords
  - Many possible representations
    - Neural networks, linear classification, Gaussian mixtures

Experiment: Single Keyboard

[Zhuang, Zhou, Tygar]

- 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 Single Keyboard

[Zhuang, Zhou, Tygar]

- Datasets

	Recording length	Number of words	Number of keys
Set 1	~12 min	~400	~2500
Set 2	~27 min	~1000	~5500
Set 3	~22 min	~800	~4200
Set 4	~24 min	~700	~4300

- Initial and final recognition rate

	Set 1 (%)		Set 2 (%)		Set 3 (%)		Set 4 (%)	
	Word	Char	Word	Char	Word	Char	Word	Char
Initial	35	76	39	80	32	73	23	68
Final	90	**96**	89	**96**	83	**95**	80	**92**

Experiment: Multiple Keyboards

[Zhuang, Zhou, Tygar]

- 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

[Zhuang, Zhou, Tygar]

- 12-minute recording with app. 2300 characters

	Keyboard 1 (%)		Keyboard 2 (%)		Keyboard 3 (%)	
	Word	Char	Word	Char	Word	Char
Initial	31	72	20	62	23	64
Final	82	**93**	82	**94**	75	**90**

Compromising Reflections

[Backes et al.]

- Typical office: monitor faces away from window
- Screen is reflected in surrounding objects
  - Teapots, eyeglasses, bottles, etc.
- Use a commodity telescope to capture reflection from a distance (up to 30 meters)
- Image-processing techniques (deconvolution) to improve the quality of captured reflections

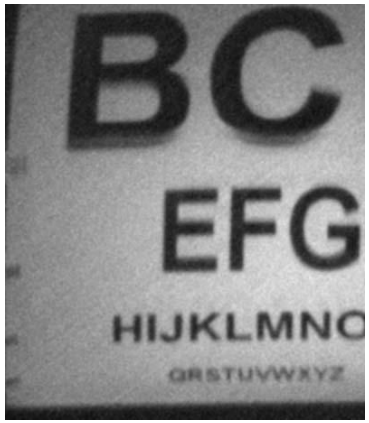
Experimental Setup

[Backes et al.]

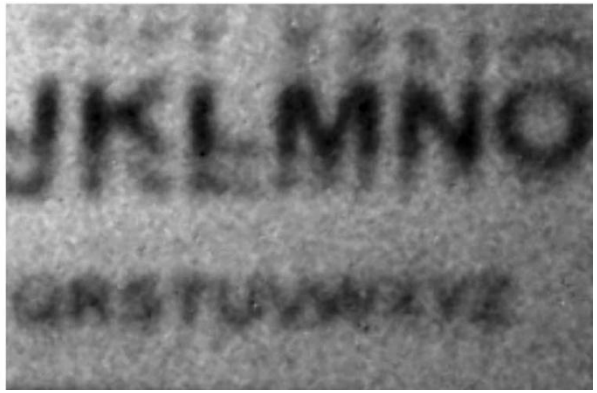
Teapots

[Backes et al.]

- From 5 meters

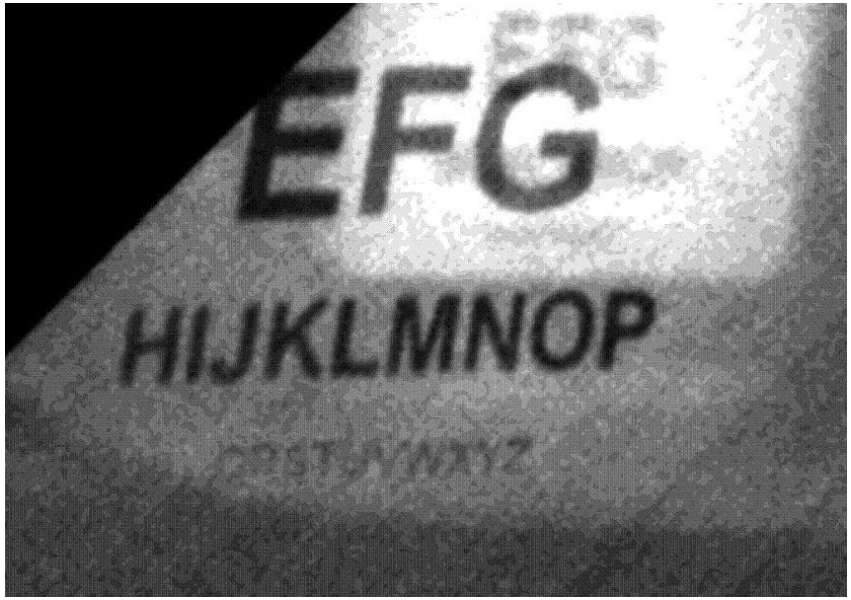




- From 10 meters

Eyeglasses

[Backes et al.]



Spoon

[Backes et al.]

Plastic Bottle

[Backes et al.]

With Better Equipment …

- Celestron C9.25 Schmidt-Cassegrain telescope
  - Street price: $2000

- SBIG ST-10XME camera
  - Street price: $6000
- Image deconvolution techniques to reduce blur
  - Out-of-focus blur
    - Large focal lengths & apertures = very shallow depth of field
  - Motion blur
  - Diffraction blur

… Human Eyes Are Readable

[Backes et al.]