CS 380S

0x1A Great Papers in Computer Security

Vitaly Shmatikov

http://www.cs.utexas.edu/~shmat/courses/cs380s/

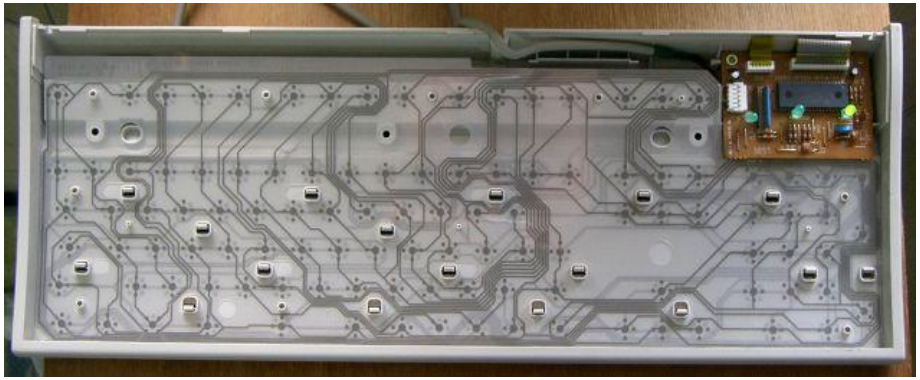
L. Zhuang, F. Zhou, D. Tygar

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



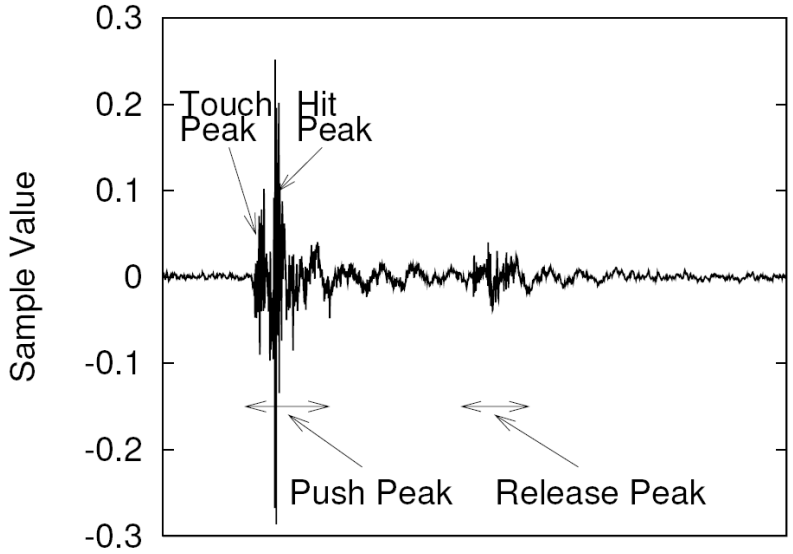
- Frequency information in the sound of the typed key can be used to learn which key it is
  - Observed by Asonov and Agrawal (2004)

"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

[Zhuang, Zhou, Tygar]

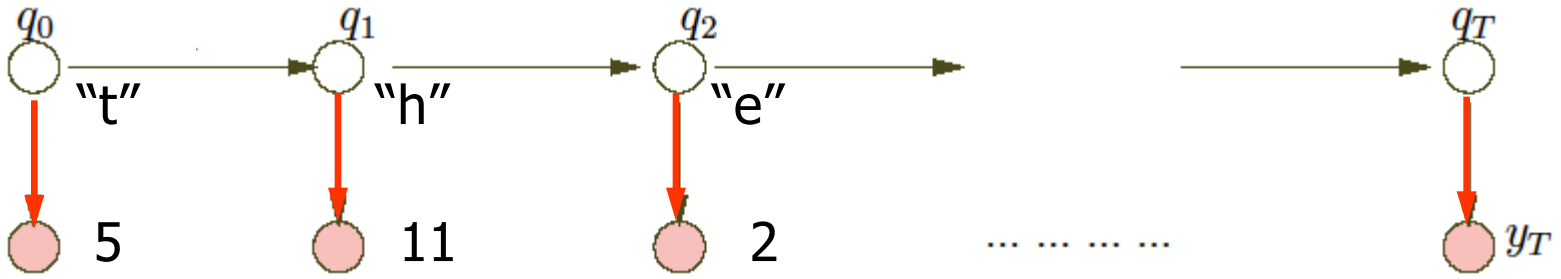


- Each keystroke is represented as a vector of Cepstrum features
  - Fourier transform of the decibel spectrum
  - Standard technique from speech processing

Bi-Grams of Characters

[Zhuang, Zhou, Tygar]

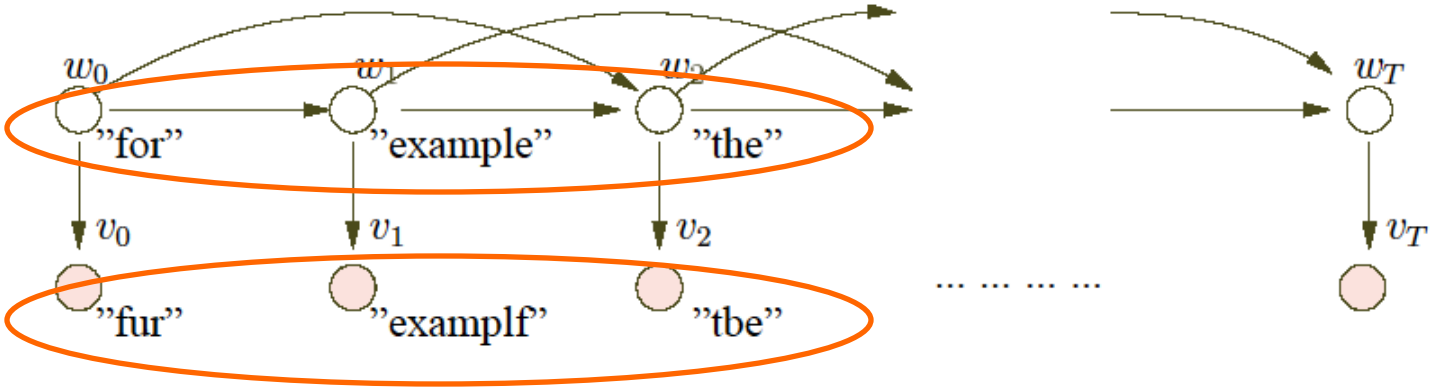
- Group keystrokes into N clusters
- Find the best mapping from cluster labels to characters
- Unsupervised learning: exploit the fact that some 2-character combinations are more common
  - Example: "th" vs. "tj"
  - Hidden Markov Models (HMMs)



Add Spelling and Grammar

[Zhuang, Zhou, Tygar]

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



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

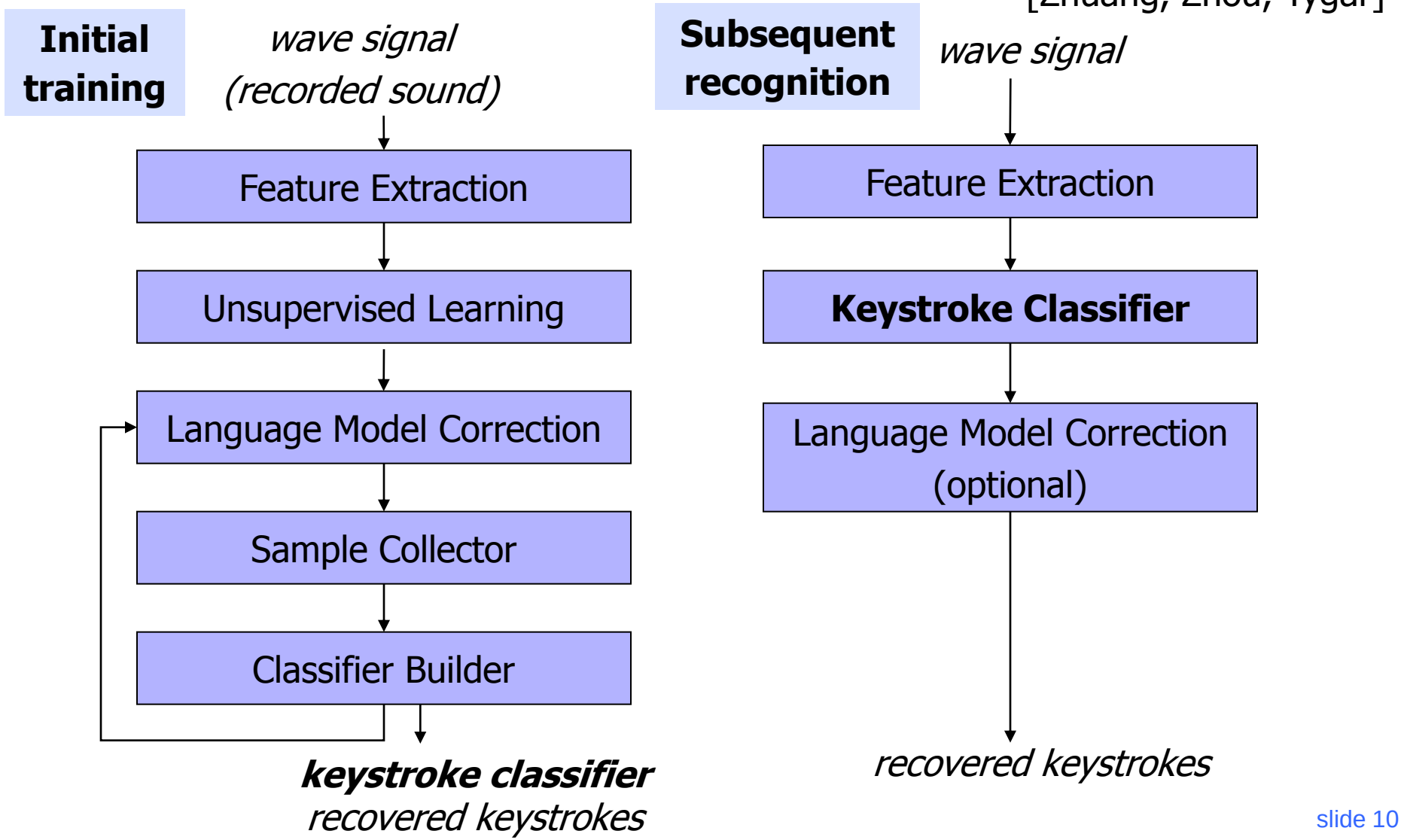
Feedback-based Training

[Zhuang, Zhou, Tygar]

- 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

Overview

[Zhuang, Zhou, Tygar]



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 a 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**

Defenses

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