Security and Privacy of Keyboard

ADVANCED TOPICS IN COMPUTER AND NETWORK SECURITY

Alessandro Benetti
Reza Ghasemi

UNIVERSITÀ DEGLI STUDI DI PADOVA

A.Y. 2022/2023

Keyboards

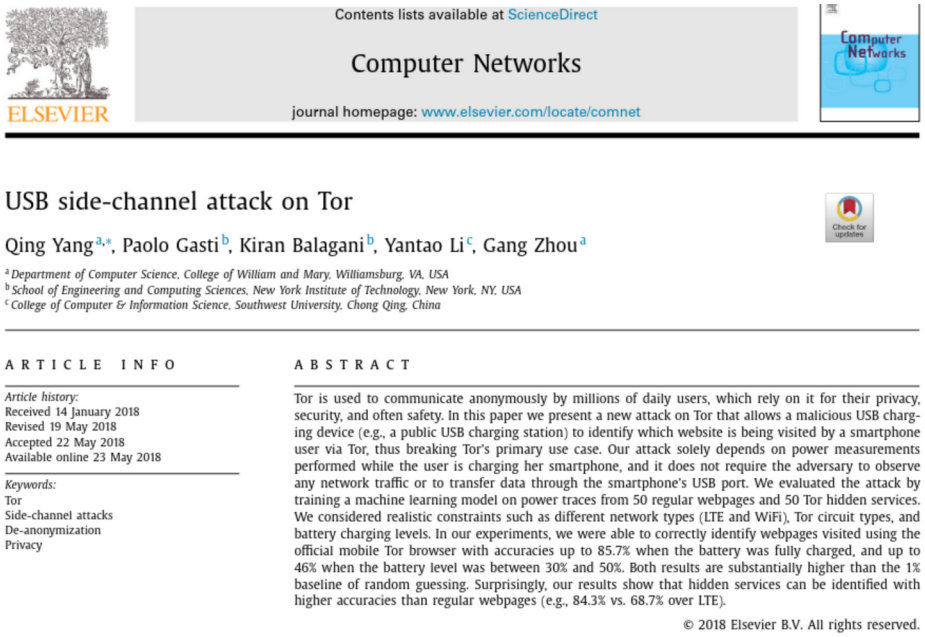
- Before keyboards, devices similar to teleprinters were used to **transmit** and **type** text data
- Up until the invention of mouse, keyboard remained the primary point of interacting with computers
- Virtual keyboards are still used in smart-phones, etc.

Side Channel Attacks

- **Definition**: Unconventional channels used to attack.
- Any physical phenomenon could be seen as a channel (e.g. power consumption, time, sound)
- One early example was Van Eck phreaking. Electromagnetic radiation leak information.

Example: Side Channel Attacks

Without observing the network traffic (which is encrypted), attacker could identify which web pages user is observing (USB Side Channel Attack)



Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

USB side-channel attack on Tor

Qing Yang[a,*], Paolo Gasti[b], Kiran Balagani[b], Yantao Li[c], Gang Zhou[a]

[a] Department of Computer Science, College of William and Mary, Williamsburg, VA, USA
[b] School of Engineering and Computing Sciences, New York Institute of Technology, New York, NY, USA
[c] College of Computer & Information Science, Southwest University, Chong Qing, China

ARTICLE INFO

Article history:
Received 14 January 2018
Revised 19 May 2018
Accepted 22 May 2018
Available online 23 May 2018

Keywords:
Tor
Side-channel attacks
De-anonymization
Privacy

ABSTRACT

Tor is used to communicate anonymously by millions of daily users, which rely on it for their privacy, security, and often safety. In this paper we present a new attack on Tor that allows a malicious USB charging device (e.g., a public USB charging station) to identify which website is being visited by a smartphone user via Tor, thus breaking Tor's primary use case. Our attack solely depends on power measurements performed while the user is charging her smartphone, and it does not require the adversary to observe any network traffic or to transfer data through the smartphone's USB port. We evaluated the attack by training a machine learning model on power traces from 50 regular webpages and 50 Tor hidden services. We considered realistic constraints such as different network types (LTE and WiFi), Tor circuit types, and battery charging levels. In our experiments, we were able to correctly identify webpages visited using the official mobile Tor browser with accuracies up to 85.7% when the battery was fully charged, and up to 46% when the battery level was between 30% and 50%. Both results are substantially higher than the 1% baseline of random guessing. Surprisingly, our results show that hidden services can be identified with higher accuracies than regular webpages (e.g., 84.3% vs. 68.7% over LTE).

Yang, Q., Gasti, P., Balagani, K., Li, Y., & Zhou, G.

Historic Example: Operation Gunman

- KGB embedded bugs within IBM selectric typewriters used in U.S. Embassy, one of the earliest cases of hardware keyloggers.
- Every keystroke was captured and stored in memory.
- When memory became full, contents were broadcasted periodically via radio bursts to nearby listening stations.
- Used for nearly eight years before being discovered.

Keylogging

Definition: Practice of recording the keys a person types on the keyboard.

Keystrokes can be identified and detected through various ways:

- WiFi signal
- Electromagnetic emanations
- CPU cache usage (e.g. a program running on host machine to measure CPU load)
- Network traffic patterns (packet length, timing, direction)

Trivial countermeasures:

- Reduce emanations (e.g. use shields to prevent emanations from leaking)
- Mask typing behavior (e.g. white noise)

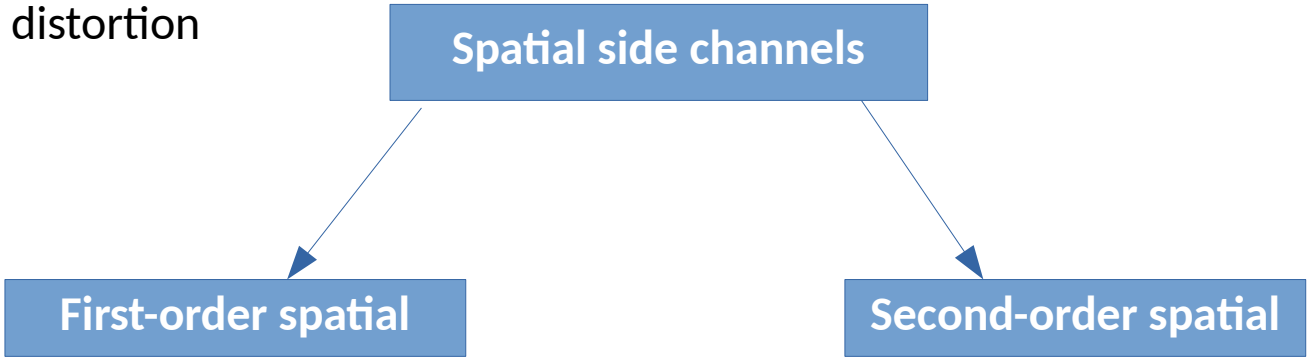
Side channel attacks may leverage:

- **Temporal information** (Keystroke timing is used to detect which keys are pressed)
- **Spatial information** (Spatial information is used to detect physical location of the keys)

Spatial Side Channels

Spatial side channel attacks can be performed through:

- Acoustic localization
- Video of the keyboard
- WiFi signal distortion



Two categories:

- **First-order**: reveals location of physical keys
- **Second-order**: provides only distance between keys (e.g. measuring acoustic similarity between two keys.

Spatial Side Channels (cont.)

- Keys within spatial proximity produce similar sounds.

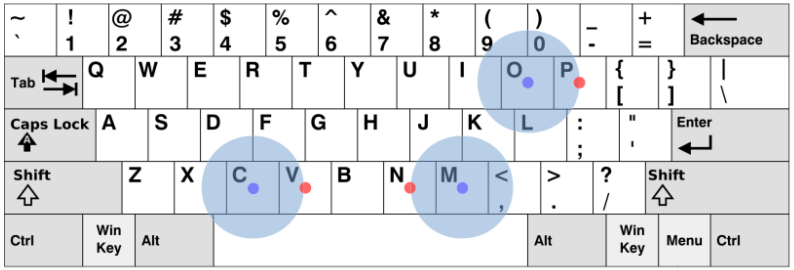


Figure (a)

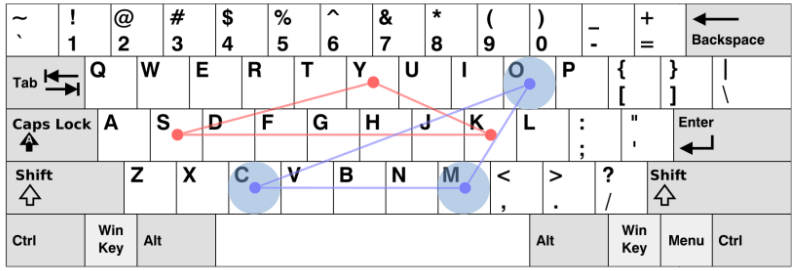


Figure (b)

Figure (a) shows 1st order spatial side channel while Figure (b) reveals 2nd order spatial side channel.
SoK: Keylogging Side Channels. (2018)

Disadvantage of Spatial Side Channels:
Spatial side channels are incapable of revealing individual keys.

Temporal Side Channels

In temporal keylogging, sequence of keystroke timings for press and release is used to predict the keys.

t^P = timing for key press t^R = timing for key release

Full keystroke is composed of two elements:

Full Keystroke = Key press + Key release

A Keystroke has three three element within its tuple: **key release** (t^R), **key press** (t^P) and **key** (k):

$$(t^p, t^r, k)$$

Advantage: Unlike spatial side channels, temporal side channels can identify individual keys!

Keylogging (cont.)

Keyboards communicate via host/computer through two ways:

- USB
- PS/2

→ **Encoding and transmission are different**

Several elements can affect precision and accuracy of measurement:

- **Physical delay**: Time from physical contact to between the user's finger and key cap to the point of actuation depends on characteristics of the keyboard. Elements which could possibly have an effect: actuation force, travel distance, etc.
- **Matrix scan rate**: The rate at which the microcontroller pulses the scanning lines in the keyboard matrix varies between keyboard models
- **Encoding**: Once key press is detected, it enters a sub-routine and it is converted to digital signal to be transmitted to the host. Delay could be used to have a narrow list of possible keys.

Keylogging (cont.)

- **Process Scheduling**: The kernel must receive scan-code and acknowledge the interrupt which adds time delay.

- **Polling rate**: Limited to USB keyboards only. PS/2 keyboards are interrupt-based, therefore do not suffer from polling delays.

Keyboards can emit different signals:

- **Acoustic**: Acoustic sound is emitted upon pressing each key which can be captured up to several meters away. In supervised approach, known waveforms can be compared to unknown ones to identify individual keys.

- **Seismic**: Vibrations which can be captured and transmitted via mobile device nearby or laser microphone.

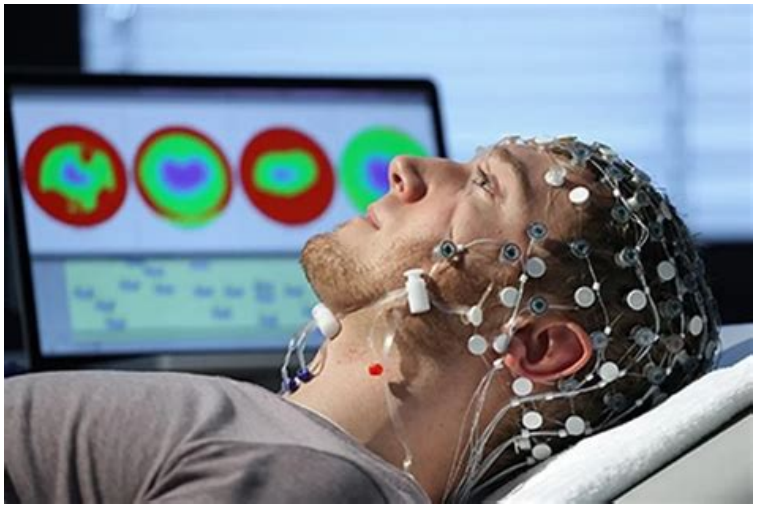
- **Electromagnetic radiation**: EM spikes enable keys to be identified by their "falling edge" scancode.

e.g. Letter E Bit pattern: 00010010011 Falling edge: ↓ ↑ ↑ ↑ ↓ ↑ ↑ ↓ ↑ ↑ ↑

EEG (electroencephalogram)

What is EEG?

a test that measures electrical activity in the brain



Attack scenario:

By observing electrical activity of the brain, attacker could learn information.

Possible defense:

User could induce fake responses to protect his real thoughts by thinking of irrelevant keys.

Acoustic Side Channel

Two modes:

- **Local**: Listening device is placed near victim (traditional approach)
- **Remote**: Attacker captures audio remotely (e.g. VoIP)

We have better approaches to attack the victim in local setting (e.g. shoulder surfing)

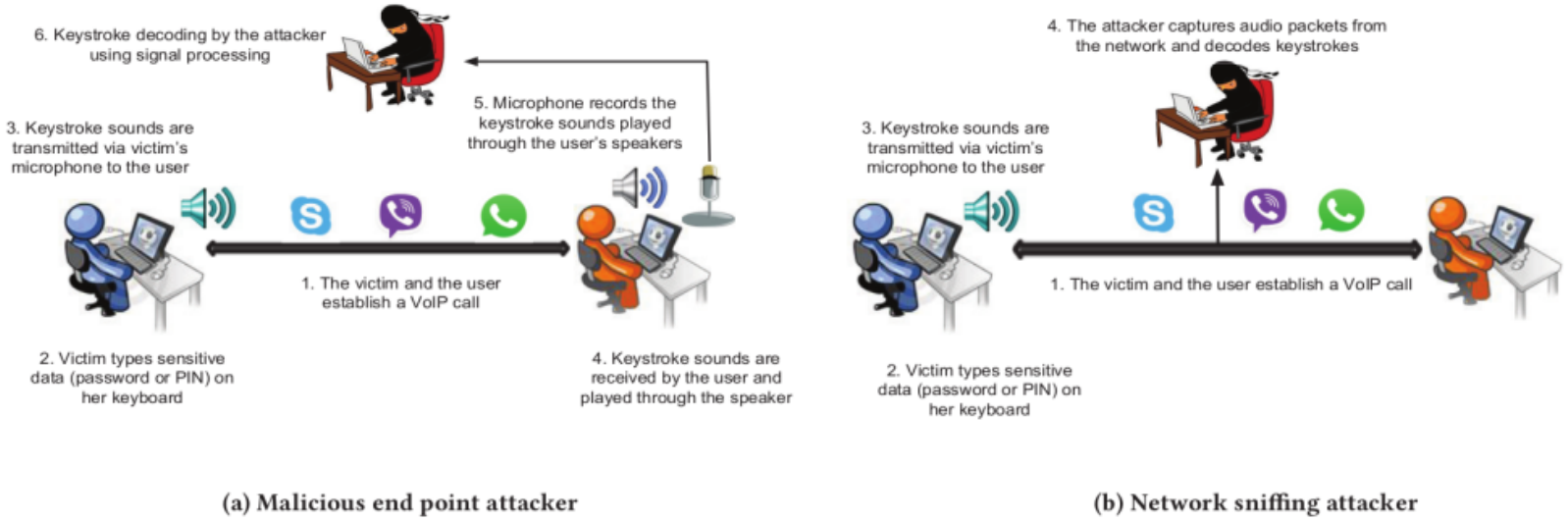
Acoustic Side Channel

Scenario: Victim is typing sensitive information while on a VoIP call.

How can the attacker build the training set?

- Use social engineering techniques to ask user to login to a website or web application to authenticate himself.
- Coercing the victim to send an email while on the call
- Online editing of a shared document

Attack Scenarios



Anand, S. A., & Saxena, N. (2018).

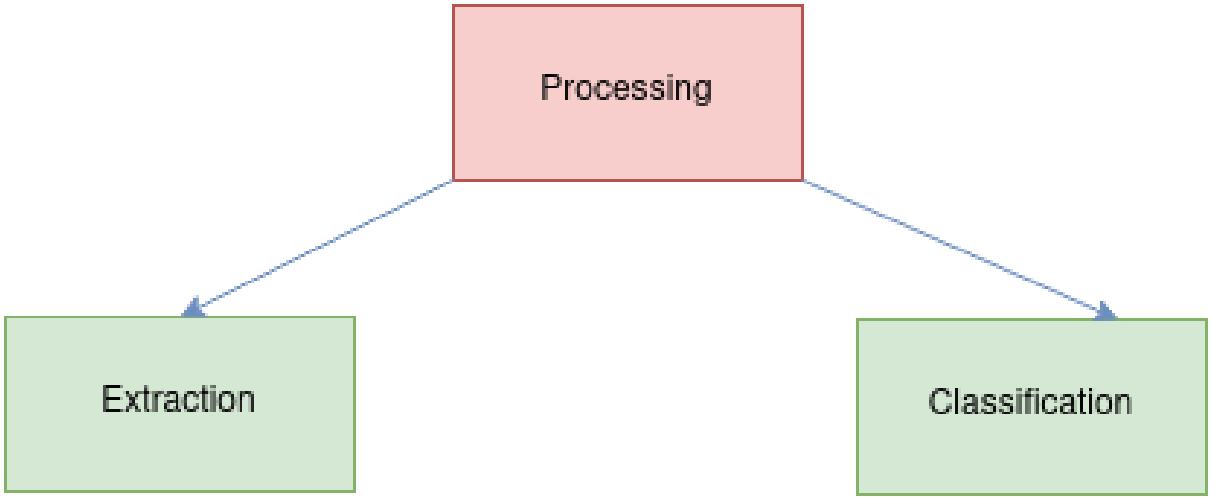
We have the two scenarios:

a) Malicious entity collects audio samples by communicating with victim

b) Malicious entity sniffs and captures audio packets from the network.

Processing

Keystroke processing is divided into two stages:



Keystroke extraction: Attacker has to collect audio samples whether remotely or locally from the victim.

Keystroke classification: After collecting audio samples, attacker has to identify which audio correlates with what key.

Classification

Different methods could be used for classification:

- Mel-frequency cepstral coefficients (**MFCCs**)
- Fast Fourier transform (FFT) coefficients
- Frequency distance measure
- Frequency time-distance measure
- ....

Machine learning method using MFCC performs better (accuracy) for both alphabet and numpad keys.

Table 1: Single key classification using time-domain and frequency-domain distance estimates

Classification Method	Accuracy (in %)
Alphabet keys (a-z)	
Cross-correlation	56.00
Frequency Distance	64.70
Frequency Time	**67.30**
Numpad keys (0-9)	
Cross-correlation	73.30
Frequency Distance	70.00
Frequency Time	**83.30**

Table 2: Single key classification using FFT coefficients

Classification Algorithm	Accuracy (in %)
Alphabet keys (a-z)	
J48	15.79
Random Forest	32.35
Linear Nearest Neighbor Search	20.92
SMO	21.95
Simple Logistic Regression	**39.54**
Multinomial Logistic Regression	**38.89**
Numpad keys (0-9)	
J48	39.67
Random Forest	49.67
Linear Nearest Neighbor Search	42.33
SMO	38.67
Simple Logistic Regression	**53.00**
Multinomial Logistic Regression	**53.67**

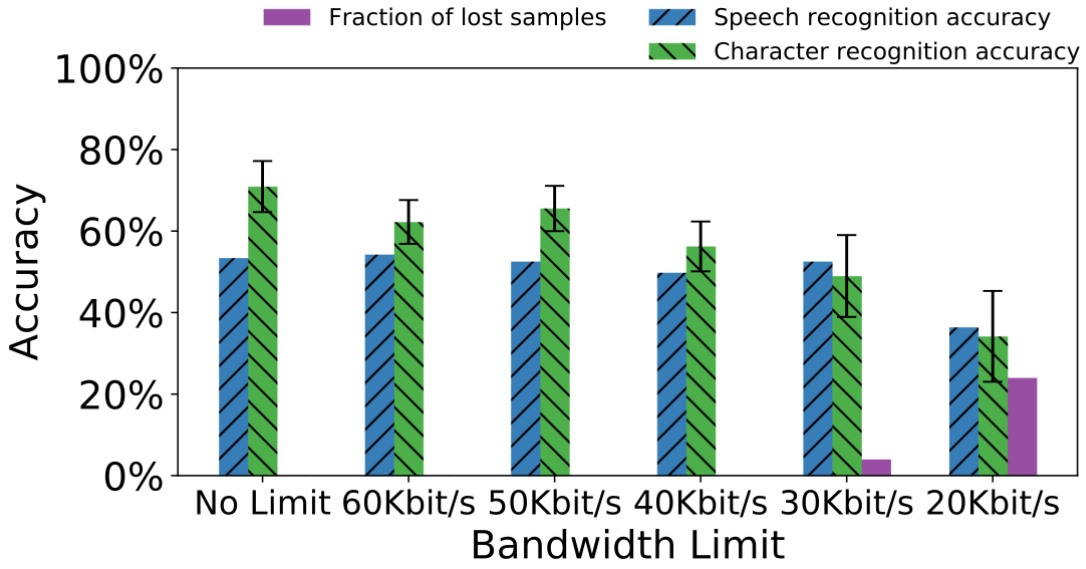
Table 3: Single key classification using MFCC

Classification Algroithm	Accuracy (in %)
Alphabet keys (a-z)	
J48	34.40
Random Forest	66.88
Linear Nearest Neighbor Search	53.91
SMO	**74.33**
Simple Logistic Regression	**73.17**
Multinomial Logistic Regression	62.52
Numpad keys (0-9)	
J48	44.67
Random Forest	**73.67**
Linear Nearest Neighbor Search	62.00
SMO	**77.33**
Simple Logistic Regression	**70.67**
Multinomial Logistic Regression	56.33

Additional Defense: Bandwidth

Bandwidth:

- Classification suffers noticeable loss under 40kbit/s → Attacker's capability to decode is degraded.
- Transmission of audio signal from victim's side to attacker's side affects the accuracy of the classifier. VoIP application by default encode and compress signals, therefore classifier might be affected by It.



Cecconello, S., Compagno, A., Conti, M., Lain, D., & Tsudik, G. (2019).

Defenses against attacks

	Modality	Defense	Method	Target	Channels Protected			Noticeable to User?	Ref.
					S1	S2	T		
User	EEG	Induce covert responses to irrelevant stimuli	Obfuscate	ID	✓	✓		✓	[71], [81]
	EEG	Filter keystroke-identifying features	Impede	DET	✓	✓	✓		[71], [82]
	Motion	Limit sensor permissions during typing	Impede	DET	✓	✓	✓		[51]
Keyboard	Acoustic	Reduce keyboard acoustic emanations	Impede	DET	✓	✓	✓	✓	[54]
	Acoustic*	Keys produce homomorphic sounds	Obfuscate	ID	✓	✓			[54]
	Acoustic*	Emit synthetic keyboard sounds	Conceal	DET	✓	✓	✓	✓	[9], [83]
	EM Rad./Cap.	Filter/shield EM emanations	Impede	DET	✓	✓	✓		[3], [84]
	EM Rad.	Randomly delay matrix scan routine	Obfuscate	DET	✓	✓	✓		[85]
	EM Rad.	Randomize matrix scan pattern	Obfuscate	ID	✓	✓			[86]
Host	CPU/Memory	Generate spurious key press/release events	Conceal	DET	✓	✓	✓		[10]
	CPU/Memory	Decrease timer resolution	Obfuscate	DET			✓		[87], [88]
Net.	HTTP	Obfuscate packet size through padding	Obfuscate	ID	✓	✓			[68]
	SSH/VoIP	Randomly delay key press/release events	Obfuscate	ID			✓	Maybe	[89], [90]

- **Obfuscate**: Decrease the SNR to make information content low for key identification. For instance user could add background noise.
- **Impede**: Restrict access to a sensor or shield emanations coming from it. Example: physical shielding
- **Conceal**: Adding redundant information. (e.g. fake keystroke sounds)

Additional Defense: Speech

During each entry of Password/PIN, user read a piece of text from an English newspaper.

Passwords: Using top 5 matching character list, only 2 out of 6 characters were decoded

PINS: 3 out of 4 PINS were decoded correctly

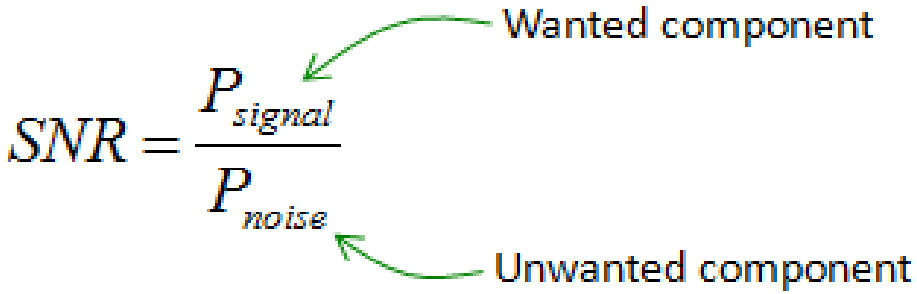
In terms of performance:

Disadvantage: User has to converse to mask his keystroke emanations (Usability)

Additional Defense: Audio Masking

Audio Masking: Cloak sensitive sound by injecting additional sound.

- The main idea is to reduce *SNR* (signal-to-noise ratio):



- Lower SNR → More difficult to filter signal from noise
- In this context: Keyboard emanations are the signal and background sound will be the noise.

Audio Masking (cont.)

Possible defense solutions:

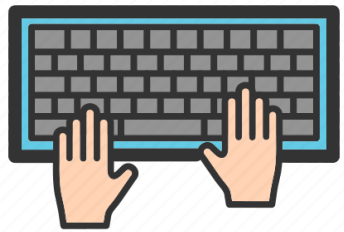
- White noise:

  Definition: Random signal with equal intensities at different frequencies

  Application: Used in meetings to mask conversations,

  by students to study to mask nearby chatter, etc.

  Disadvantage: Susceptible to filtering by most applications and microphones and not very effective



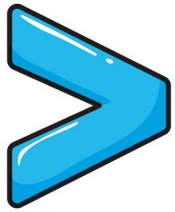
- Masking via fake keystrokes:

  Fake keystrokes in the same frequency spectrum, so that

  it overlaps with real keystroke sounds

Fake keystroke vs. White Noise

Fake keystrokes are more effective as a cloak compared to using white noise.



White Noise has no effect on the accuracy of the attack:

- Out of the 180 decoded characters, 16 characters were decoded successfully.
- Using top-5 matching list, percentage of accuracy increased to 67.2%

Case Study: Bayrob Group

- Installed malware on users device that would show fake eBay pages for products like cars.
- Blocked websites such as Crime Complaint Center of FBI to prevent citizens from filing report.
- Fake vehicle history and delivery services were created.
- In the beginning malware was tailored for each vicitm.
- They had very strong OPSEC (e.g. radio noise to mask keyboard sounds).

#RSAC

Some good rules

1. Don't talk openly	1. OTR, radio noise, no phone talk ✓
2. Don't operate from home	2. Stolen wifi, hacked routers, proxies, TOR ✓
3. Encrypt everything	3. SFTP, SSH, PGP, OTR, LUKS, Truecrypt,+ ✓
4. No logs	4. Logging disabled ✓
5. Create Personas	5. Hacker Handles ✓
6. Don't contaminate	6. Isolated hacking environment ✓
7. Don't trust	7. Built all tech themselves ✓
8. Be paranoid	8. Triple encrypted drives, proxychaining ✓
9. Don't talk to police	9. A lot of pressure ✓
10. Don't give people power over you	10. Limited inner circle ✓

Conclusions

- It is not possible to completely eliminate keylogging side channels attacks.
- Different layers and communications channels require different protection mechanisms. No perfect solution exists.
- Protection mechanisms must be considered by acknowledging a user's threat model and adversary's capabilities (challenging objective).
- Security is the goal, but usability of the user should be considered as well.