Identification of Pressed Keys by Acoustic Transfer Function

IEEE International Conference on Systems, Man, and Cybernetics - SMC2015

Gerson de Souza Faria Hae Yong Kim

Escola Politécnica, Universidade de São Paulo, Brazil

Presentation: Prof. Reinaldo A. C. Bianchi, Centro Universitário FEI, Brazil

October 10, 2015

Program

Program

Introduction : problem statement

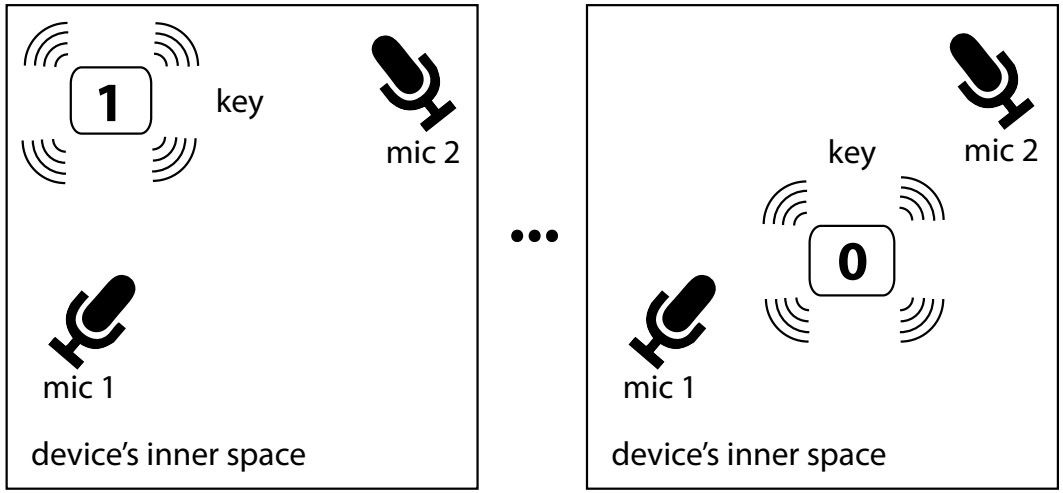
- The interaction between human beings and PIN-pads (which deal with $) can leak sensitive information in unsuspected ways.
- The sound of the keystrokes captured by two microphones discloses the pressed key with 99% of accuracy in some models.
- Brand new devices are currently vulnerable to the attack here presented (**certification failure**).

Program

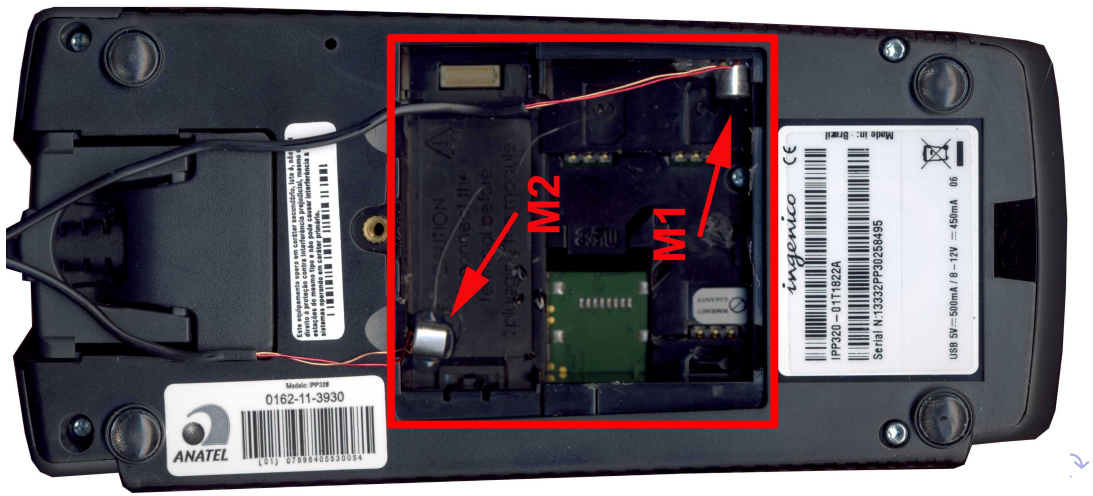
Acoustic Model

Hypothesis

The device's empty space, the locations of the two microphones and the sound sources form a linear time-invariant system. The only variables are the sound sources (locations of keys).



system '1' system '0'



Acoustic Transfer Function (ATF)

We consider one microphone signal x as input and the other y as output of a linear system.

There are ten systems, one for each key.

The system of a key k is given by the convolution in time domain or multiplication in frequency domain:

$$y(t) = h_k(t) * x(t)$$

$$\text{Fourier transform} \updownarrow$$

$$Y(f) = H_k(f) \cdot X(f)$$

Acoustic Transfer Function (ATF)

The transfer function vectors $H_k(f)$ characterize the key k. It can be estimated using Welch's Averaged Periodogram.

Matlab function `tfestimate` implements this method.

The features we use are the magnitudes of the transfer function vectors.

We reduce the original dimension 257 to 30-50 through PCA (*Principal Component Analysis*).

We use them to train a Neural Network.

Program

Acoustic Transfer Function (ATF)

Ingenico iPP320 experiment

1st vulnerability

SAM compartment provides the space for installing the bugs and a unique acoustic property for each key.

2nd vulnerability

The “click” sound emitted by the key is filtered by the acoustic system, yielding an identifiable transfer function.

1st vulnerability

SAM compartment provides the space for installing the bugs and a unique acoustic property for each key.

2nd vulnerability

The "click" sound emitted by the key is filtered by the acoustic system, yielding an identifiable transfer function.

Acoustic Transfer Function (ATF)
Ingenico iPP320 experiment

1st vulnerability

SAM compartment provides the space for installing the bugs and a unique acoustic property for each key.

2nd vulnerability

The “click” sound emitted by the key is filtered by the acoustic system, yielding an identifiable transfer function.

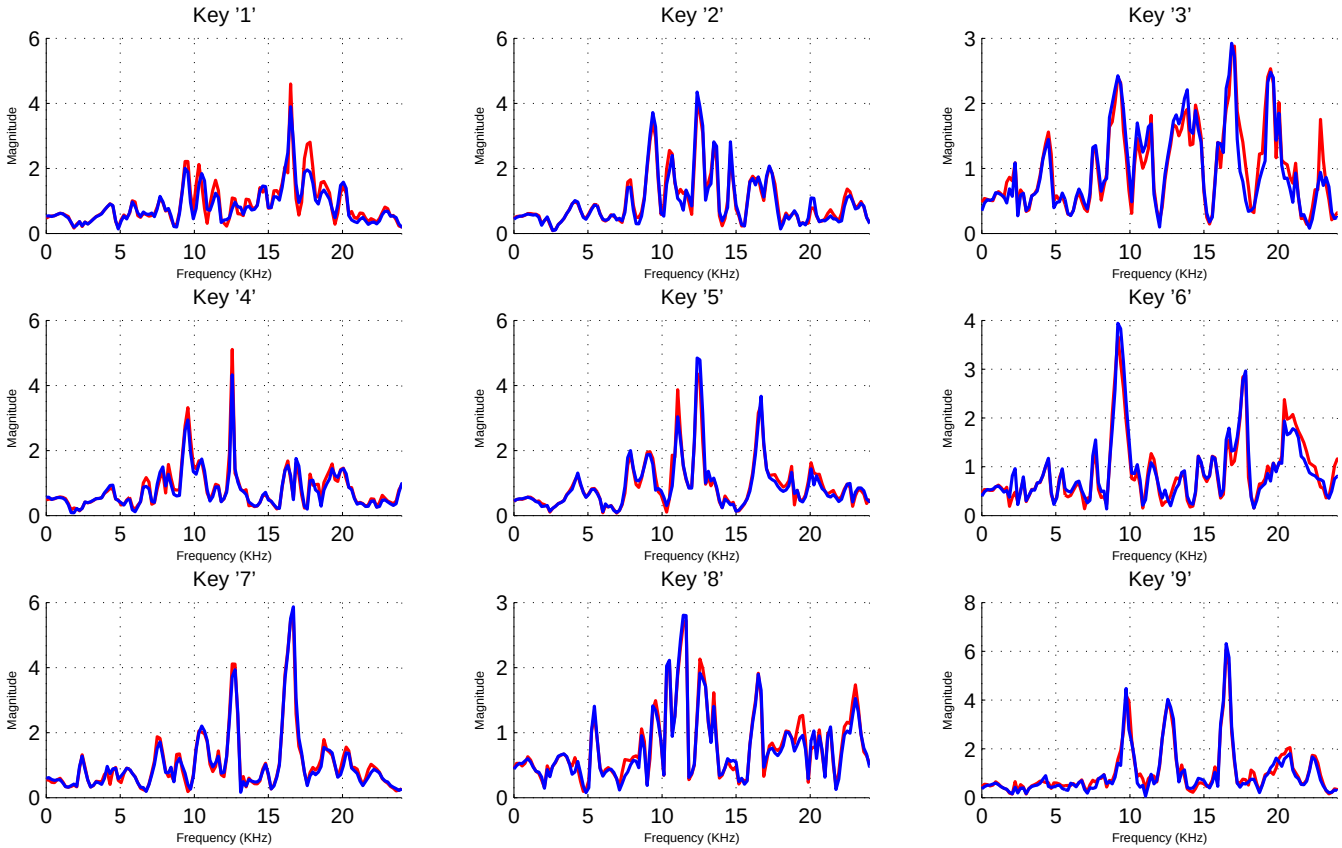
Acoustic Transfer Function (ATF)
Ingenico iPP320 experiment

Two people pressed the keys ‘0’ to ‘9’ many times.

We computed an average transfer function for each person and key.

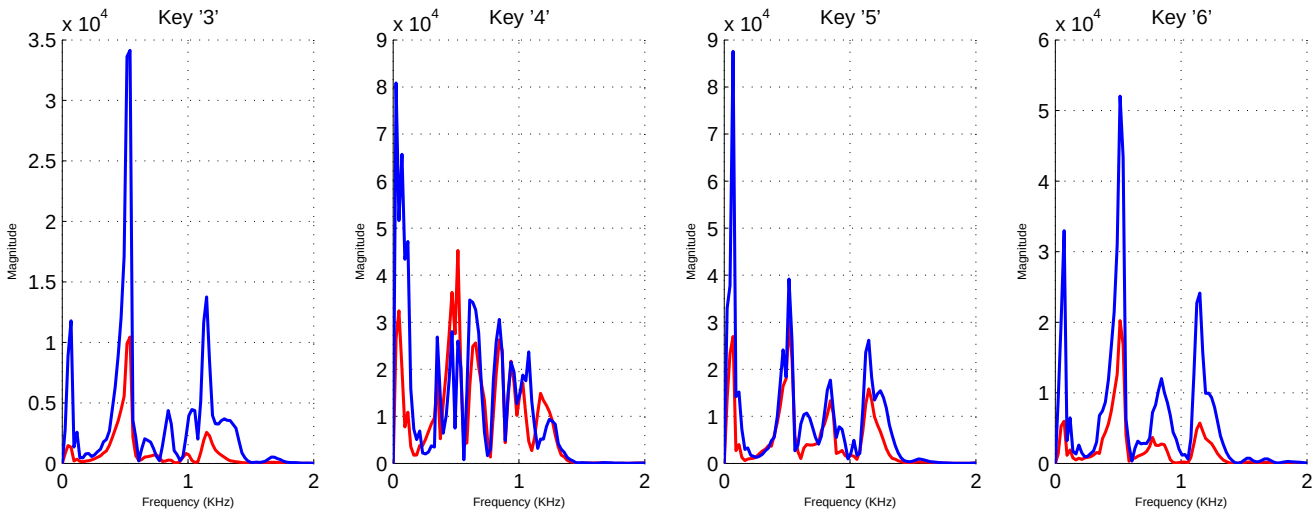
Acoustic Transfer Function (ATF)
Ingenico iPP320 experiment

Transfer functions are similar between persons and distinct between keys. Ideal for the attack.



Acoustic Transfer Function (ATF)

Ingenico iPP320 experiment



The classic frequency spectrum attack assumes that each key generates a specific sound spectrum.

Our experiments show that frequency spectra are very distinct between persons.

So, it is difficult to identify the pressed key by analyzing frequency spectrum.

Acoustic Transfer Function (ATF)

Ingenico iPP320 experiment

Key	1	2	3	4	5	6	7	8	9	0	Acc.(%)
1	**244**	1									99.6
2		**245**			1	3				1	98.0
3			**230**								100.0
4				**250**							100.0
5					**205**						100.0
6						**235**					100.0
7							**240**				100.0
8								**245**			100.0
9		1			1	2	1		**245**		98.0
0										**250**	100.0

The linear time invariant model was quite adequate for this experiment, with a classification accuracy of **99.6±0.8%.**

Acoustic Transfer Function (ATF)
PPC910 Experiment

1st vulnerability

There is room enough in the SAM compartment to install the bugs.

2nd vulnerability: Inexistent!

No “click” sounds when the keys are pressed, making it harder to attack the device.

1st vulnerability

There is room enough in the SAM compartment to install the bugs.

2nd vulnerability: Inexistent!

No "click" sounds when the keys are pressed, making it harder to attack the device.

Acoustic Transfer Function (ATF)
PPC910 Experiment

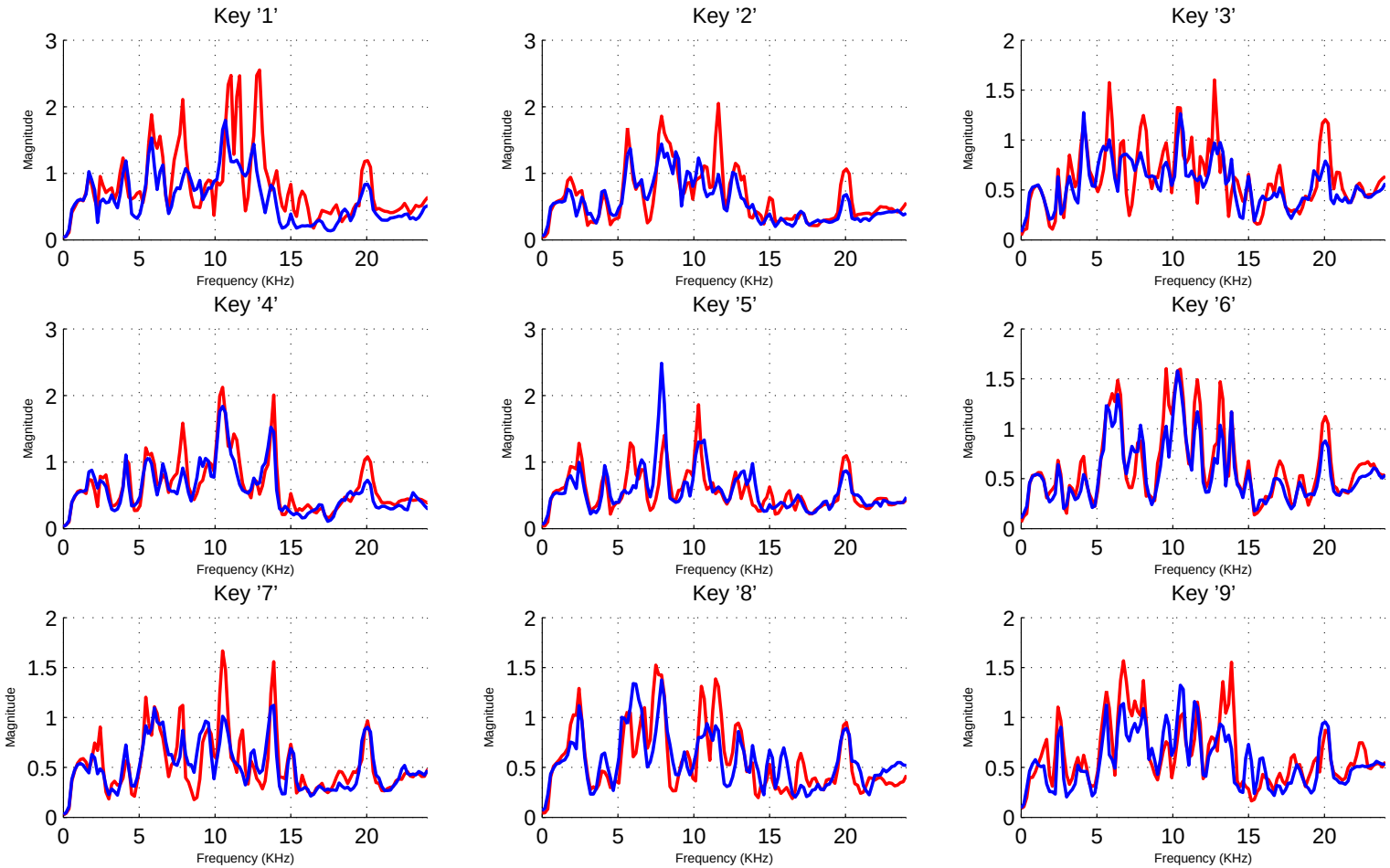
1st vulnerability

There is room enough in the SAM compartment to install the bugs.

2nd vulnerability: inexistent!

No “click” sounds when the keys are pressed, making it harder to attack the device.

Transfer functions different between the two persons.



Acoustic Transfer Function (ATF)
PPC910 Experiment

Key	1	2	3	4	5	6	7	8	9	0	Acc.(%)
1	**20**	28	10	32	9	2	7		21	1	15.4
2	3	**119**		13	11	7	6	7	26	13	58.0
3		3	**41**	11	8	1	1	4	12	9	45.6
4	1	10		**128**	9	1	3		6	7	77.6
5	3	8		23	**56**	1	19	15	50	5	31.1
6	1	14	2	11	5	**103**	9	3	7	10	62.4
7		17		20	16	3	**51**	1	5	17	39.2
8	1	14		6	12	1	9	**17**	3	37	17.0
9		33	3	15	3	10	3	48	**64**	1	35.6
0		1			4	3		1	16	**70**	73.7

We obtained a success rate of only **46±22%**, due to low signal to noise ratio (the “click” is barely audible).

Program

Conclusions

It is actually possible to steal PIN numbers from some PIN-pad models using this attack.

There are models quite vulnerable and models not as vulnerable to this attack.

There are two countermeasures to mitigate the possibility of this attack:

- The devices should not have a service compartment where bugs can be embedded.
- The keystrokes should not emit audible “clicks”.

Thank you!

gerson.faria@usp.br
hae@lps.usp.br