Sniffing Keystrokes With Lasers/Voltmeters

Side Channel Attacks Using Optical Sampling Of Mechanical Energy And Power Line Leakage

Andrea Barisani
Chief Security Engineer
<andrea@inversepath.com>

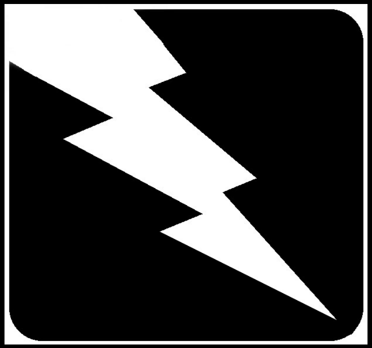
Daniele Bianco
Hardware Hacker
<daniele@inversepath.com>

INVERSE PATH
http://www.inversepath.com

Introduction

DISCLAIMER:

All the equipment and/or circuits and/or schematics provided in the presentation must be treated as examples, use the presented information at your own risk! Safety first!



Andrea Barisani <andrea@inversepath.com>
Daniele Bianco <daniele@inversepath.com>

Two Unconventional Attacks

- Attack 1: Power Line Leakage detection against wired PS/2 keyboards

- Attack 2: Optical Sampling of Mechanical Energy against laptop keyboards

Why bother ?

- Getting bored by software...hardware hacking is good fun!
- Unconventional side channel attacks
- Relatively cheap hardware
- FRIGGING LASER BEAMS!
- As always....more important: girls will melt when you show this...

- This is still a work in progress, we are planning to considerably refine the data/equipment presented in the next months

TEMPEST

- What is TEMPEST ?

  Transmitted **E**lectro-**M**agnetic **P**ulse / **E**nergy **S**tandards & **T**esting

  Tiny **E**lectro**M**agnetic **P**articles **E**mitting **S**ecret **T**hings

  The **E**missions **M**ight **P**roduce **E**xtremely **S**weet **T**alks

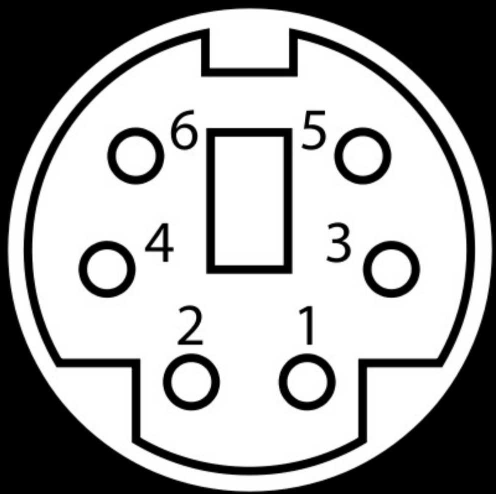
- Investigations and studies of Compromising Emanations or Fortuitous Leakage
- Unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose information
- The term was coined in the late 60's and early 70's as a codename for the NSA operation to secure electronic communications equipment from potential eavesdroppers

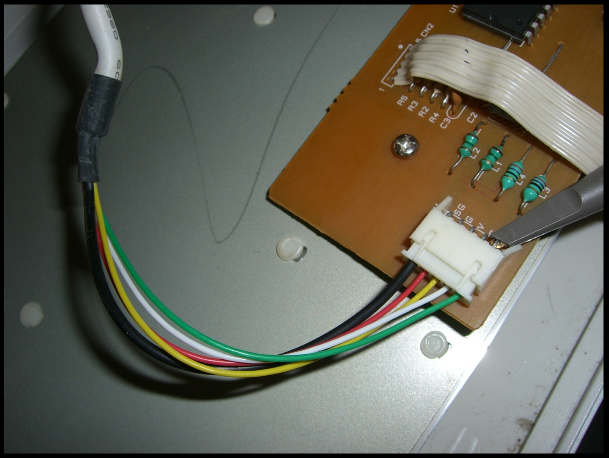
Public Research Relevant to Attack 1

- *Van Eck, Wim* (1985). "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?"
- *Kuhn, M.G.* (2002). "Optical time-domain eavesdropping risks of CRT displays"
- Kuhn, M.G. (2004). "Electromagnetic Eavesdropping Risks of Flat-Panel Displays"
- *J. Loughry, D. A. Umphress* (2002). "Information Leakage from Optical Emanations"
- *Martin Vuagnoux, Sylvain Pasini* (awaiting peer review) "Compromising radiation emanations of wired keyboards"

First Attack
Theory

- Keyboard PS/2 cable carries the following wires:
  - Pin 1 Data
  - Pin 3 Ground
  - Pin 4 +5 V DC
  - Pin 5 Clock
  - Pin 2/6 Unused





First Attack
Theory

- The wires are very close to each other and poorly shielded
- There is a fortuitous leak of information going from the data wire (as well as other sources) to the ground wire and/or cable shielding
- The ground wire is routed to the *main* power adapter/cable ground which is then connected to the power socket and then the electric grid

First Attack
Theory

- Information about the keystrokes leaks to the electric grid
- It can be detected on the power plug, including nearby ones sharing the same electric line
- The clock frequency of PS/2 signal is lower than any other component or signal emanated from the PC (everything else is tipically above the MHz)
- Isolate the leakage by filtering out the signal from the noise
- Profit!

First Attack Theory

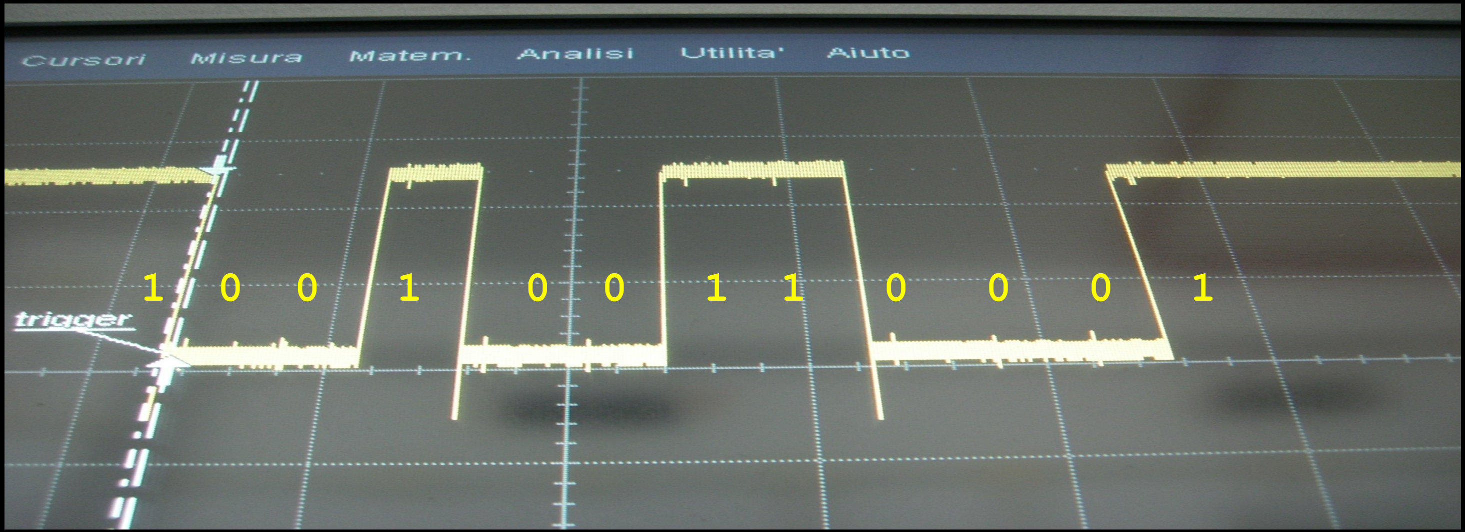
- There is some documentation suggesting the possibility of this attack in literature, though no extensive research is available (maybe some government agency...)
- While working on this research we had some independent confirmation, the cool preliminary results of *Martin Vuagnoux, Sylvain Pasini* also suggest that "the shared ground may acts as an antenna and significantly improve the range of the attack" (we look forward to read their paper!)

The PS/2 Signal

- Data is transmitted one bit at a time
- Each byte is sent in a frame consisting of 11-12 (h2d) bits

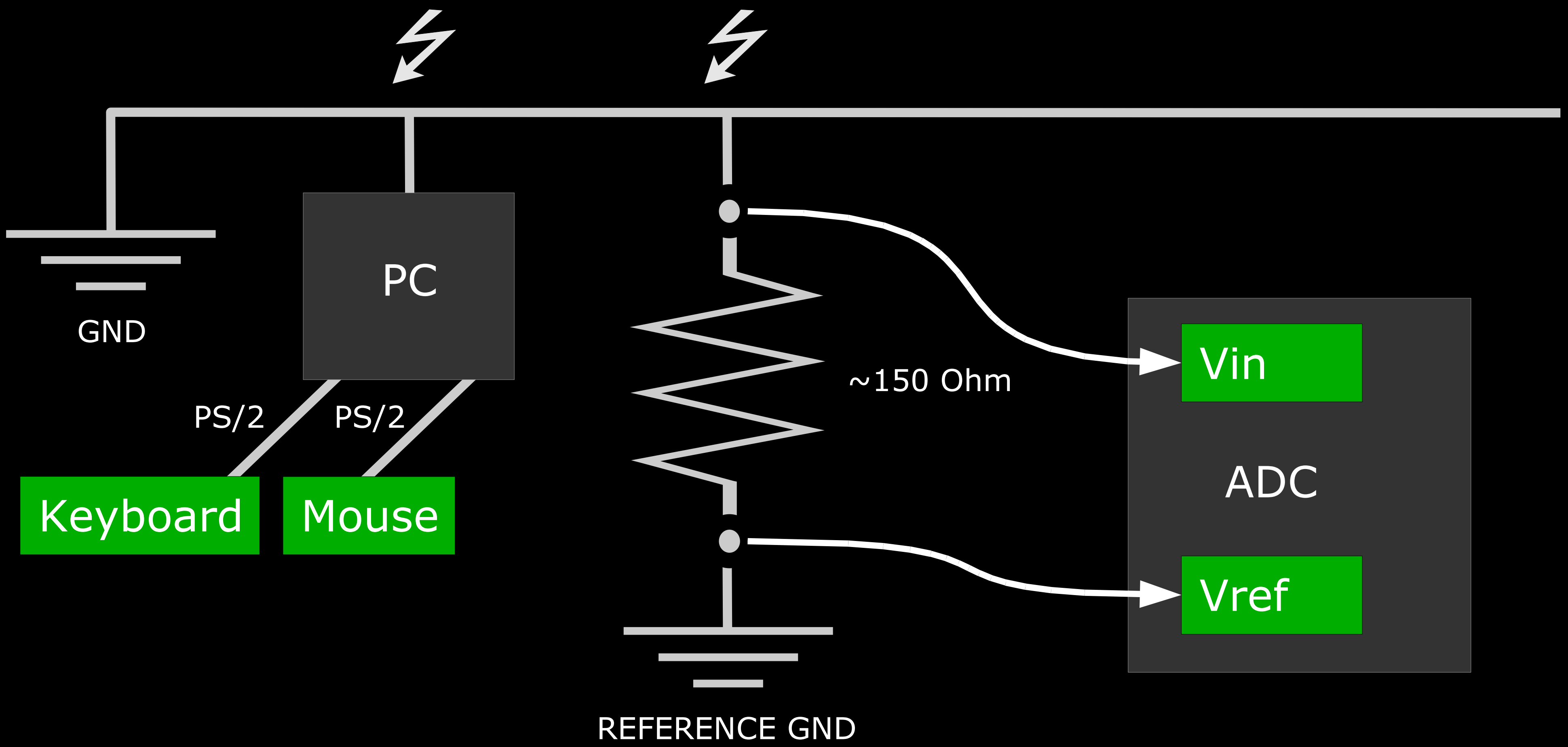
Start (1 bit)	Data (8 bits)	Parity (1 bit)	Stop (1 bit)	Ack (1 bit)

- Letter 'b' (scan code 32): `| 0 | 01001100 | 0 | 1 |`



- The clock frequency range is 10 - 16.7 kHz

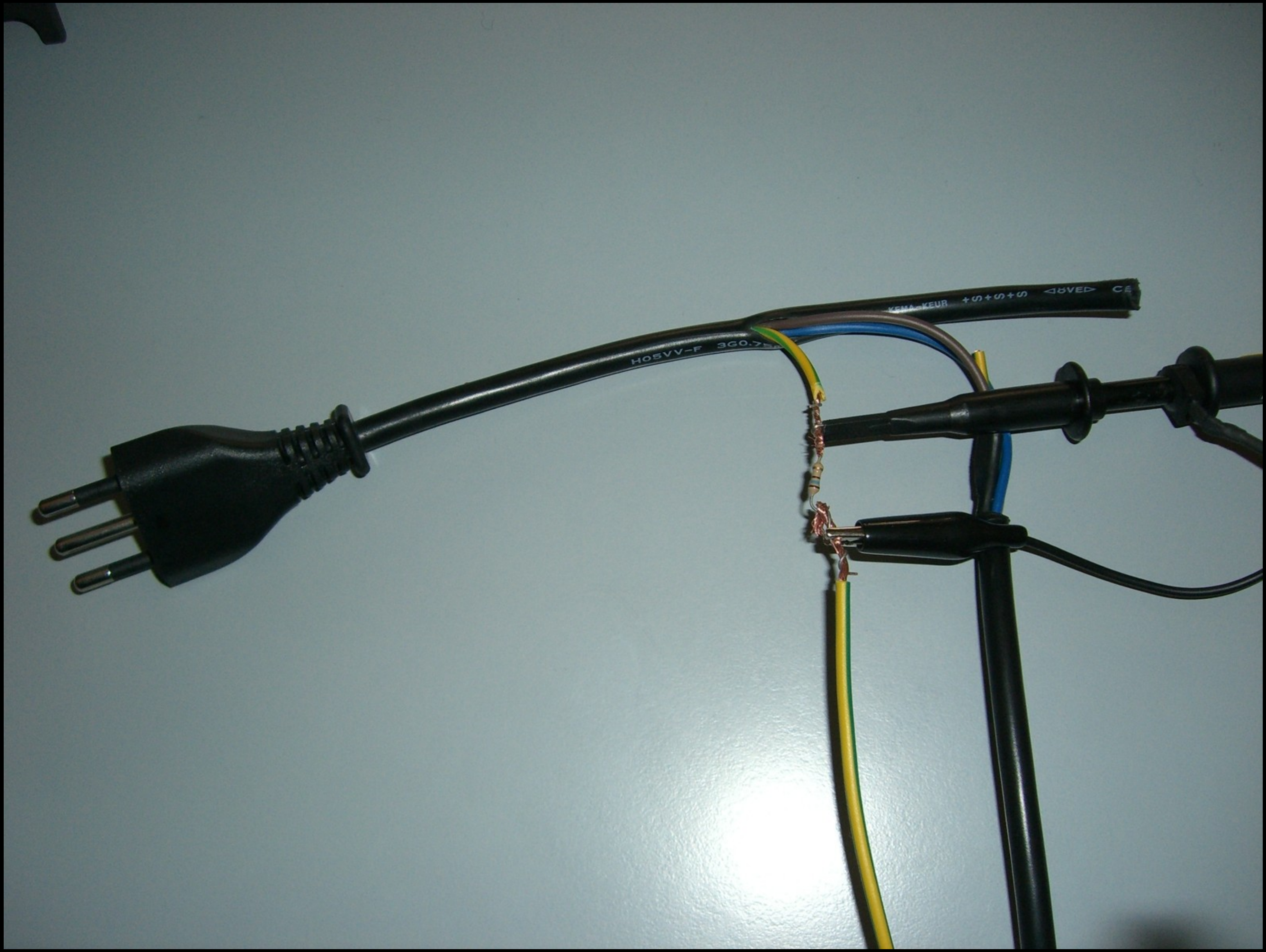
Diagram


GND
PC
PS/2
PS/2
Keyboard
Mouse
~150 Ohm
REFERENCE GND
Vin
ADC
Vref

Testing the Theory

- We used a digital oscilloscope as ADC for our initial test
- We route the ground of a nearby power socket to the ADC
- We measure the current dispersed on the ground using the voltage potential difference between the two ends of the resistor
- A “reference” ground clean of electrical system noise is used for improving the measurement (yes, it is weird)
- “nearby” power socket refers to anything connected to the same electrical system

The Evil Power Cable

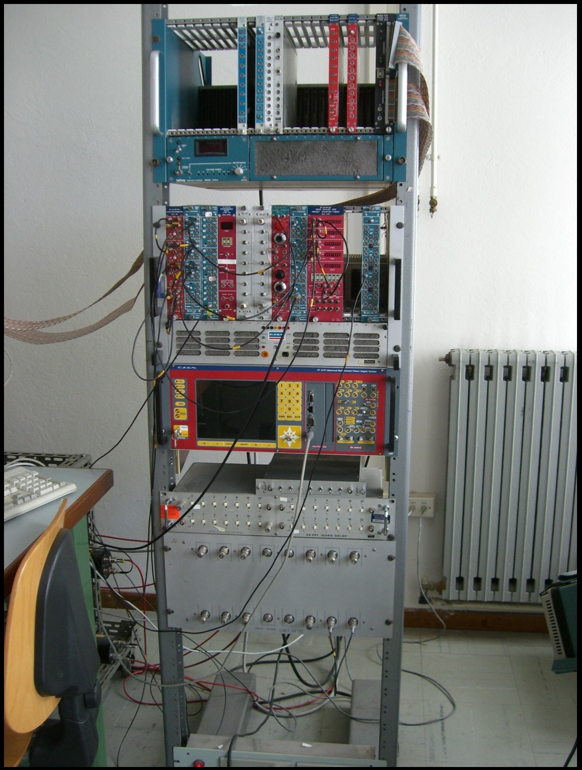


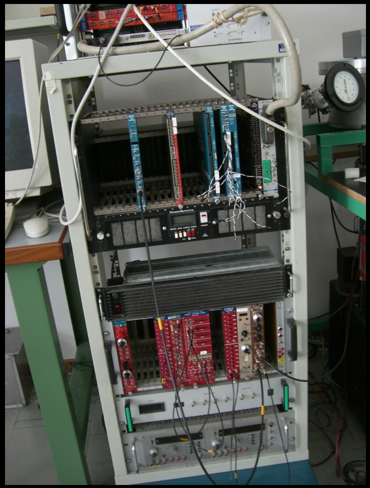
The Reference Ground

- Sinks and WC are perfect! (hint for spies: hotel rooms have those) ...very classy...

The Testing Lab

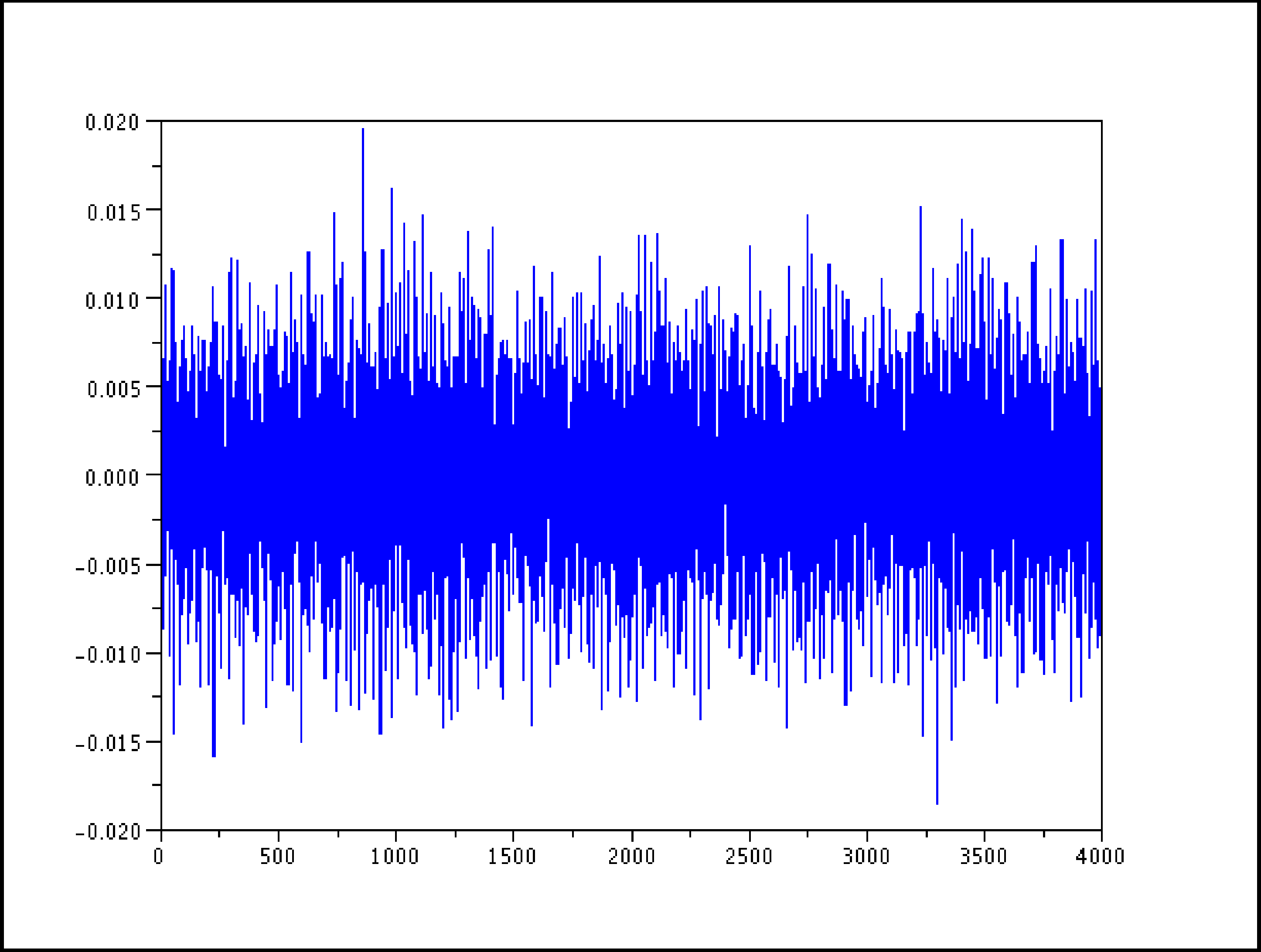
- The testing has been performed in a nuclear physics laboratory with lots of particle detectors, power adapters and other noisy equipment running
- Complex electric grid topology
- The ground was extremely noisy, substantially more than a normal scenario





Sniffing the Signals

- Original data



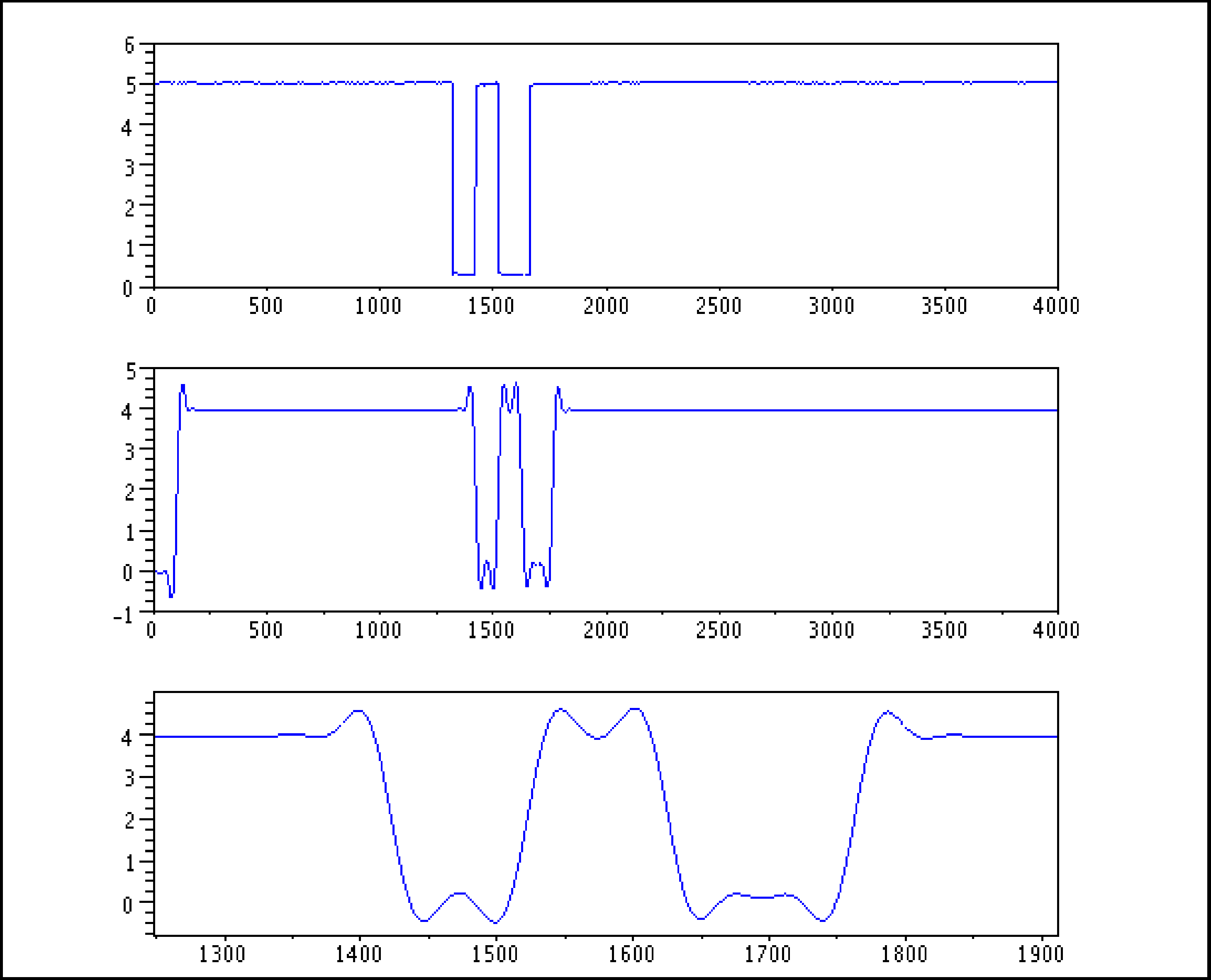
Filtering the Noise

- We need to find our 10 – 16.7 kHz signal among a huge amount of noise
- A Finite Impulse Response (FIR) acting as a Band Pass filter selecting frequencies between 1 – 20 kHz is used
- 1 Msps / 100 ksps is a sufficient rate for the analysis

- Scilab example:

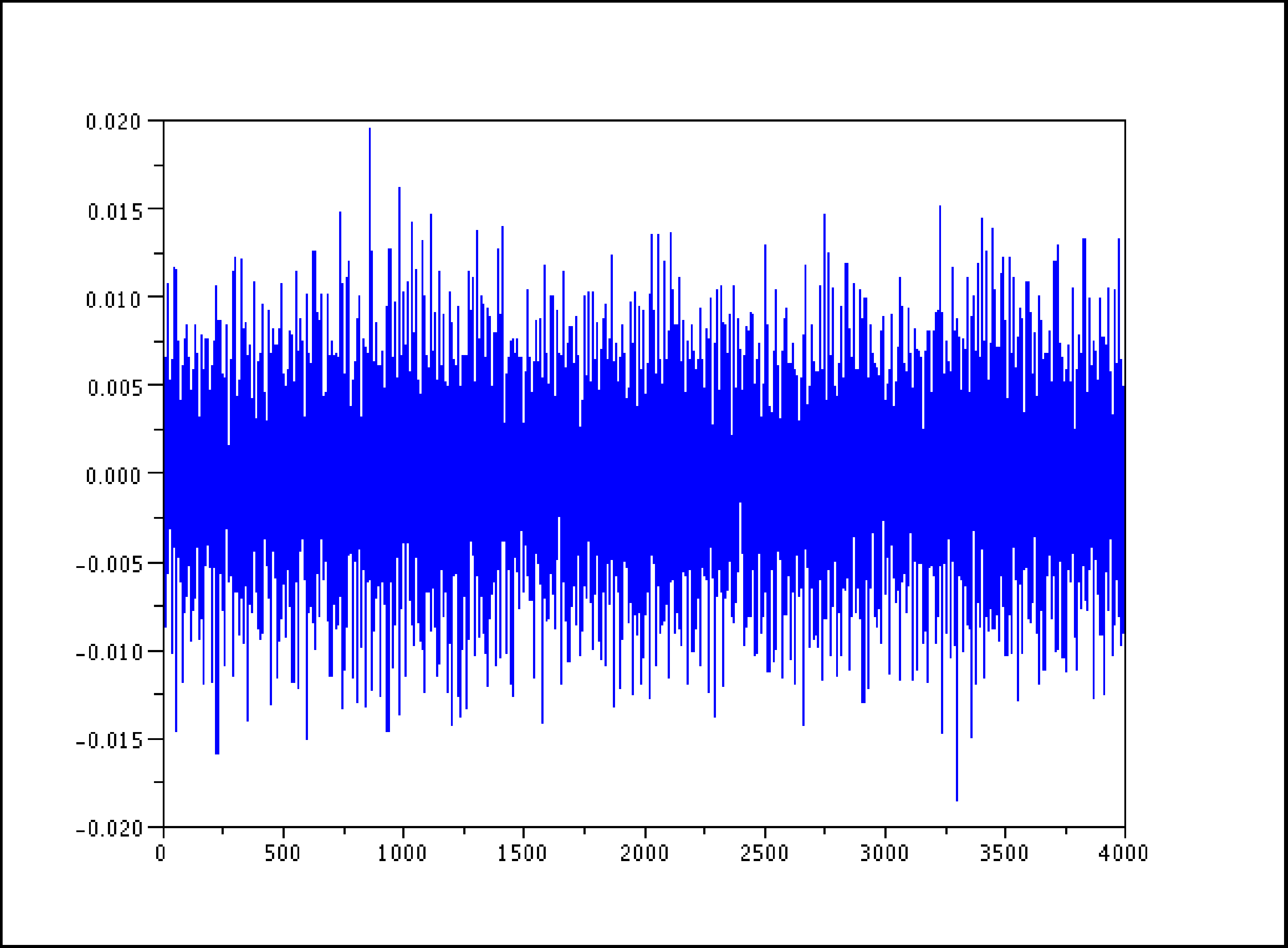
```
[h,filter_mag,fr] = wfir('bp',order,[.001,.02],'hm',[0,0]);
```

Filtering the Noise



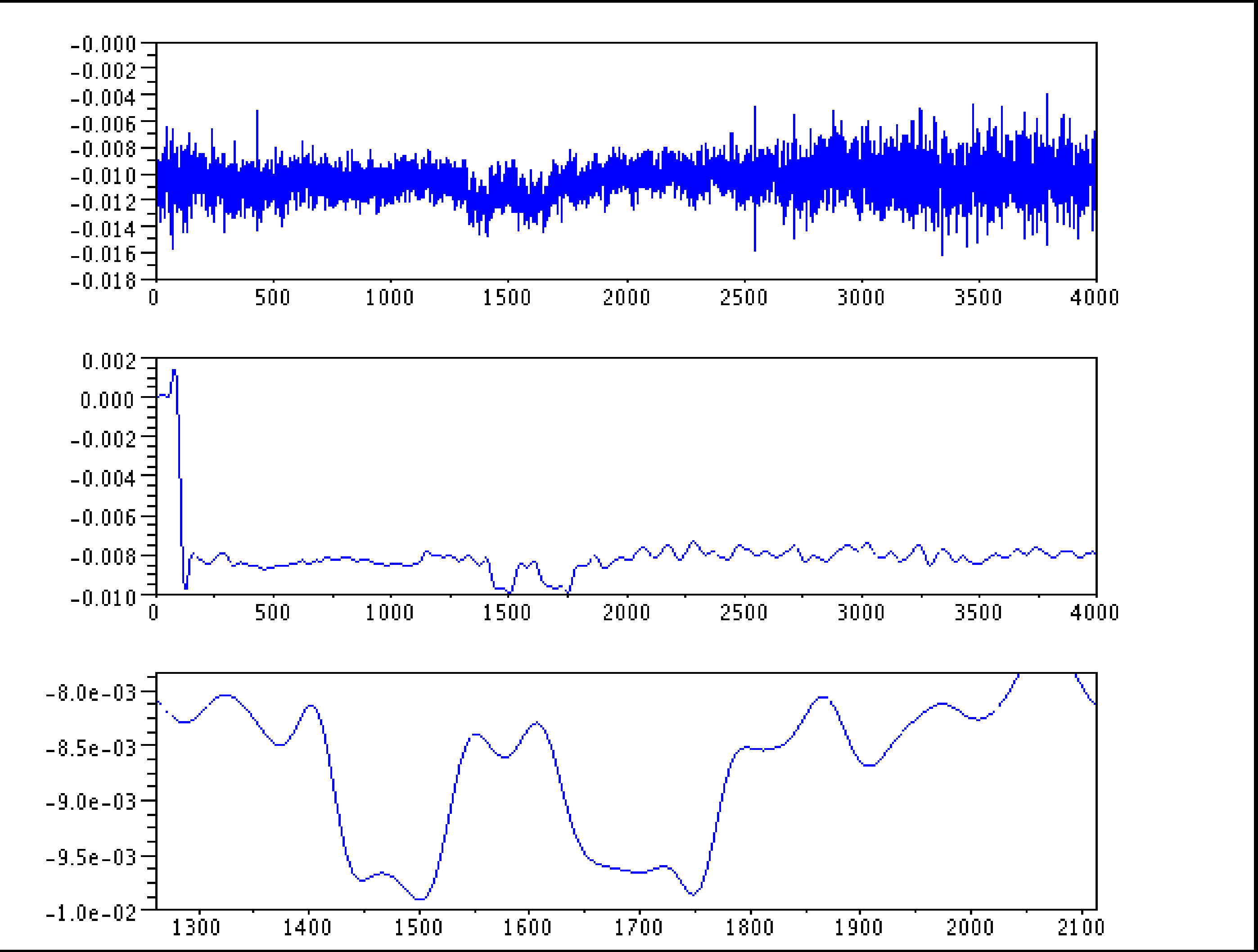
Results

- Noisy ground signal

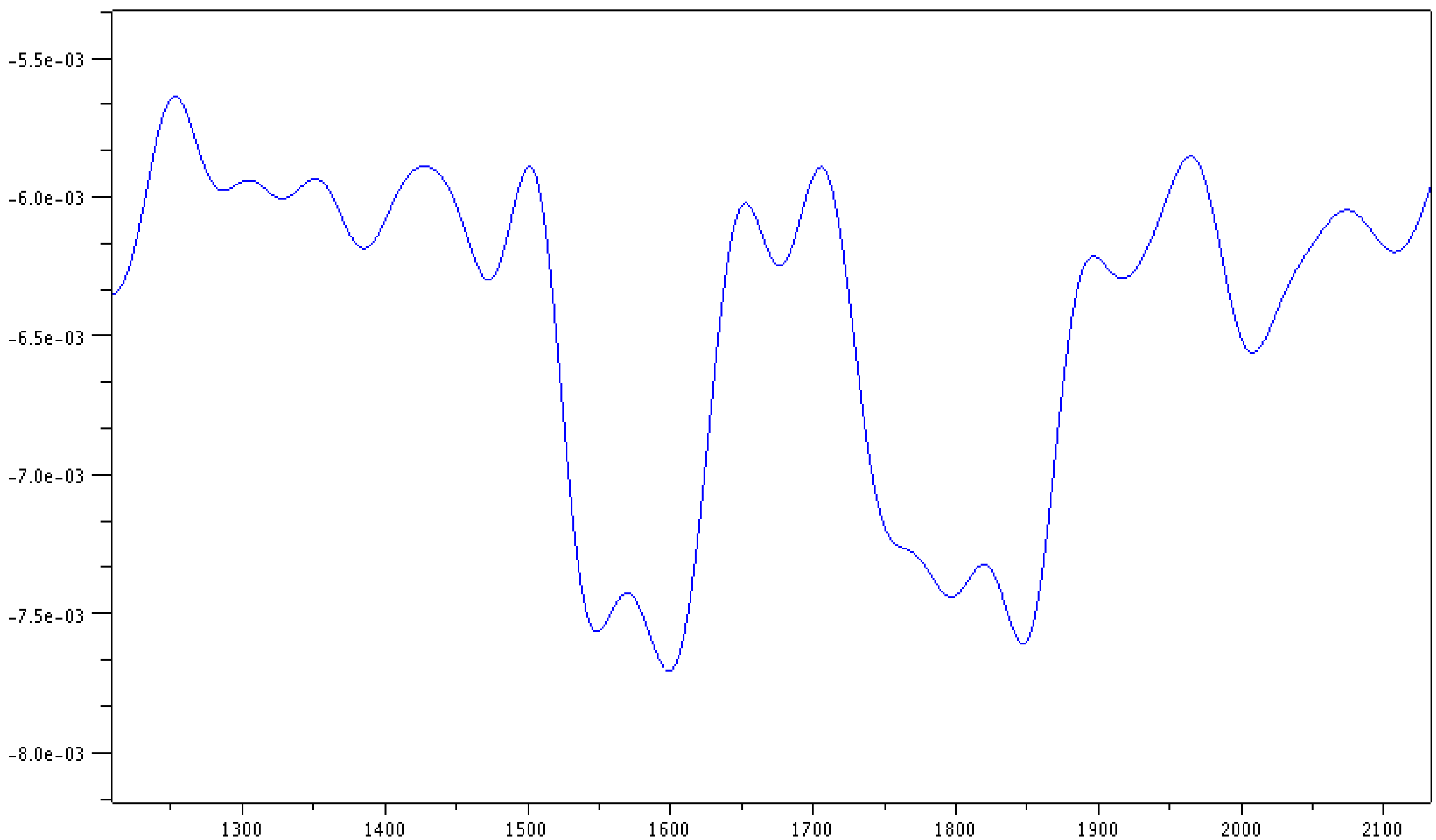


Results

- Ground noise + filtered signal comparison

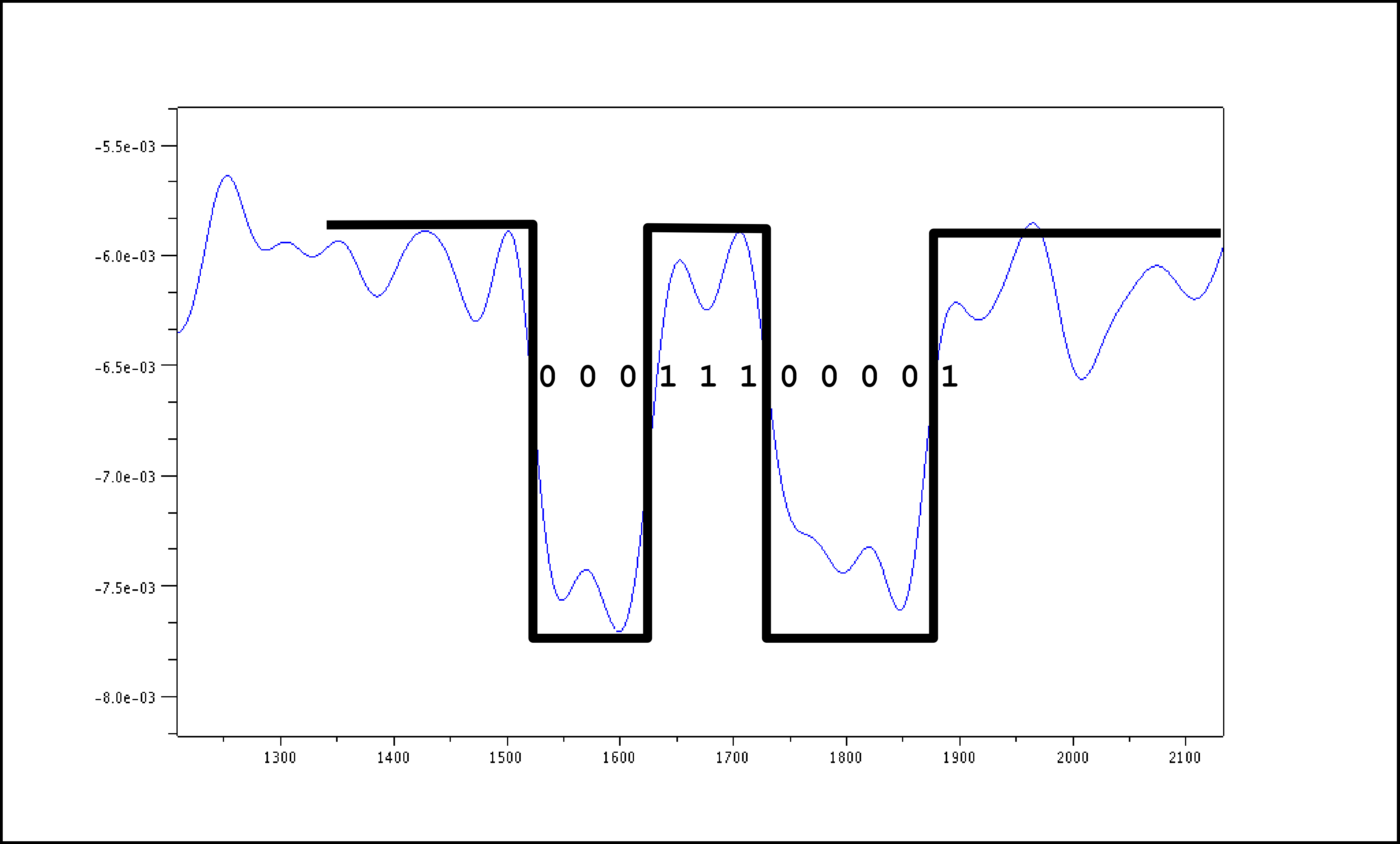


Results


-5.5e-03
-6.0e-03
-6.5e-03
-7.0e-03
-7.5e-03
-8.0e-03
1300
1400
1500
1600
1700
1800
1900
2000
2100

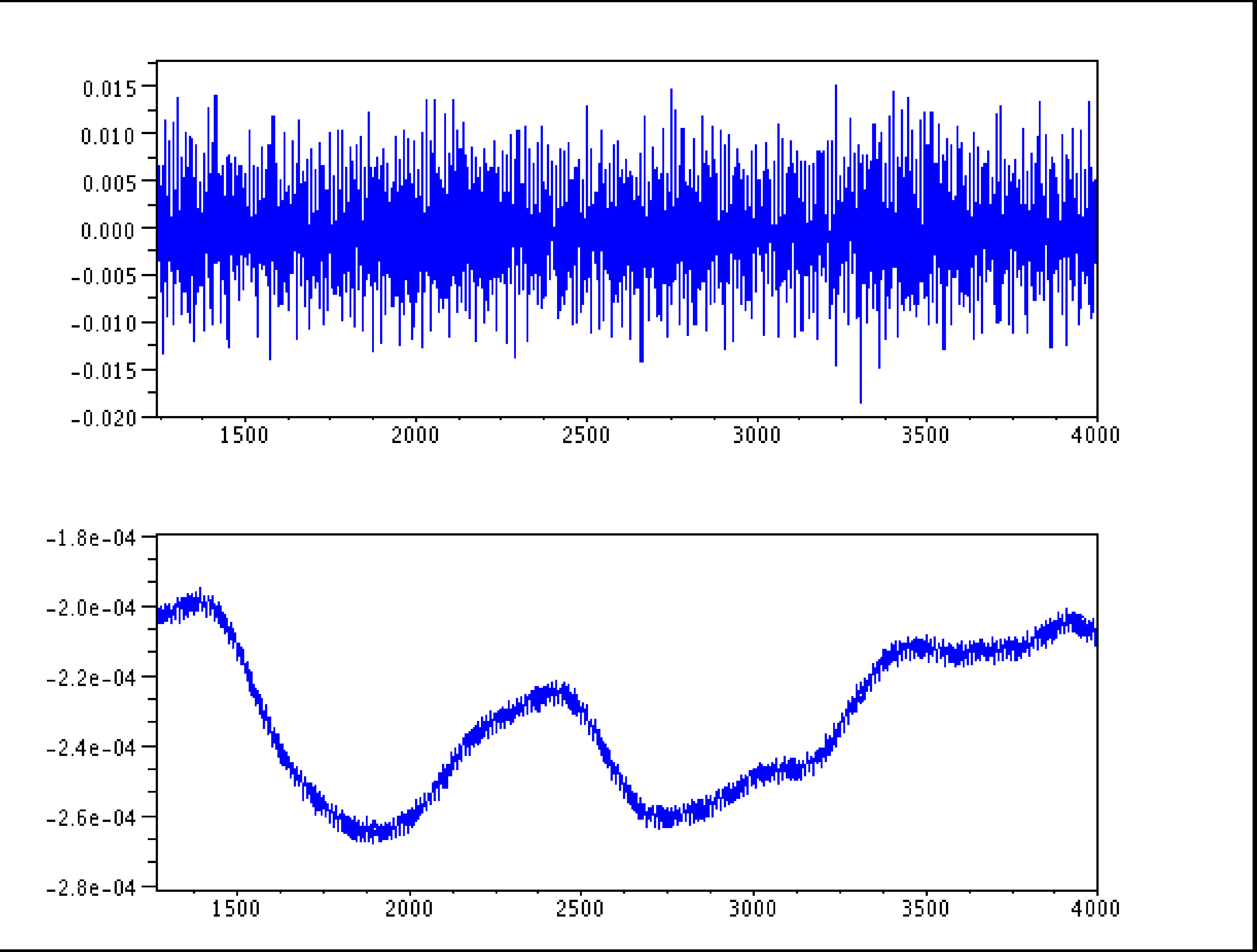
Results

- | 0 | 00111000 | 0 | 1 | = letter 'a'

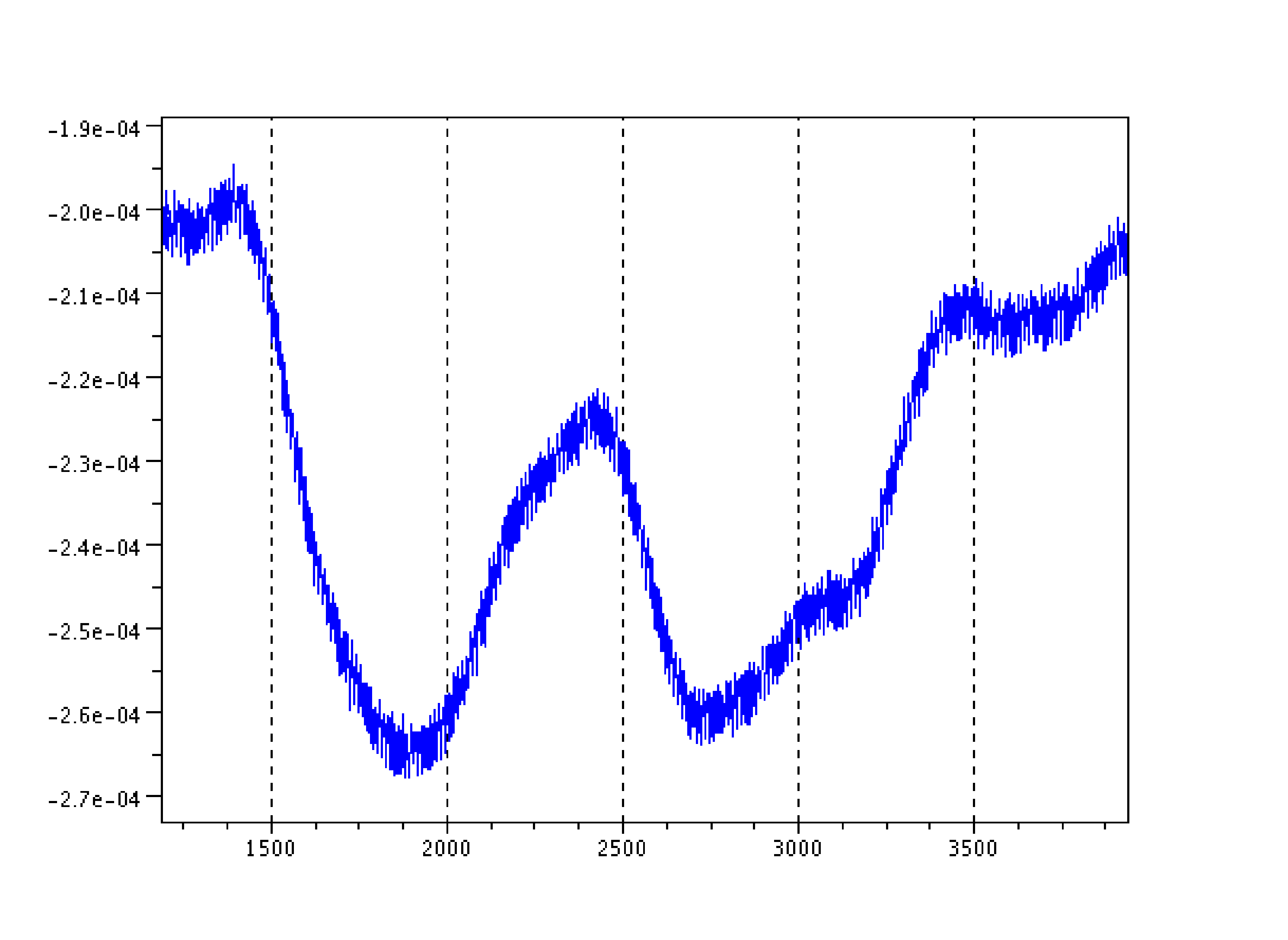


Results

- Ground noise + filtered signal comparison

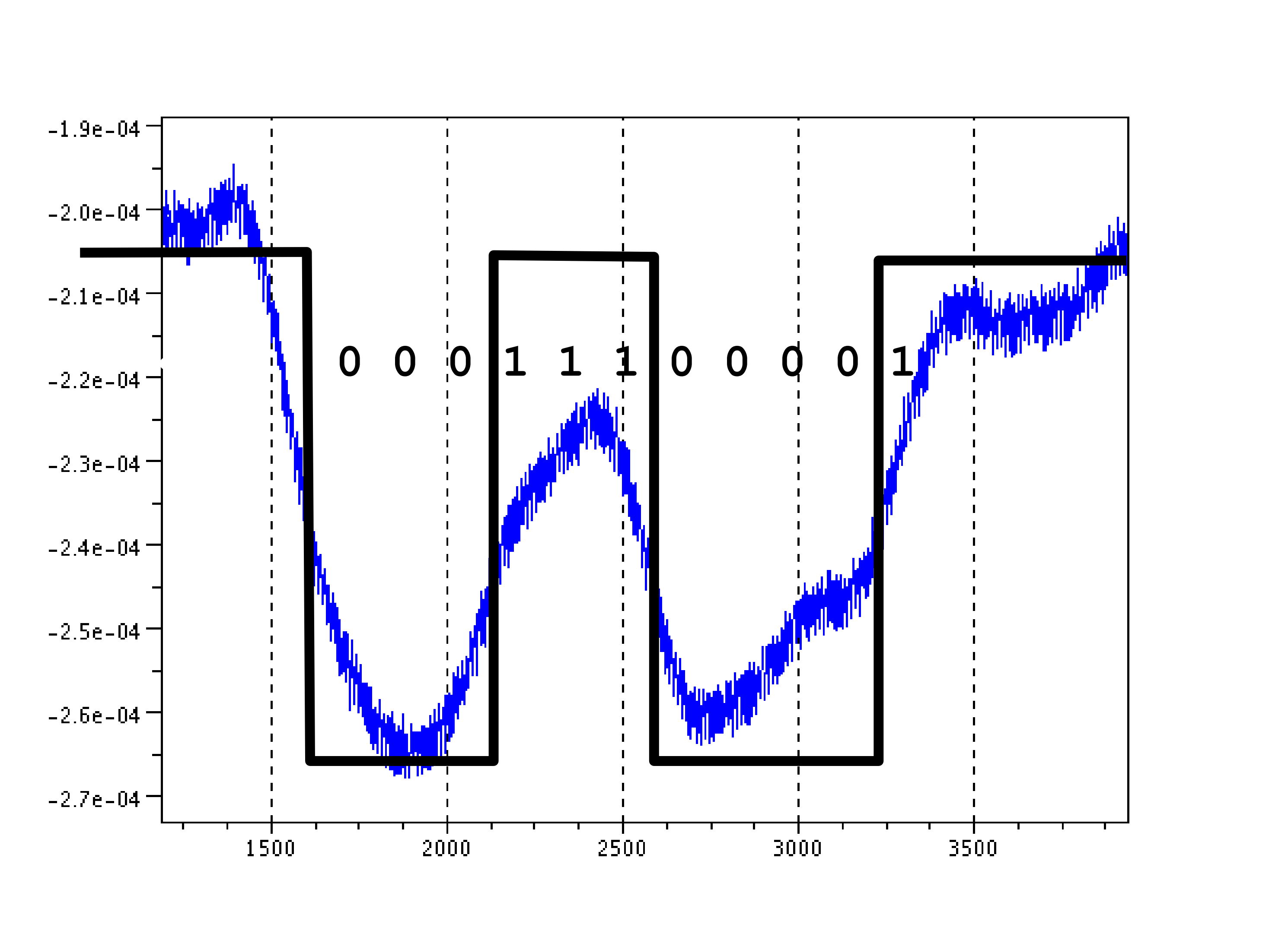


Results

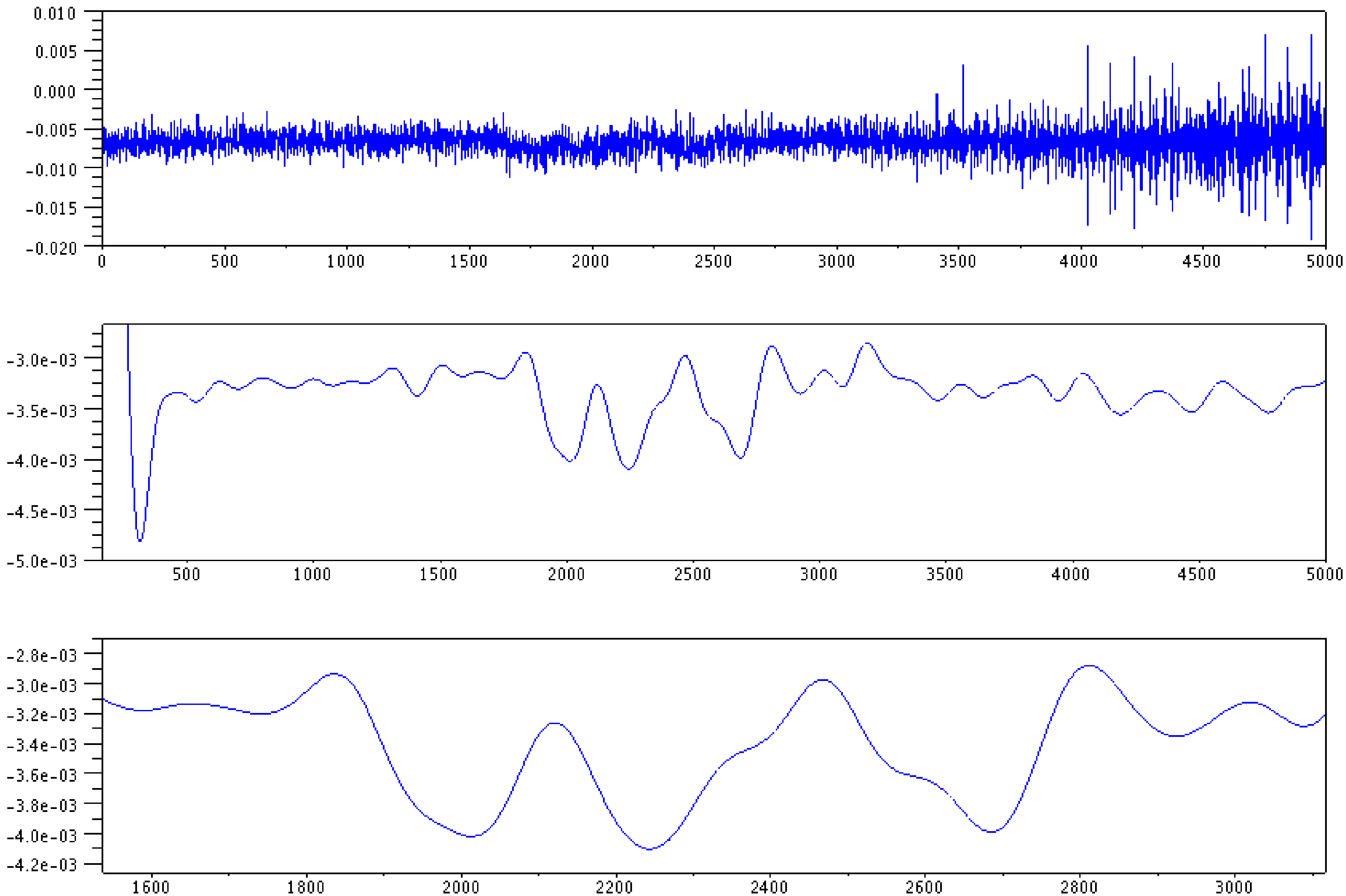

-1.9e-04
-2.0e-04
-2.1e-04
-2.2e-04
-2.3e-04
-2.4e-04
-2.5e-04
-2.6e-04
-2.7e-04
1500
2000
2500
3000
3500

Results

- | 0 | 00111000 | 0 | 1 | = letter 'a'

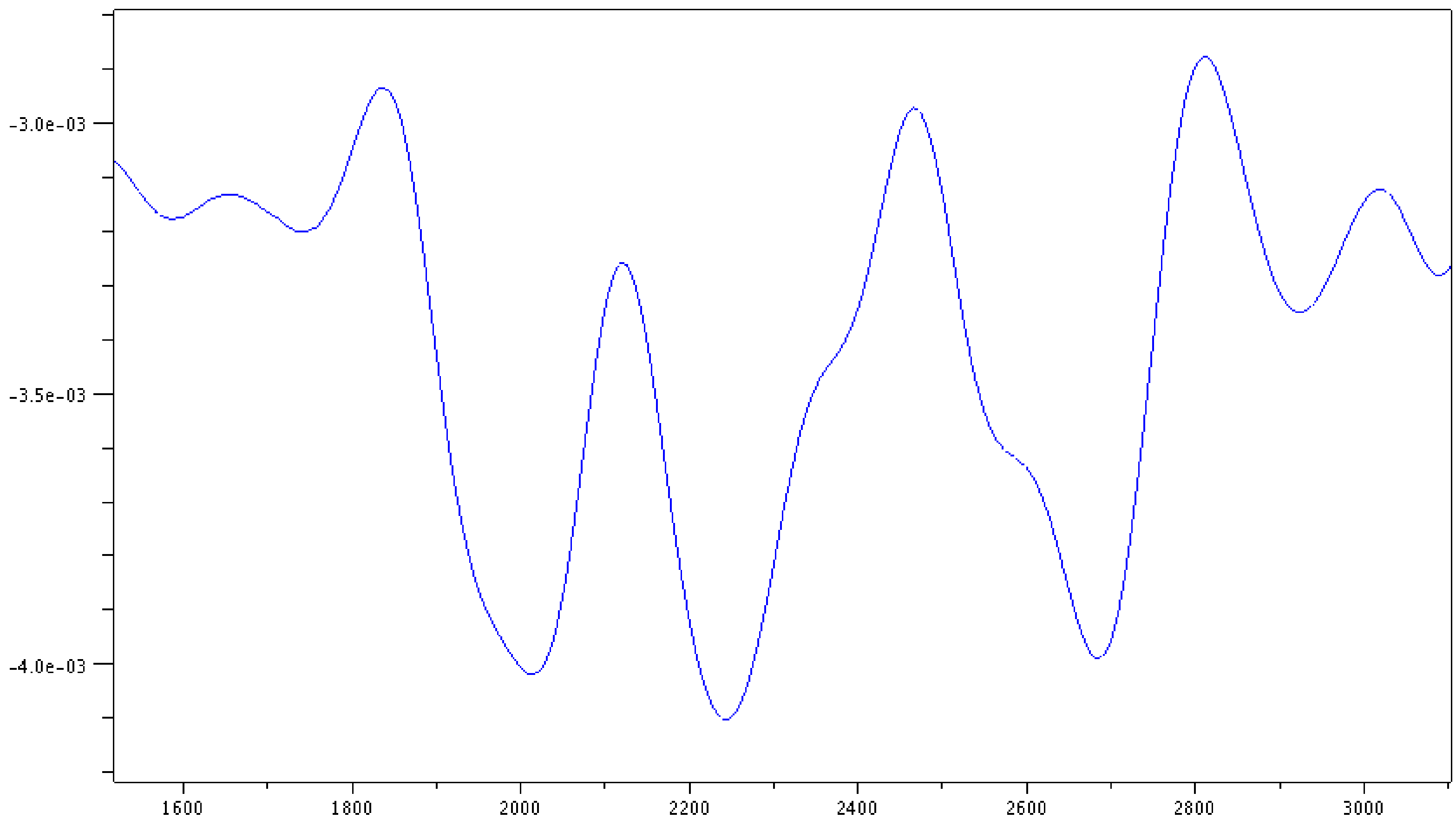


Results



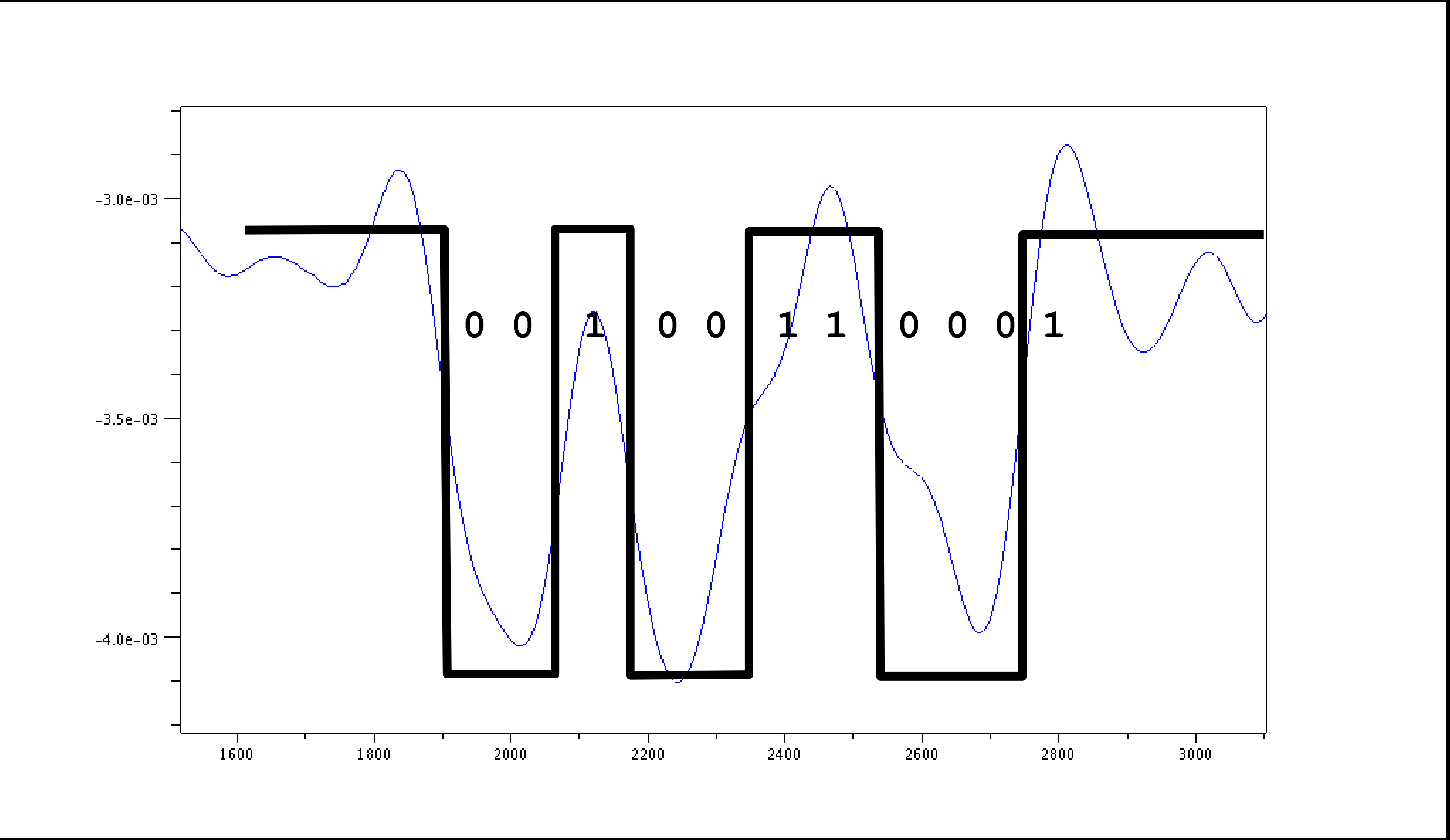
0.010
0.005
0.000
-0.005
-0.010
-0.015
-0.020
0
500
1000
1500
2000
2500
3000
3500
4000
4500
5000
-3.0e-03
-3.5e-03
-4.0e-03
-4.5e-03
-5.0e-03
500
1000
1500
2000
2500
3000
3500
4000
4500
5000
-2.8e-03
-3.0e-03
-3.2e-03
-3.4e-03
-3.6e-03
-3.8e-03
-4.0e-03
-4.2e-03
1600
1800
2000
2200
2400
2600
2800
3000

Results



Results

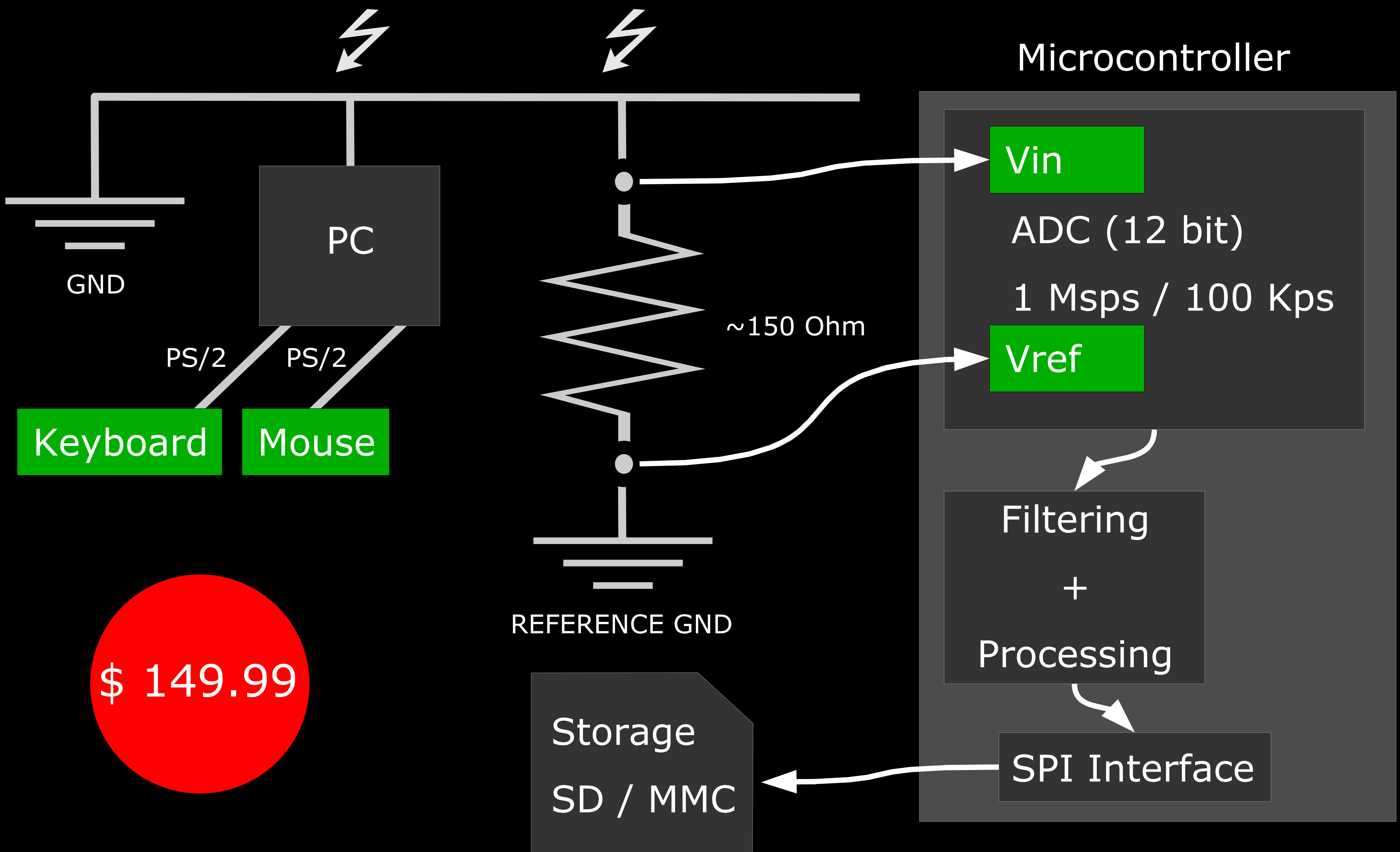
- | 0 | 01001100 | 0 | 1 | = letter 'b'



Estimating Attenuation

- Attenuation coefficients for wire copper are often estimated for much higher frequencies (>1Mhz)
- Considering a typical copper cable with a coefficient of 0.1 dB after 60m 50% of the signal survives (*theoretically!*)
- In our tests we didn't notice significant differences between the signal at 1.5m and 15m
- A typical signal has an output power of ~1 pW (10^-12 Watt)

Continuous Sniffing



Attack Scenario

- Depending on the sensitivity of the equipment, keystrokes can be probed from the nearby room or even farther...
- ...or power plugs can be tampered with their “sniffing” version (though this is not really interesting)
- Appealing alternate targets are ATM machines that use PS/2 or similar keypads (most ATM are standard PCs)
- We are confident that more expensive equipment can lead to more precise measurements...the data is (buried) there!

Notes

- This doesn't work against USB keyboards because of differential signaling
- There might be other factors responsible in minor part for the signal interference on the ground, like power fluctuations of the keyboard microcontroller...
- ...these are difficult to pinpoint but they aid the leakage
- *Vuagnoux & Pasini* attacks seems more practical (kudos to them!), unless you shield the room walls but forget about the power grid ;), but this attack might have more range
- the attack definetly deserves more investigation! (which we will continue in the next months)

Workarounds

http://www.fickr.com/photos/thefineed1/68647955 http://creativecommons.org/licenses/by-nc-sa/2.0

Public Research Relevant to Attack 2

- *Dmitri Asonov, Rakesh Agrawal* (2004). "Keyboard Acoustic Emanations”
- Li Zhuang, Feng Zhou, J.D. Tygar (2005). “Keyboard Acoustic Emanations Revisited”

- these are all brilliant people much more serious than us...kudos to them too!

Second Attack Theory

- As we cannot use the previous attack on laptops we need something different
- Previous research addresses keystrokes acoustic
- Laser microphones can be used for monitoring sounds at a great distance
- Why not pointing the laser microphone directly at the laptop and sample vibrations?
- Profit!

Laser Microphone Assembly

LASER RADIATION

- 1 x Laser (more expensive lasers means more range)
- 1 x Photoresistor or Photodiode
- 1 x Resistor
- 1 x AA Battery
- 1 x Universal Power Adapter
- 1 x Jack Cable
- 1 x Laptop with sound card
- 2 x Tripod
- 1 x Focusing lens (for long distances)
- *Optional*: amplifier, optical bandpass filter, duct tape ...

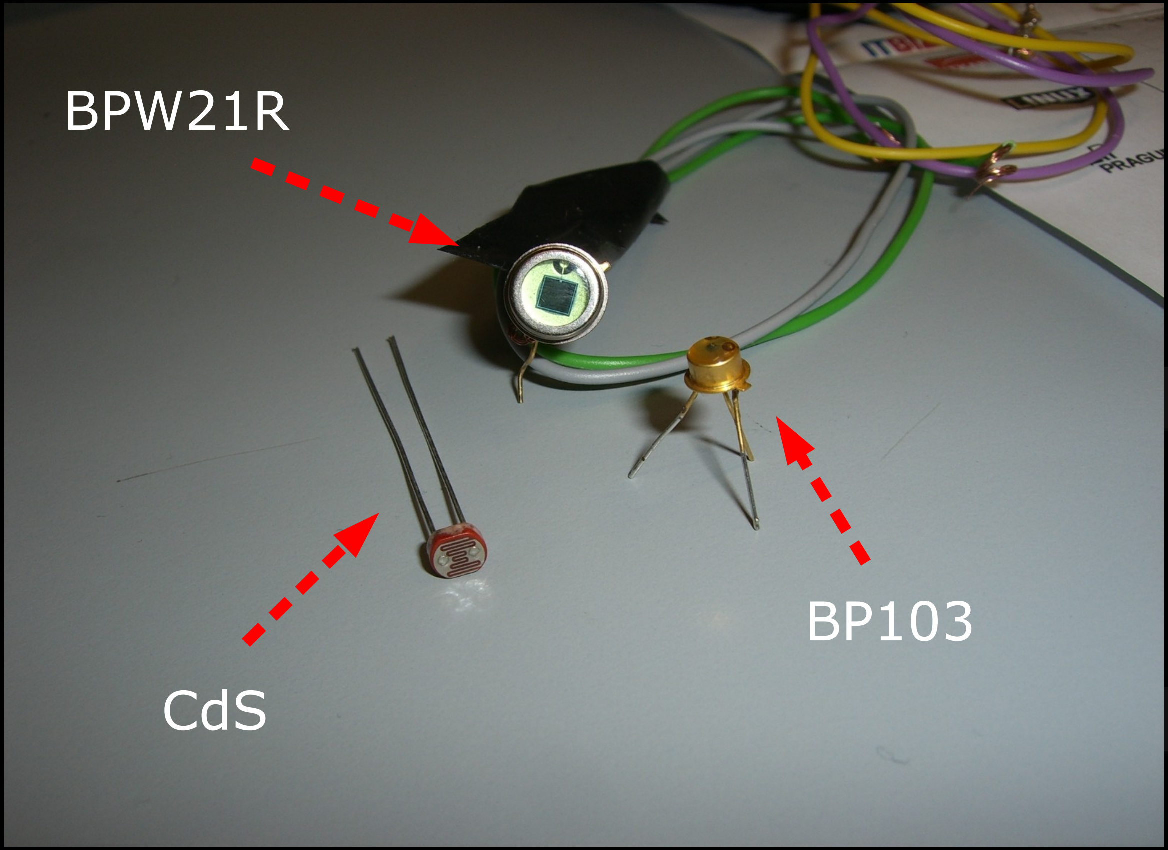
$ 79.99

TX (The Laser)

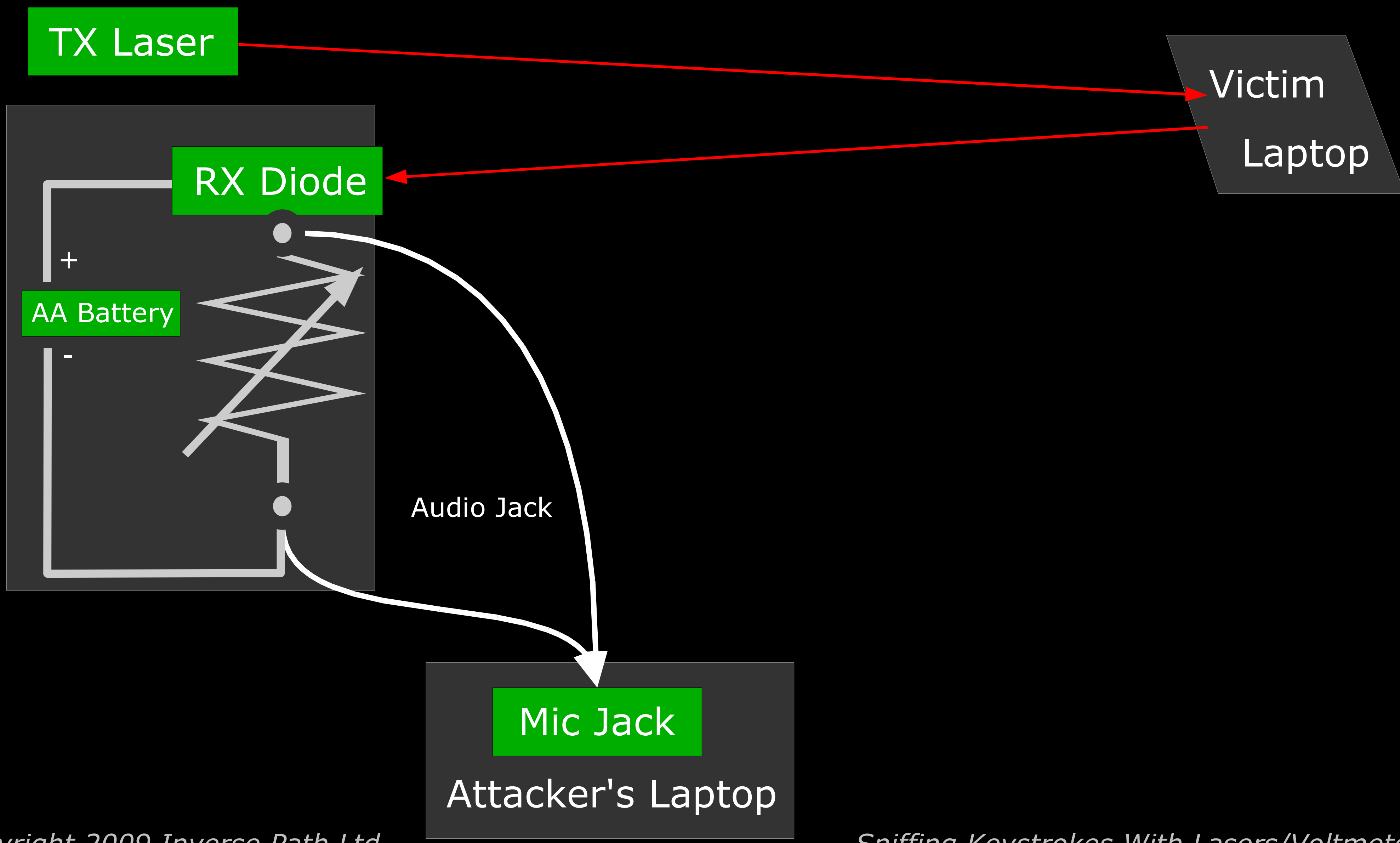
- Class IIIR, 670 nm, <5 mW power, <2 mrad divergence (good for short range, 15-30 meters), cheap and poor laser

RX (Photo Detector)

- BP103 or...
- Cadmium Sulfide (CdS) Photoresitor or...
- BPW21R Silicon PN Photodiode



Diagram


TX Laser
Victim
Laptop
RX Diode
+
AA Battery
-
Audio Jack
Mic Jack
Attacker's Laptop

The Device

The Device

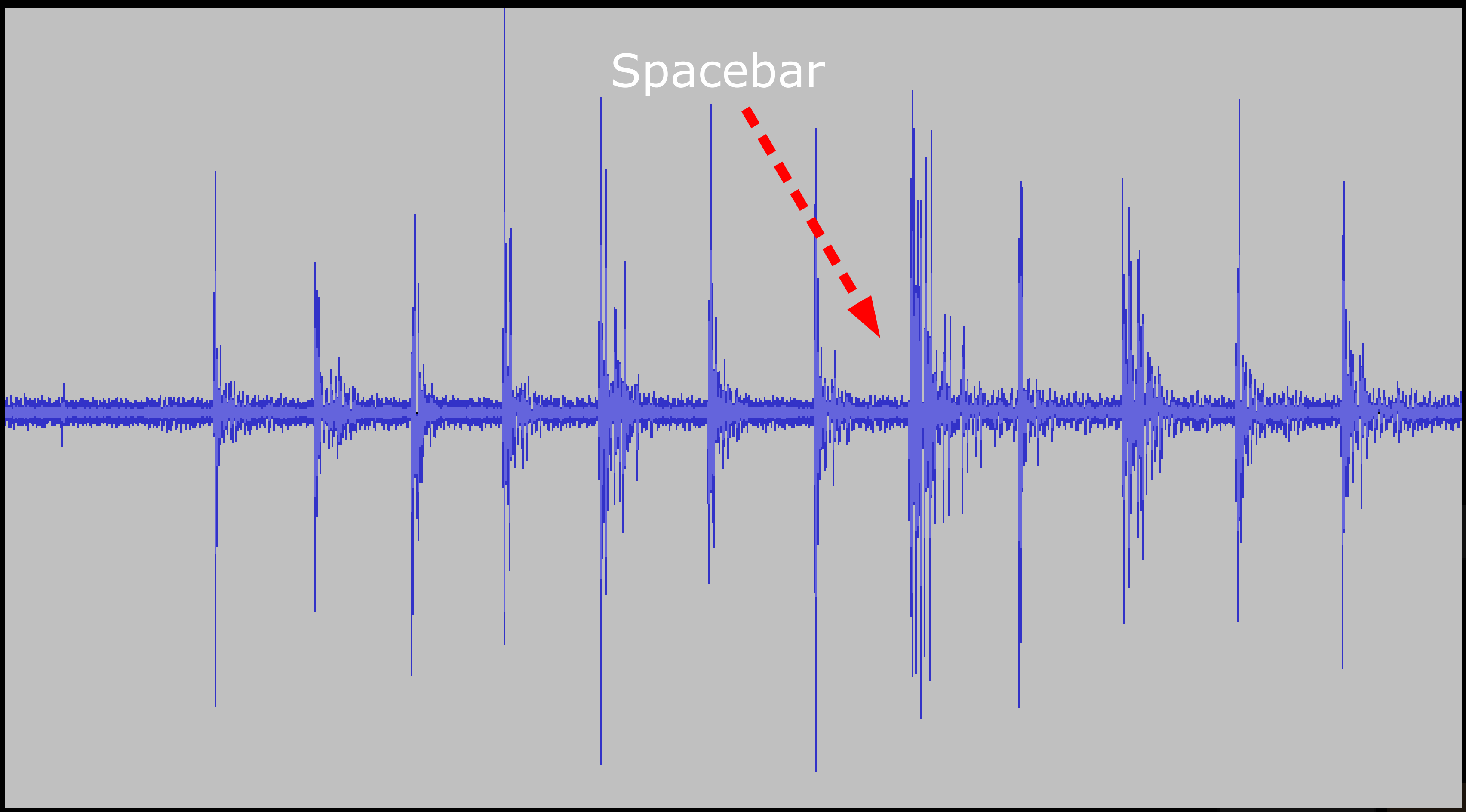
Audio Detection

- In order to test the device we first tried with audio
- A variable resistor helps a lot
- Good results below 30 meters without any hard core tuning
- Longer distances requires precise calibration and filtering

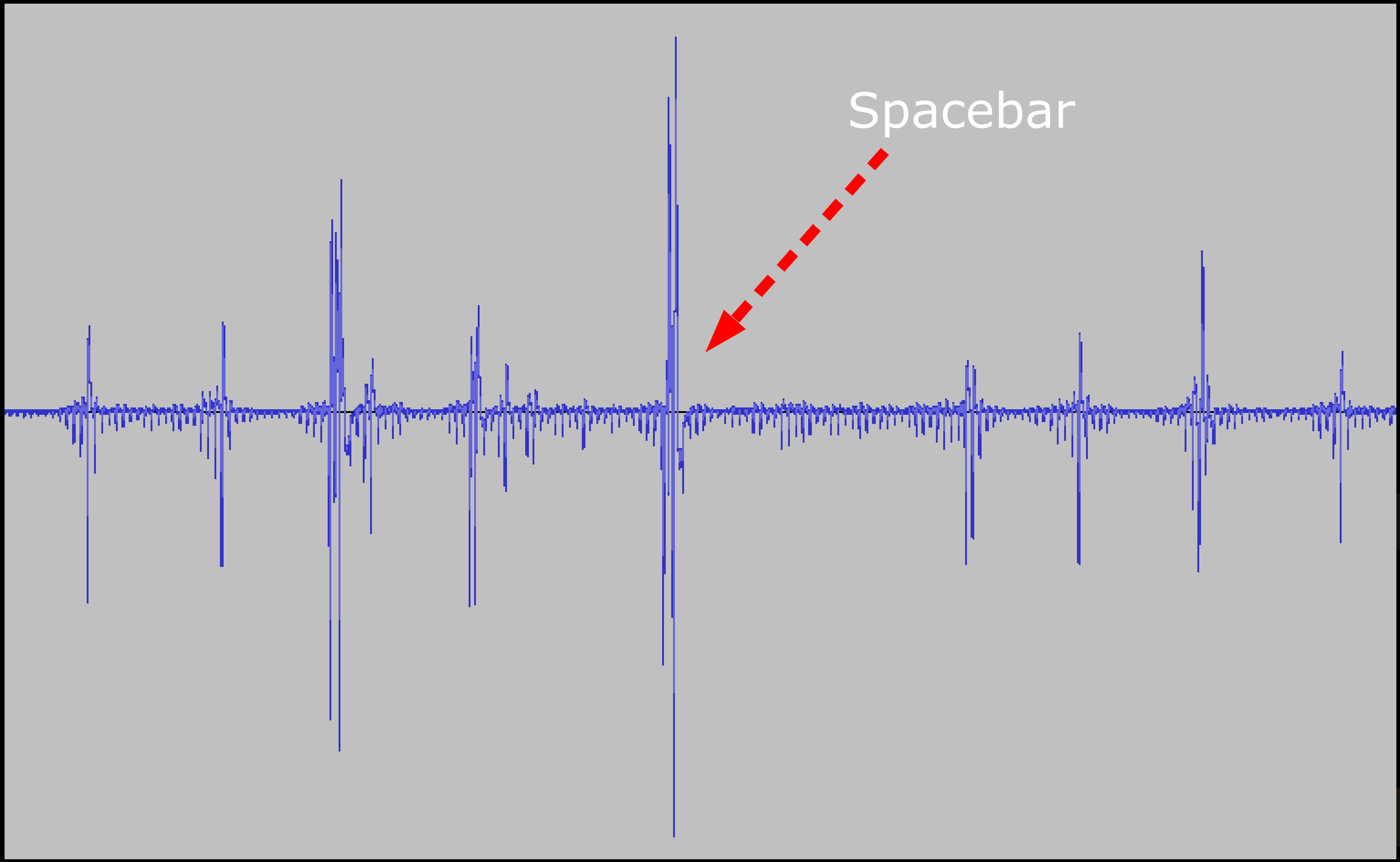
Keystrokes Detection

- We aim the beam directly at the laptop case, generally the LCD display lid
- Aiming at the top of the lid catches more resonant vibrations (to be substracted later via signal analysis)
- Aiming closer to the hinges produces better results

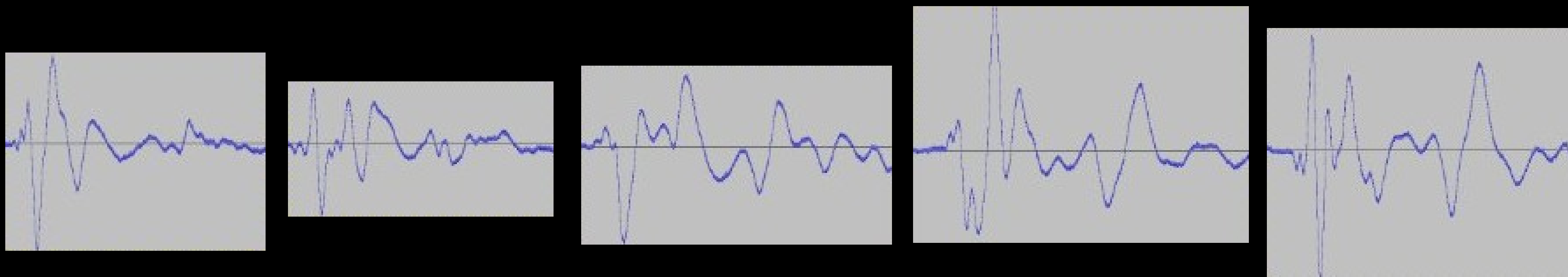
Sample - Keystrokes

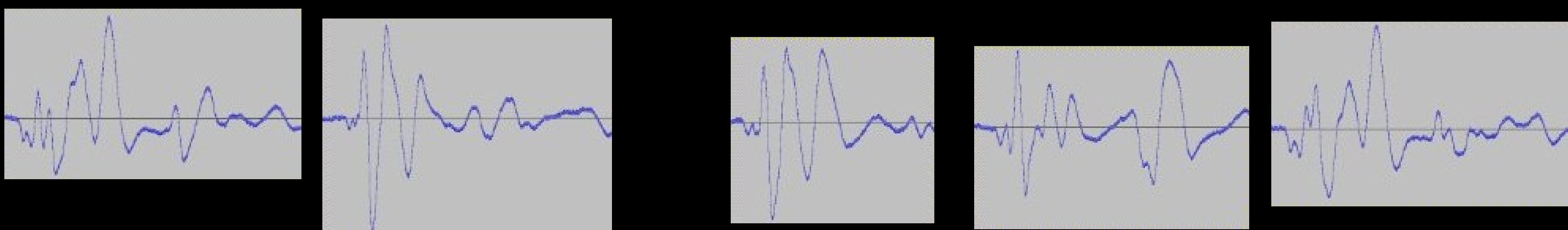


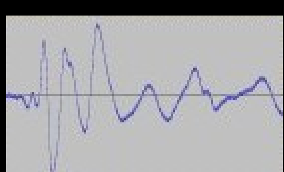
Sample - Keystrokes



Sample - Keystrokes



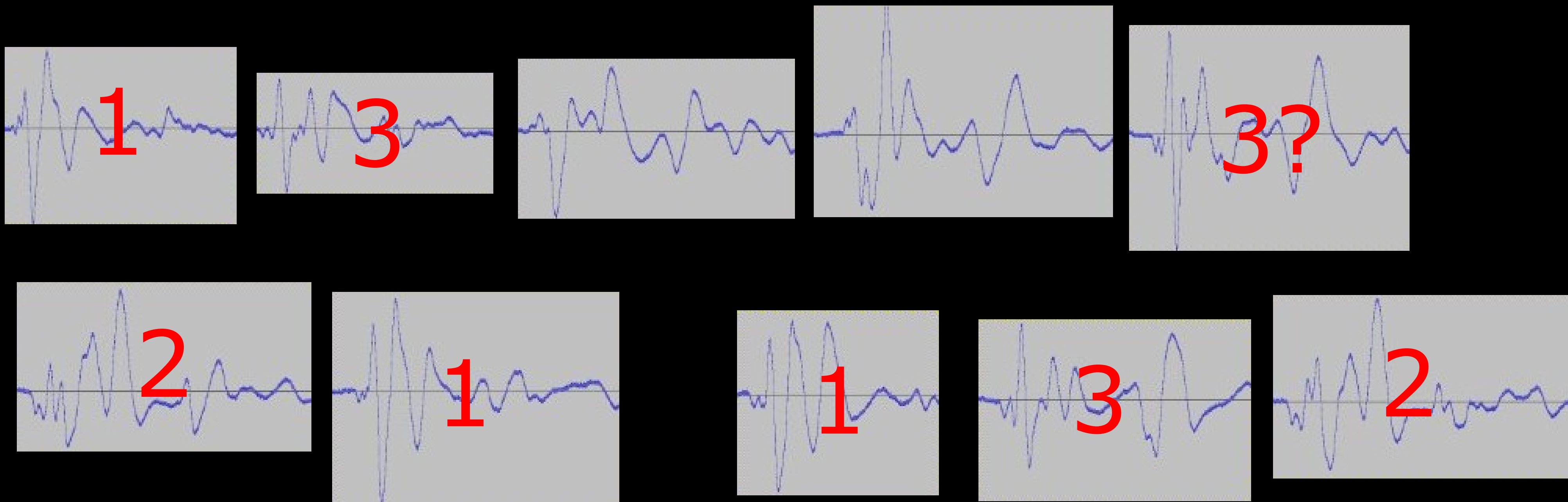




It's just like

Wheel of Fortune!

Sample - Keystrokes

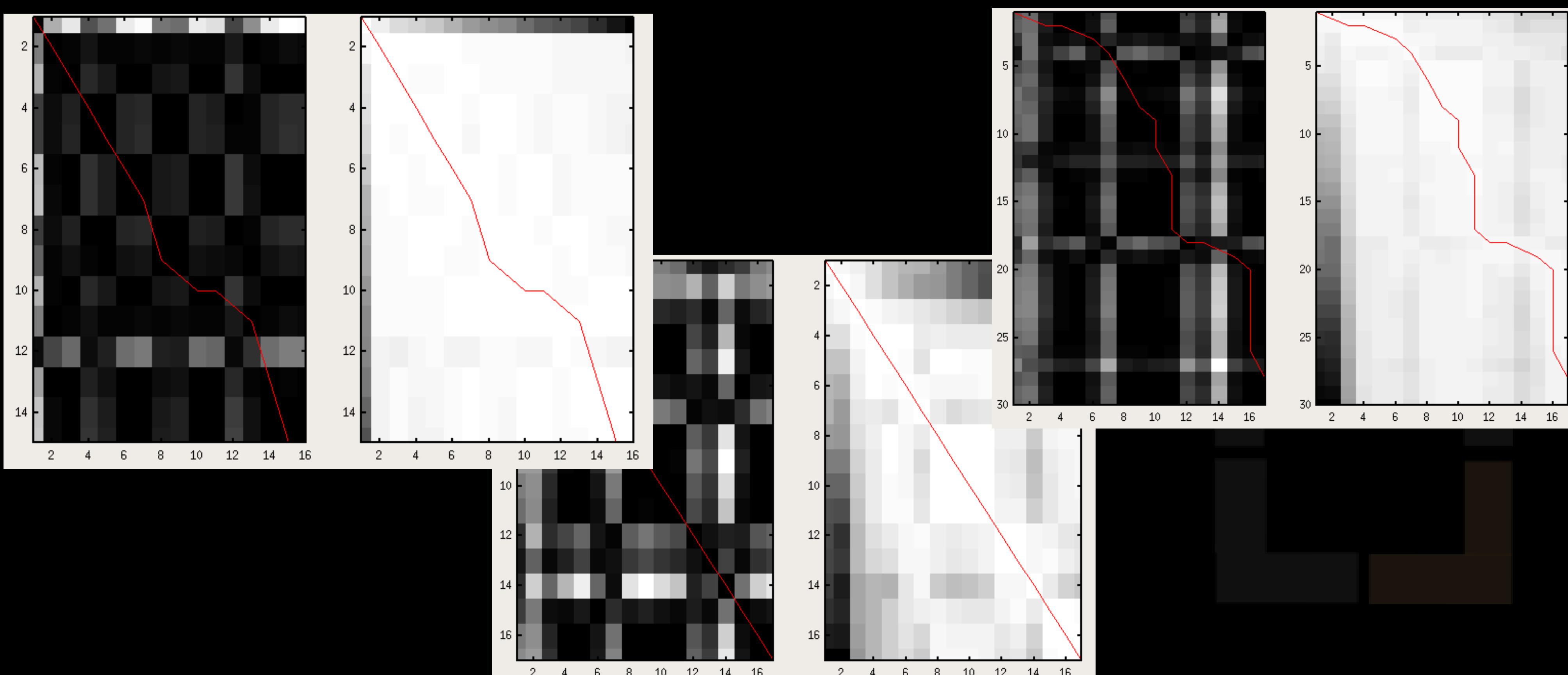


It's just like

Wheel of Fortune!

Scoring Technique

- Dynamic Time Warping (DTW) is a good technique for measuring the similarity of signals with different time/speed
- Generally applied to Audio (speech recognition) and Video

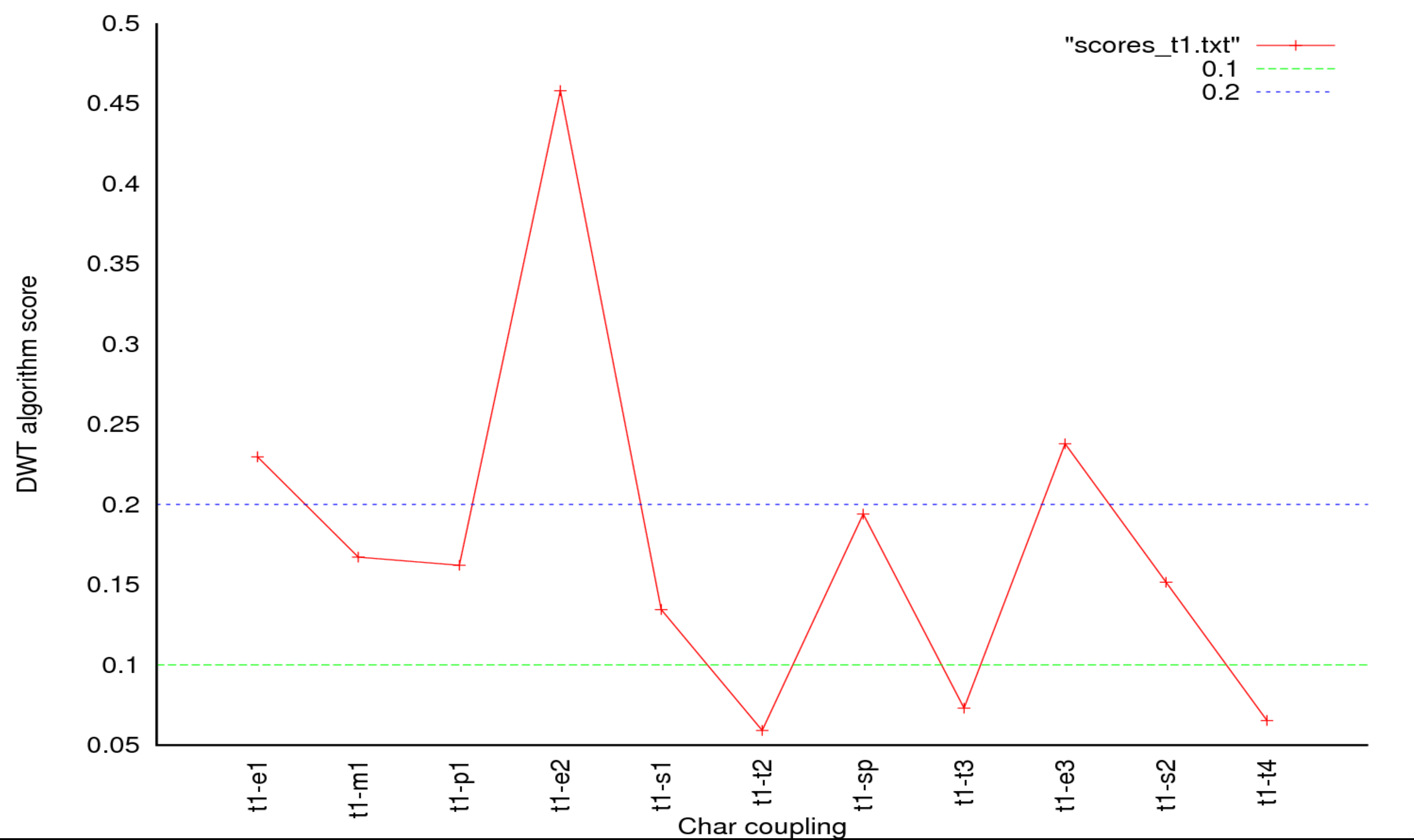


Scoring Results

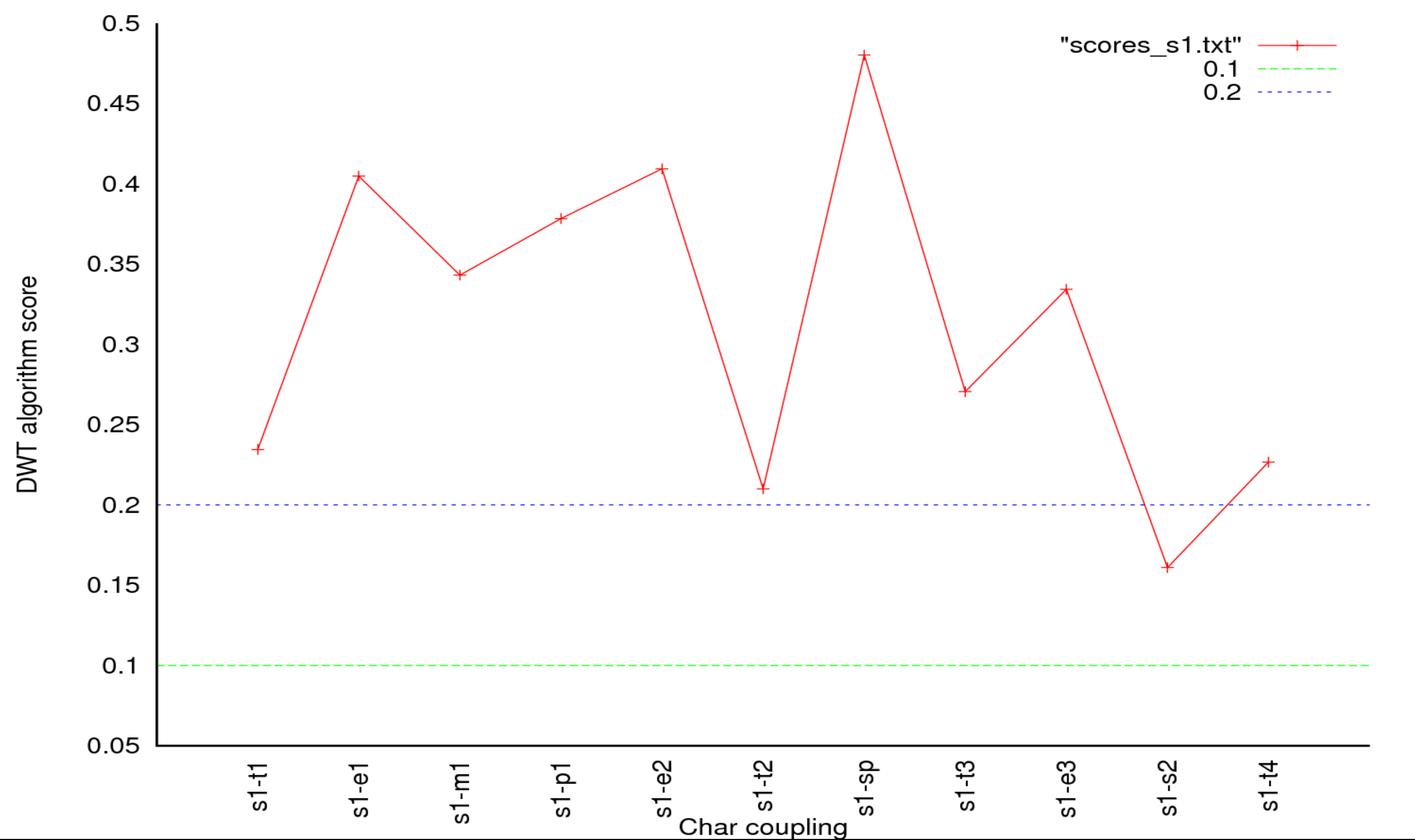
```
chars 1 <> 7  = 0.066    chars 7 <> 8  = 0.029    chars 8 <> 7  = 0.029
chars 1 <> 8  = 0.072    chars 7 <> 1  = 0.066    chars 8 <> 1  = 0.072
chars 1 <> 3  = 0.167    chars 7 <> 3  = 0.161    chars 8 <> 3  = 0.146
chars 1 <> 10 = 0.188    chars 7 <> 10 = 0.191    chars 8 <> 6  = 0.226
chars 1 <> 6  = 0.209    chars 7 <> 6  = 0.270    chars 8 <> 10 = 0.244

chars 6 <> 10 = 0.160     chars 10 <> 6 = 0.160     chars 11 <> 1  = 0.065
chars 6 <> 1  = 0.209     chars 10 <> 7 = 0.191     chars 11 <> 8  = 0.029
chars 6 <> 8  = 0.226     chars 10 <> 1 = 0.188     chars 11 <> 7  = 0.072
chars 6 <> 7  = 0.270     chars 10 <> 8 = 0.244     chars 11 <> 3  = 0.146
chars 6 <> 3  = 0.343     chars 10 <> 3 = 0.250     chars 11 <> 6  = 0.226
```

- chars 1, 7, 8 and 11 are definetly identical like 6 and 10
- char 3 and 4 looks different than anything else
- final result with complete scoring: 1?XY321 1321

Scoring Results



Scoring Results



Pattern Matching

```
./WoF '1_XY321 1321' /usr/share/dict/american-english

hogwash hash (???)
salmons sons (???)
secrets sets (maybe)
sermons sons (???)
sockets sets (meh)
soviets sets (cold war!)
statues sues (well everything sues in America)
straits sits (???)
subways says (???)
tempest test (OMG)
tidiest test (meh)
tiniest test (meh)
trident tent (yeah right...)
```

Pattern Matching

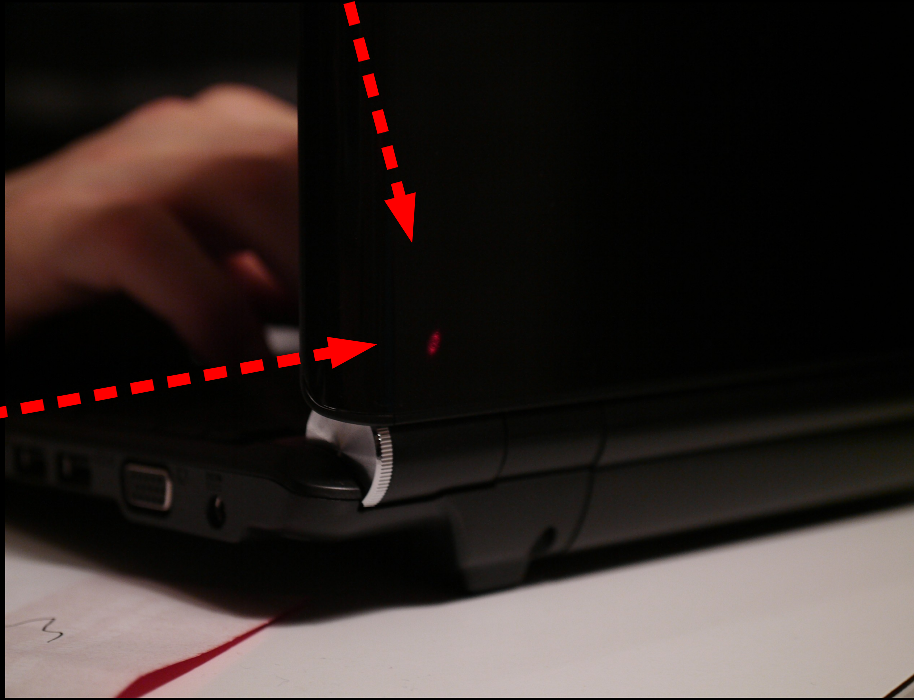
- If we spot a '*the*' (which is common in the English language) we narrow down the odds to 5 cases
- Consider that this sample result involves just 2 or 3 words without any previous data (although with 3 common letters spread around)
- Sampling more words dramatically increases matching
- Non-word passwords can be narrowed down considerably if a sample of English data is available from the same session

Attack Scenario
Laptops

LASER RADIATION

- Asus EEE PC

Reflective Plastic Case



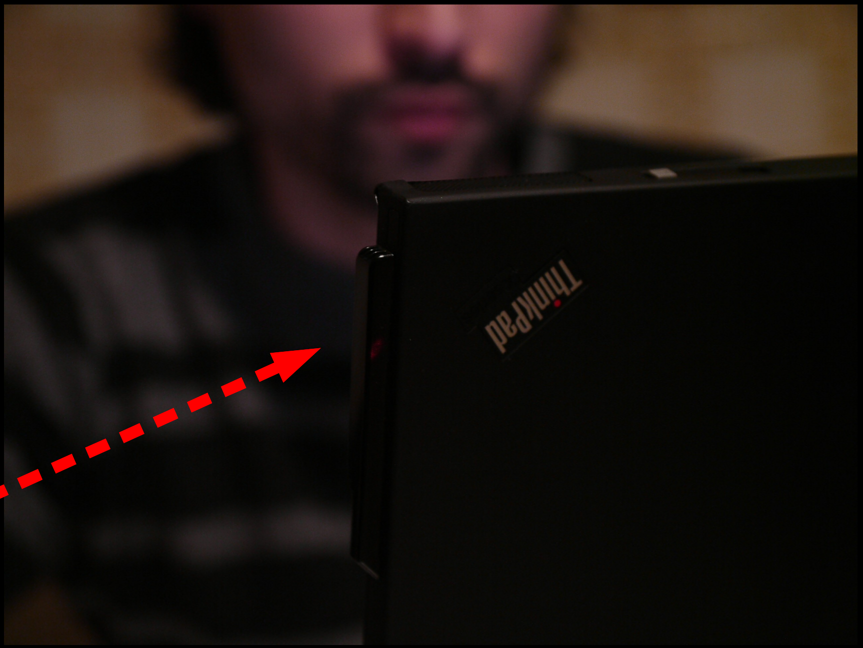
PWNED!

Attack Scenario
Laptops

LASER RADIATION

- IBM/Lenovo Thinkpad

Logo



Wireless Antenna

Attack Scenario
Laptops

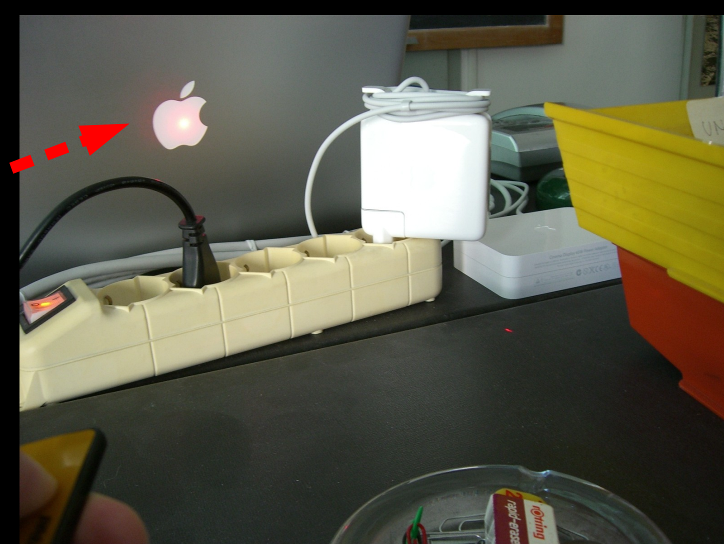
LASER RADIATION

- Apple (we always thought that glossy == evil)

Glass ? Oh yeah!

Case, not good

The Logo is very good too...



Attack Scenario
The Environment

- Obviously a line-of-sight is needed, either in front or above the target
- TX / RX can be at completely different locations
- The more money you throw at the equipment the longer the range
- Other kinds of laser microphone using interferometry and double transmitters can be used
- Attack is possible even with a (possibly double) glass window in the way, reflection loss is 4% at every pass
- Infrared laser can be used for stealthyness

Notes

- Changing radically typing position (unusual) and mistyping words (very common) decrease accuracy
- Mistyping can be compensated, neural networks and/or custom dictionaries with key region mappings instead of words can be used for the first pass
- We believe that previous researches against acoustic emanations can be applied too
- We know it's hard to get a line of sight for the laser microphone, but it could be really worth it :) (social engineer your victim!)

The End

Thanks for listening! - Questions?

(shameless plug)

http://www.inversepath.com