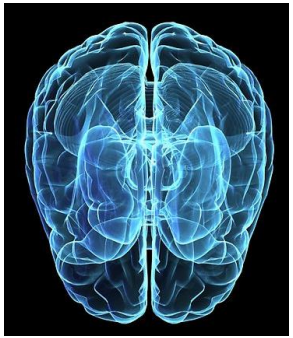
Brain Waves Surfing: (In)security in EEG (Electroencephalography) Technologies



Alejandro Hernández (@nitr0usmx)
Senior Consultant

IOActive
Hardware | Software | Wetware
SECURITY SERVICES

About me

- Senior Security Consultant at IOActive
- Fuzzing & programming enthusiast
- Computer systems engineer (not neuroscientist)
- Passionate about security (~12 years now)
- From Chiapas, Mexico

IOActive

Agenda

- Why this talk?
- Neuroscience 101
- EEG / Brain Waves
- (In)security aspects
  - Design
  - Encryption
  - Authentication
  - Resilience
  - The *"Tower of Babel"* of EEG file formats
  - Misc
- Regulatory compliance / best practices for digital EEG
- Conclusion / further research

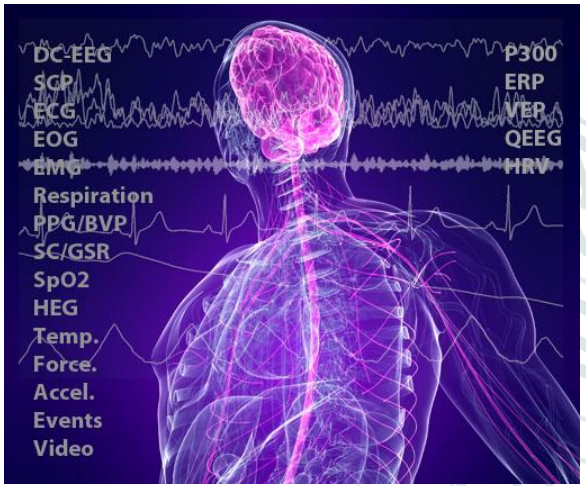
IOActive™

This is NOT an invasive-BCI talk to become Johnny Mnemonic

IOActive™

Why this talk?

- Nowadays we mostly care about
  - Computer/Network/Information security
  - Mobile security
  - ICS/SCADA security
  - Car security
  - IoT security
  - **What about our biosignals?**
    - Any signal generated by our bodies
    - EKG, EMG, MMG, MEG, EOG
    - **EEG (brain signals)**
      - **Acquisition, storage, processing and transmission**



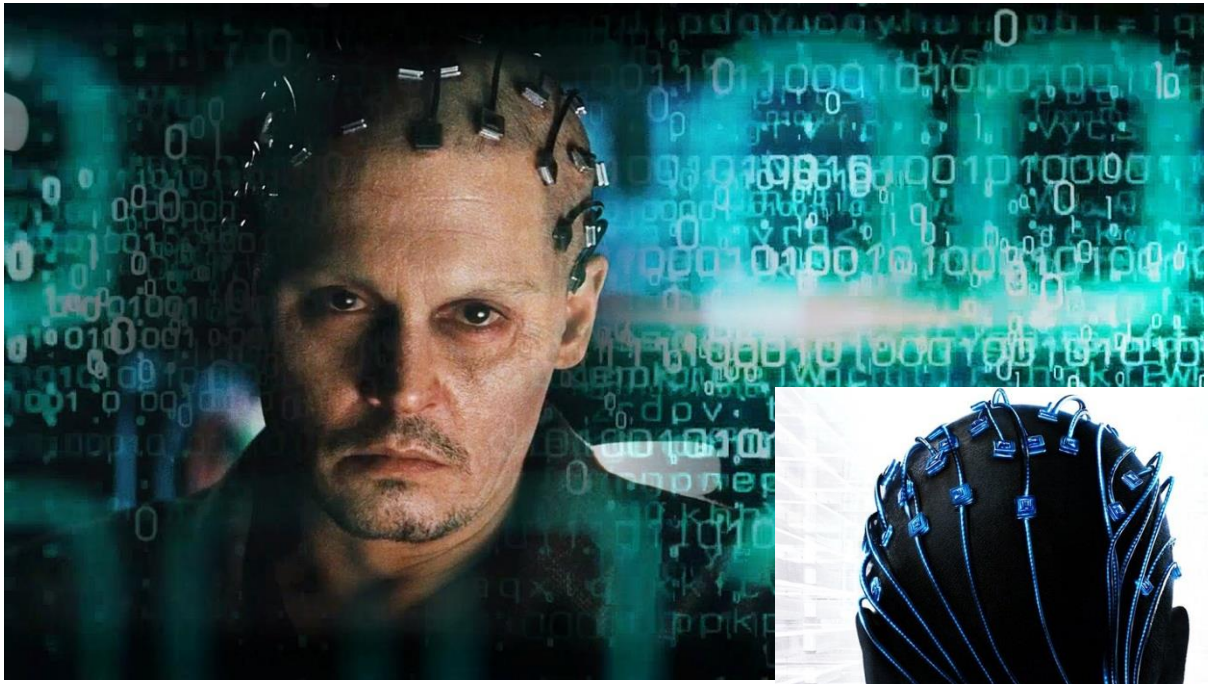
IOActive™

Why this talk?

- EEG tech is being adopted more and more
- Brain stuff is cool, specially in
  - **Cyberpunk** movies
  - **Sci-Fi** literature

IOActive™

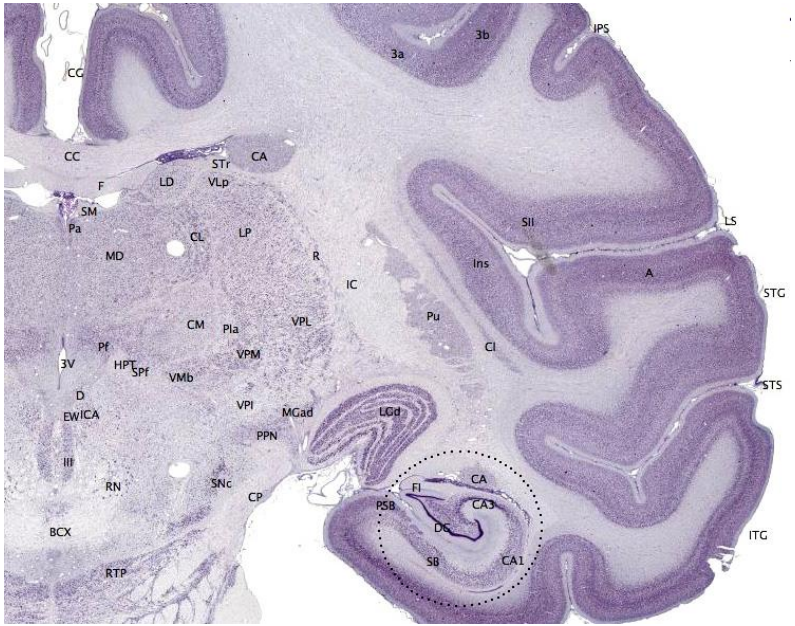
IOActive™

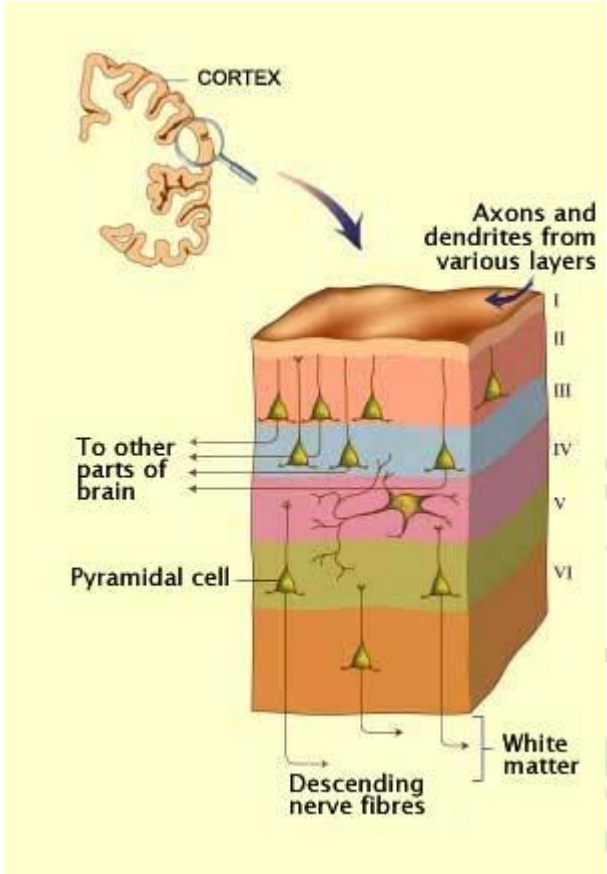


IOActive™

Neuroscience 101

- Cerebral cortex
  - The outer layer

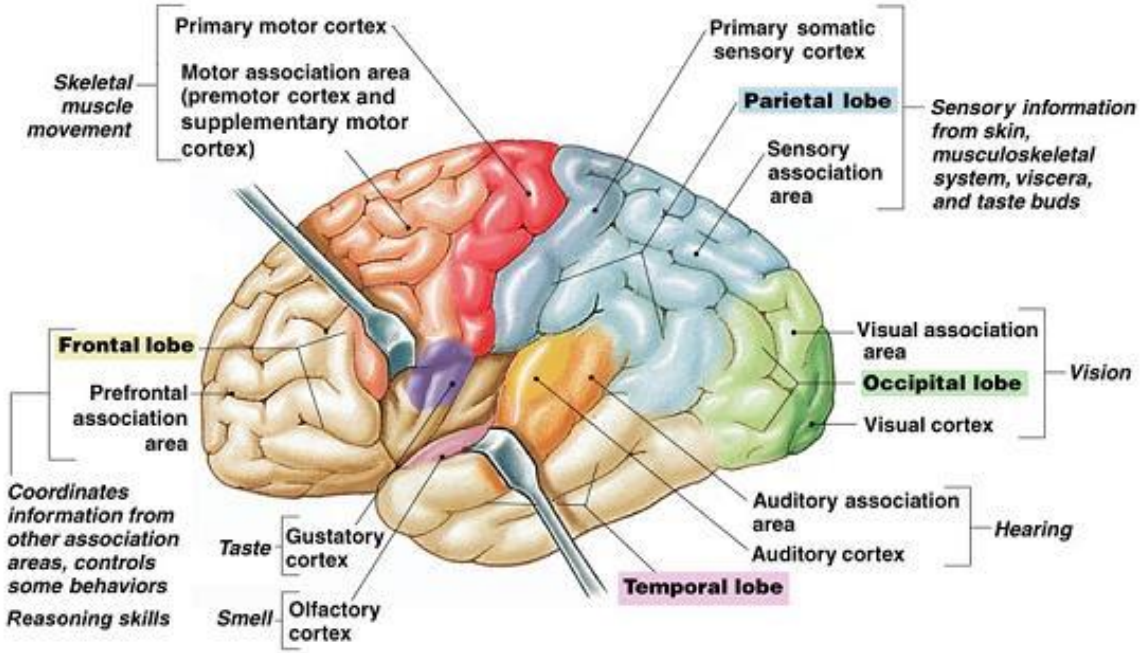




IOActive™

Neuroscience 101

- Lobes

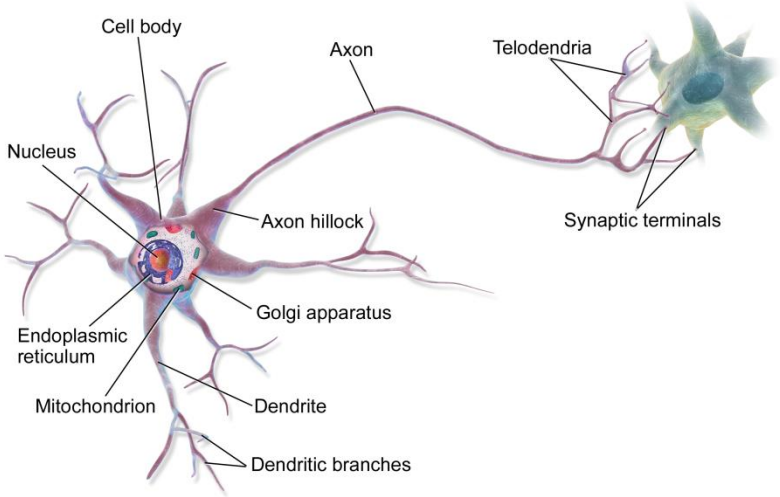


Copyright © 2007 Pearson Education, Inc., publishing as Benjamin Cummings.

Fig. 9-15

Neuroscience 101

- Neurons
  - Electrically excitable cells
  - Processes and transmits information through chemical and **electrical signals**



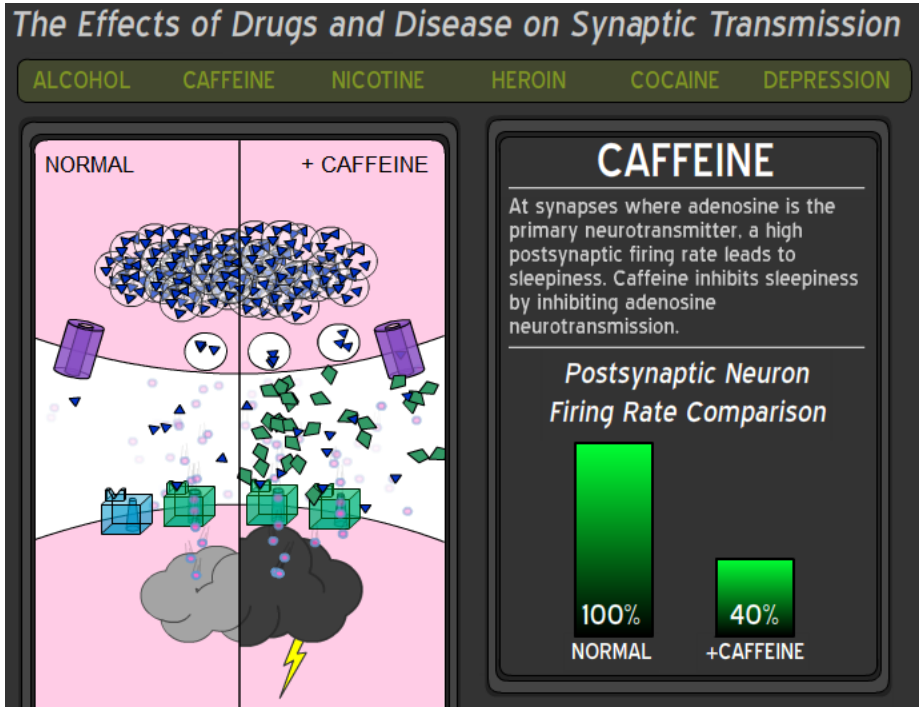
IOActive™

Neuroscience 101

- Synapse
  - The pass of chemical or electrical signal to another cell

IOActive™

Neuroscience 101

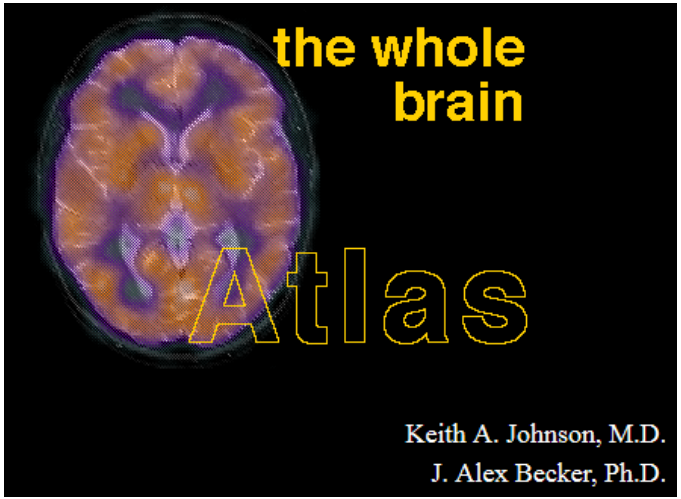


The Effects of Drugs and Disease on Synaptic Transmission
http://outreach.mcb.harvard.edu/animations/synapse.swf

IOActive™

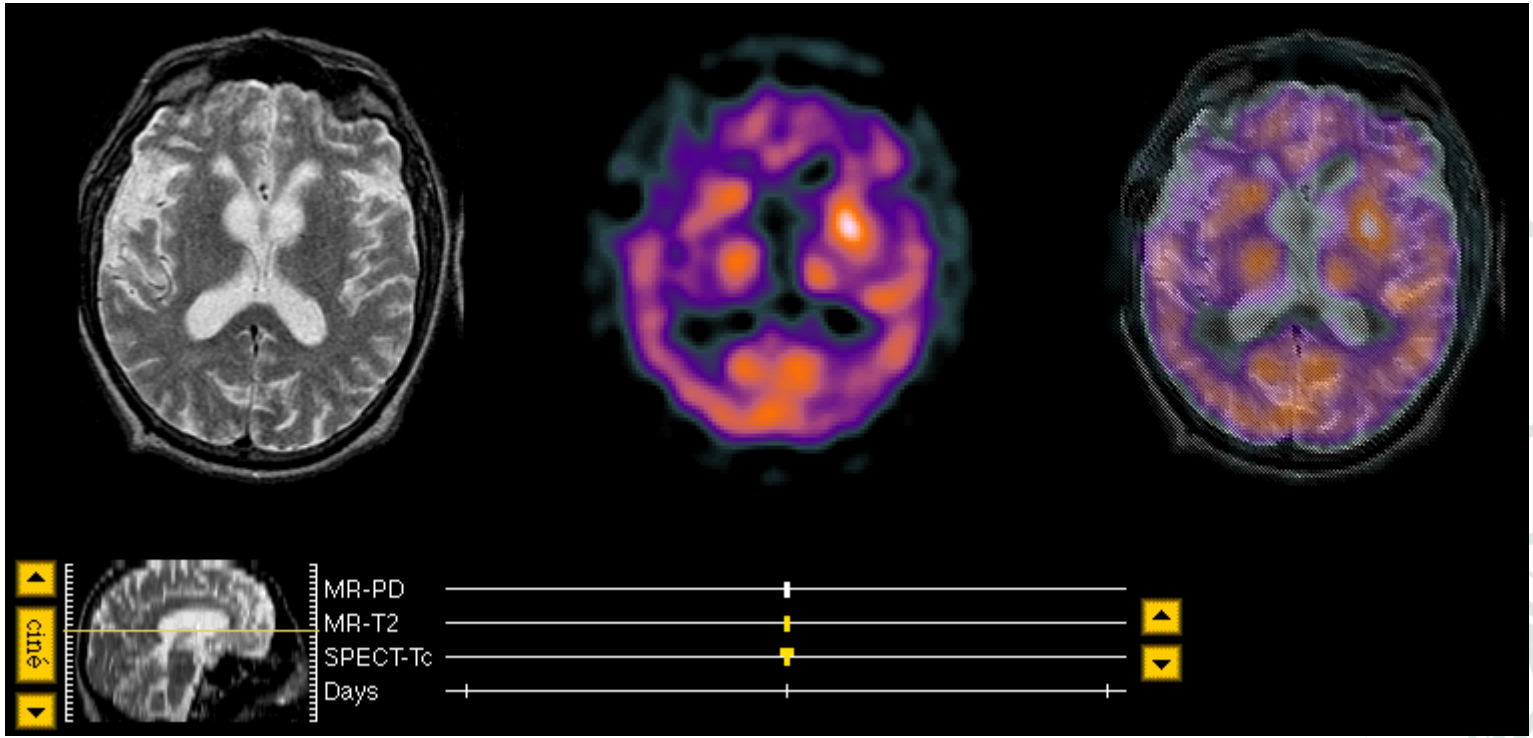
Neuroscience 101

- Want more?
  - Google hint: "*human brain is so complex*"
  - http://www.med.harvard.edu/AANLIB/



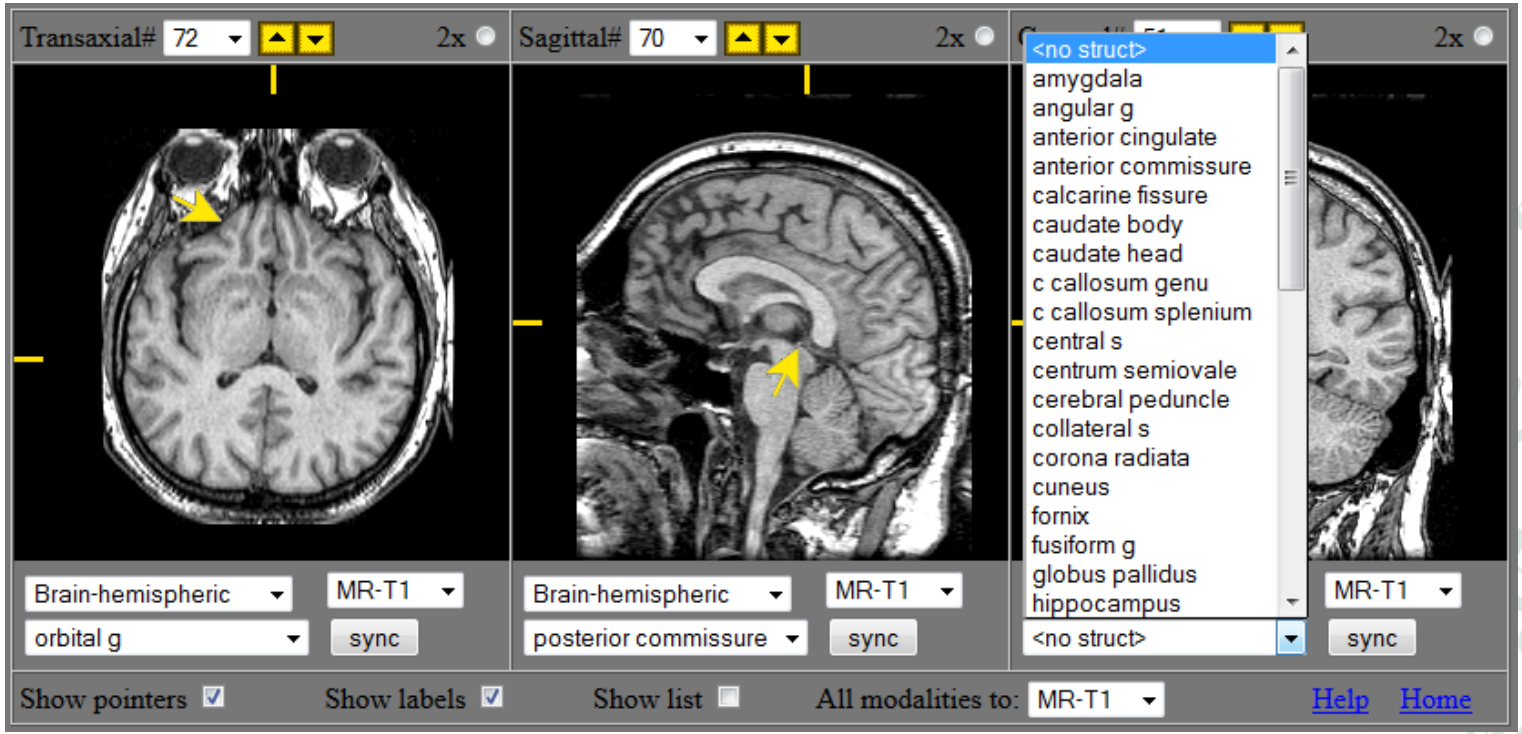
IOActive™

Neuroscience 101



IOActive™

Neuroscience 101



IOActive

EEG / Brain Waves

- Invasive vs Non-invasive

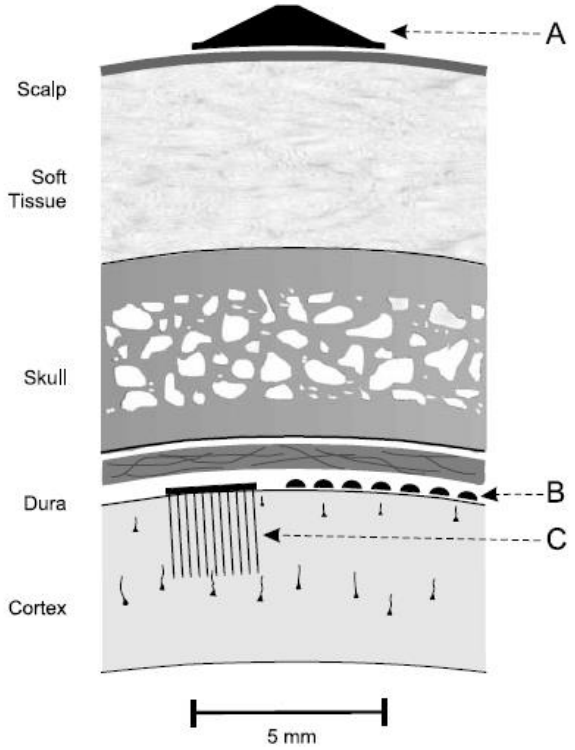


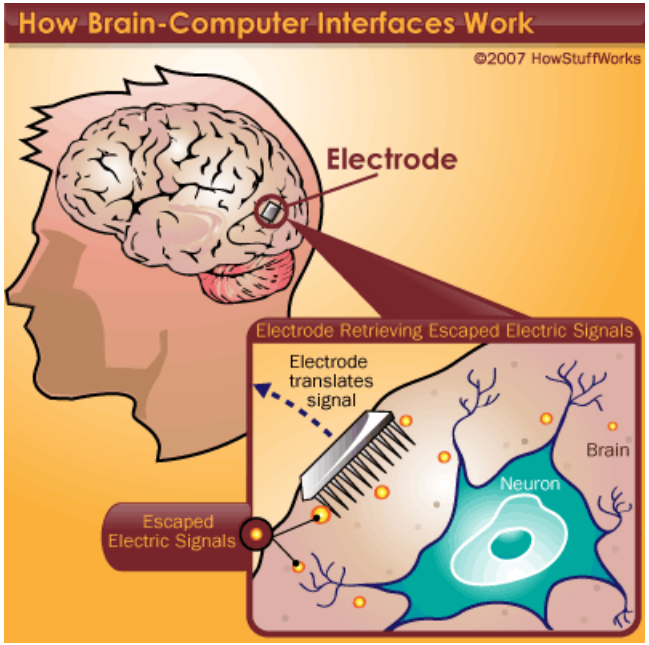
Fig. 2.1 Different types of sensors most commonly used in BCI research. *A*: Electrodes are placed non-invasively on the scalp (electroencephalography (EEG)). *B*: Electrodes are placed on the surface of the brain (electrocorticography (ECoG)). *C*: Electrodes are placed invasively within the brain (single-neuron recordings). (From [112])

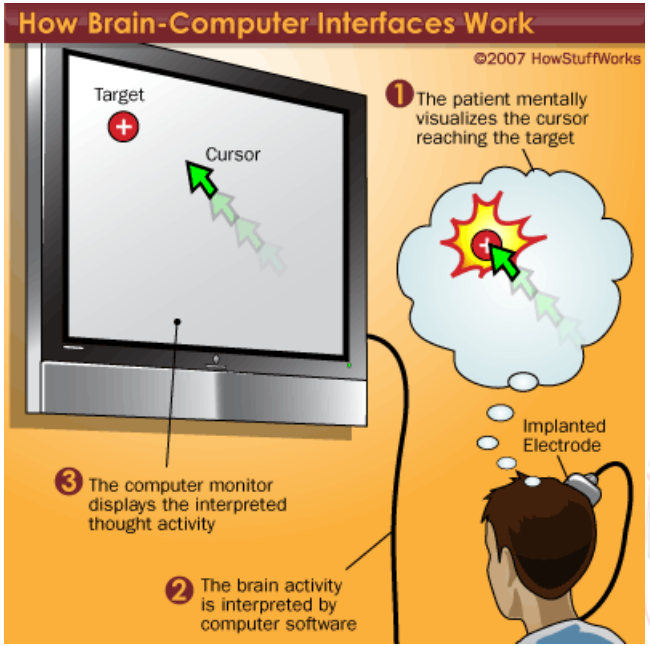
Schalk, Gerwin, Mellinger, Jürgen. (2010). *A Practical Guide to Brain–Computer Interfacing with BCI2000. General-Purpose Software for Brain-Computer Interface Research, Data Acquisition, Stimulus Presentation, and Brain Monitoring.* 1st Edition. Springer-Verlag London.

IOActive™

EEG / Brain Waves

- Invasive vs Non-invasive
  - Invasive





IOActive™

EEG / Brain Waves

- Invasive vs Non-invasive
  - Invasive
    - E.g. BrainGate

IOActive™

EEG / Brain Waves

- Invasive vs Non-invasive
  - Non-invasive: EEG is the most used non-invasive method
    - EEG (*Electroencephalography*)
      - Electrodes on the scalp
    - Not MRI (*Magnetic Resonance Imaging*)
    - Not TMS (T*ranscranial Magnetic Stimulation*)

IOActive™

EEG / Brain Waves

- What is EEG?
  - *“Representation over time of the voltage generated by electrodes recorded at different regions of the brain. The EEG is produced by synaptic activity of cortical neurons.”*

Krauss, G., Fisher, R., Kaplan, P. (September 1st, 2011). *The Johns Hopkins Atlas of Digital EEG: An Interactive Training Guide.* 2nd Edition. Johns Hopkins University Press.

IOActive™

EEG / Brain Waves

- What is EEG?
  - Ease of use non-invasive method to measure the brain activity over time
  - Susceptible to noise

IOActive™

EEG / Brain Waves

- What is EEG?
  - *“The current brain technologies are like trying to listen to a conversation in a football stadium from a blimp”* -- John Donoghue

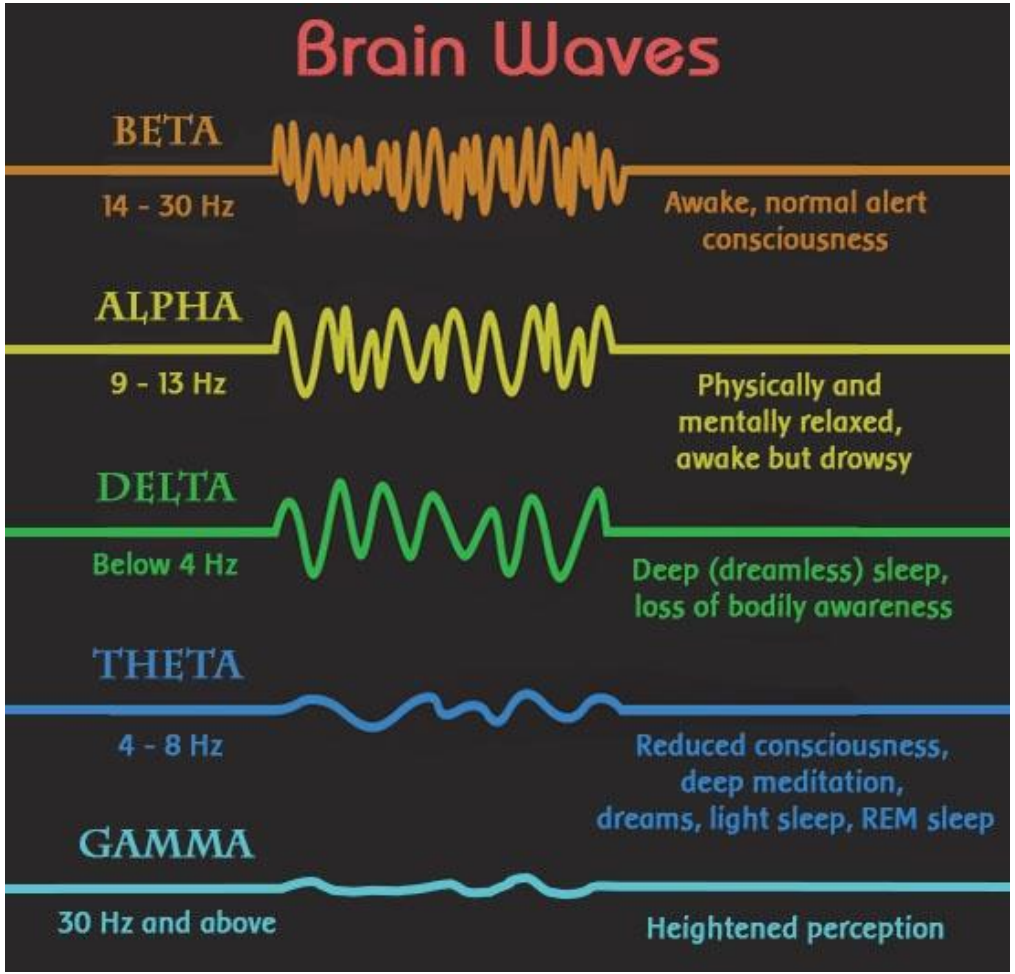
Disruptions: Brain Computer Interfaces Inch Closer to Mainstream
http://bits.blogs.nytimes.com/2013/04/28/disruptions-no-words-no-gestures-just-your-brain-as-a-control-pad/

IOActive™

EEG / Brain Waves

- Brain waves / Frequencies
  - EEG activity is quite small, measured in microvolts (*μV*) with the main frequencies of interest up to approximately 30 Hertz (*Hz*).

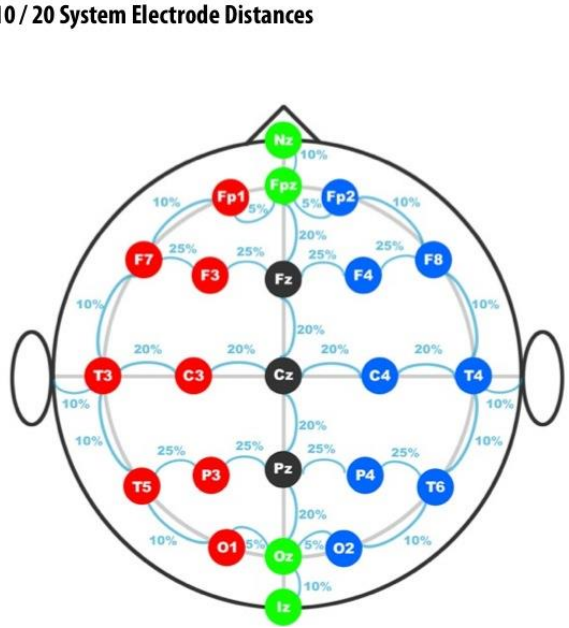
IOActive™



IOActive™

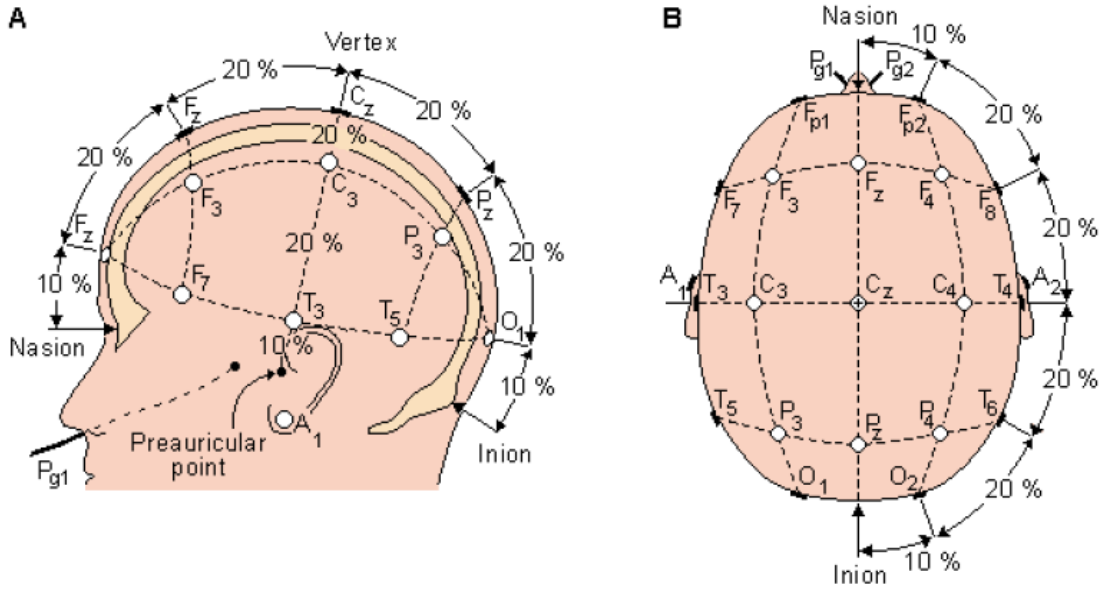
EEG / Brain Waves

- Electrodes / Montages
  - 10-20 System (Internationally recognized method)



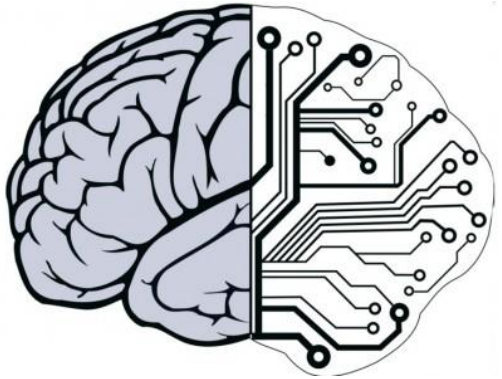
EEG / Brain Waves

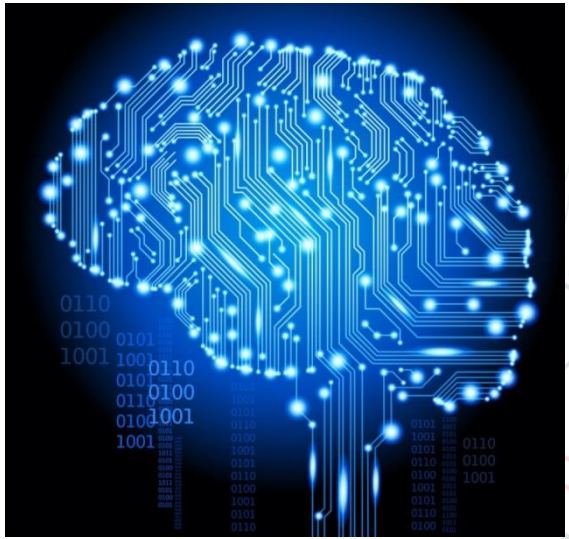
- Electrodes / Montages
  - 10-20 System (Internationally recognized method)



EEG / Brain Waves

- ADC (Analog to Digital conversion)
  - Brain Waves = Analog Signals
  - Digital EEG = Digital Signals
    - Filters and amplifiers in between

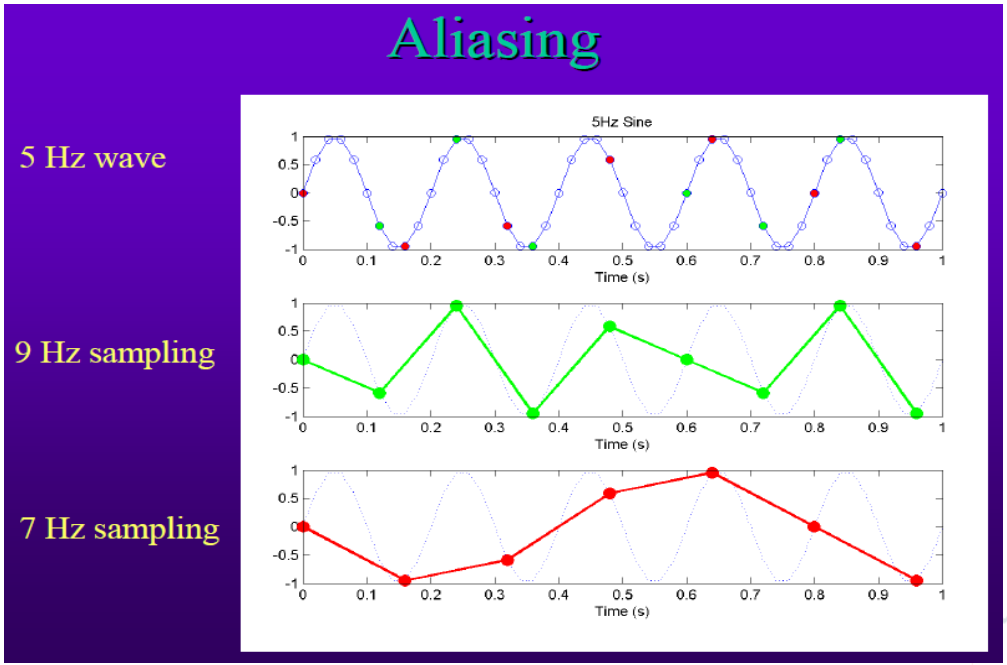




IOActive™

EEG / Brain Waves

- Sampling



Gotman, J. *Digital EEG - From Basics to Advanced Analysis*.
Montreal Neurological Institute. McGill University.

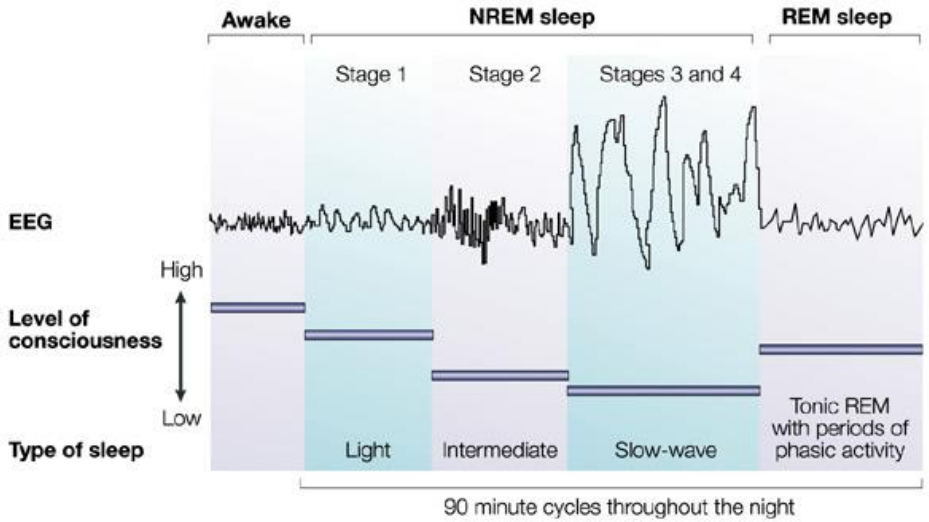
IOActive™

EEG / Brain Waves

- Patterns / Artifacts

EEG / Brain Waves

- Patterns / Artifacts
  - E.g. Stages of sleep



Nature Reviews | Immunology

IOActive

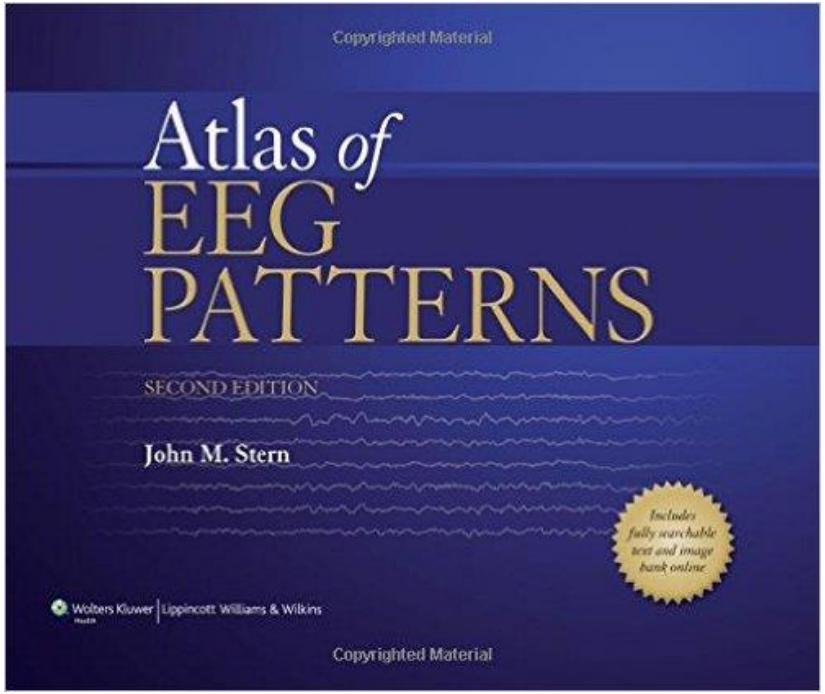
EEG / Brain Waves

- Patterns / Artifacts
  - Artifacts: EEG recording events not due brain activity
    - Eye movement / fluttering
    - Blinking
    - Sweating
    - Muscle movements
    - Electrode shake
    - Etc. etc. etc.

IOActive™

EEG / Brain Waves

- Patterns / Artifacts



IOActive™

EEG / Brain Waves

- Acquisition
  - Commercial
    - Clinical use
      - Expensive hardware (thousands of USD)

    - Cheap hardware
      - NeuroSky MindWave
      - EMOTIV EPOC

IOActive™

EEG / Brain Waves

- Acquisition
  - Non-commercial
    - OpenEEG
    - OpenBCI
    - Many open source software

IOActive™

EEG / Brain Waves

- Acquisition
  - **Demo: Visualization of brain waves with [NeuroSky MindWave]**

Features

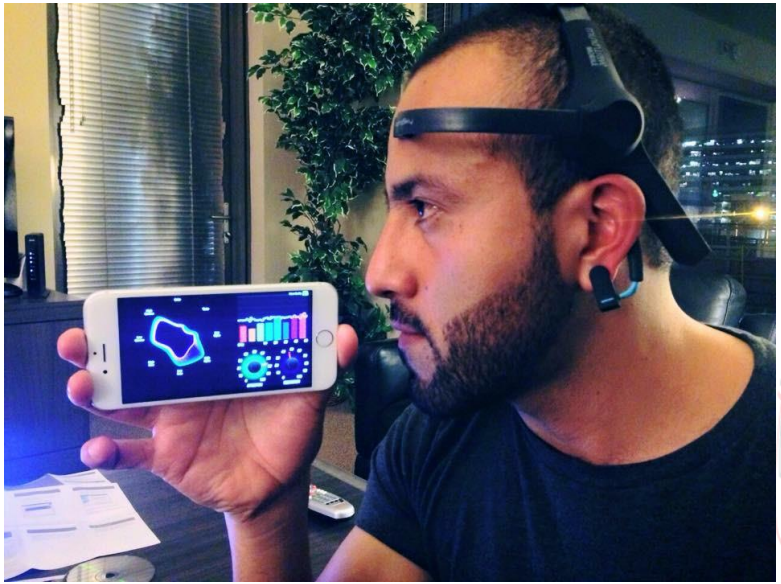
- Direct connect to dry electrode
- One EEG channel + Reference + Ground
- Extremely low-level signal detection
- Advanced filter with high noise immunity
- RAW EEG at 512Hz

Dimensions

- Size: 2.79cm x 1.52cm x 0.25cm
- Weight (Max) 130mg

Specifications

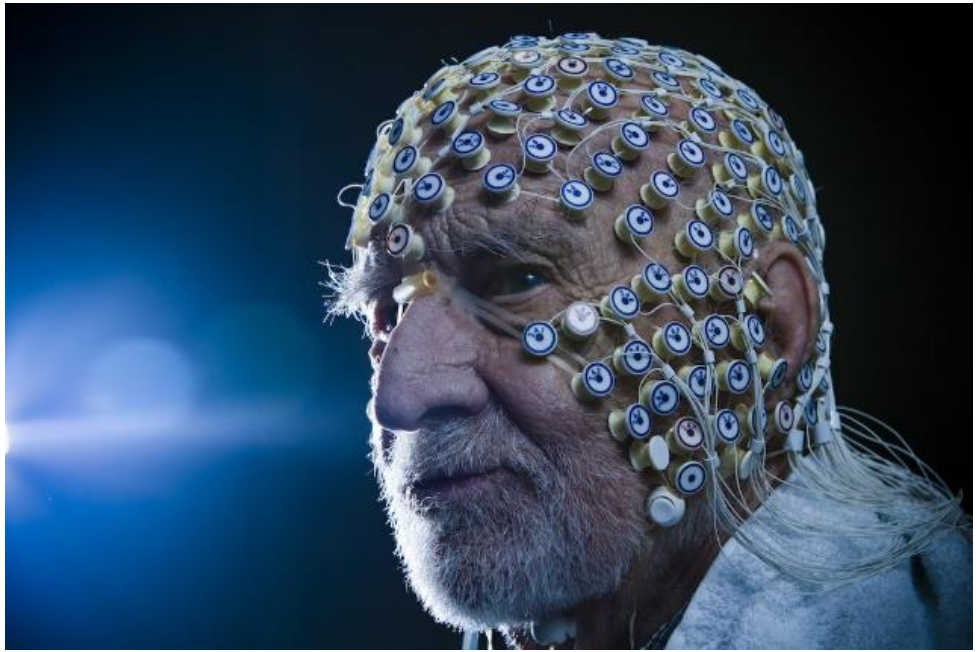
- 512Hz sampling rate
- 3-100Hz frequency range



IOActive™

EEG / Brain Waves

- Uses EEG
  - The importance of security



IOActive™

EEG / Brain Waves

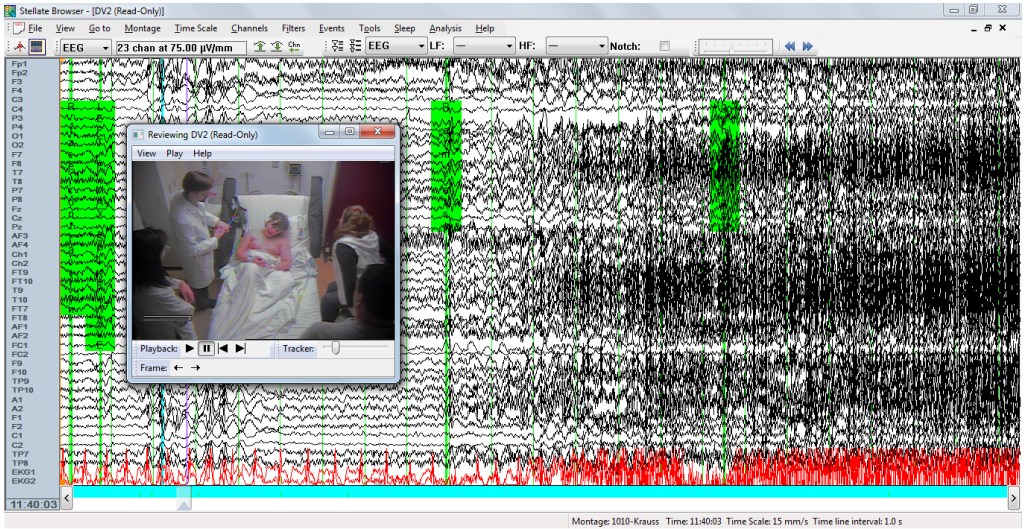
- Uses EEG
  - Clinical
    - *"The EEG is perhaps most useful in the diagnosis and classification of **seizure disorders**… EEGs can be focally abnormal even in the absence of visible change on an MRI… **Sleep disorders** include **narcolepsy, sleep apnea, various parasomnias**, and several other conditions. Narcolepsy can be diagnosed by a combination of clinical history and EEG showing rapid descent into rapid eye movement (REM) sleep."*

Krauss, G., Fisher, R., Kaplan, P. (September 1st, 2011). *The Johns Hopkins Atlas of Digital EEG: An Interactive Training Guide.* 2nd Edition. Johns Hopkins University Press.

IOActive

EEG / Brain Waves

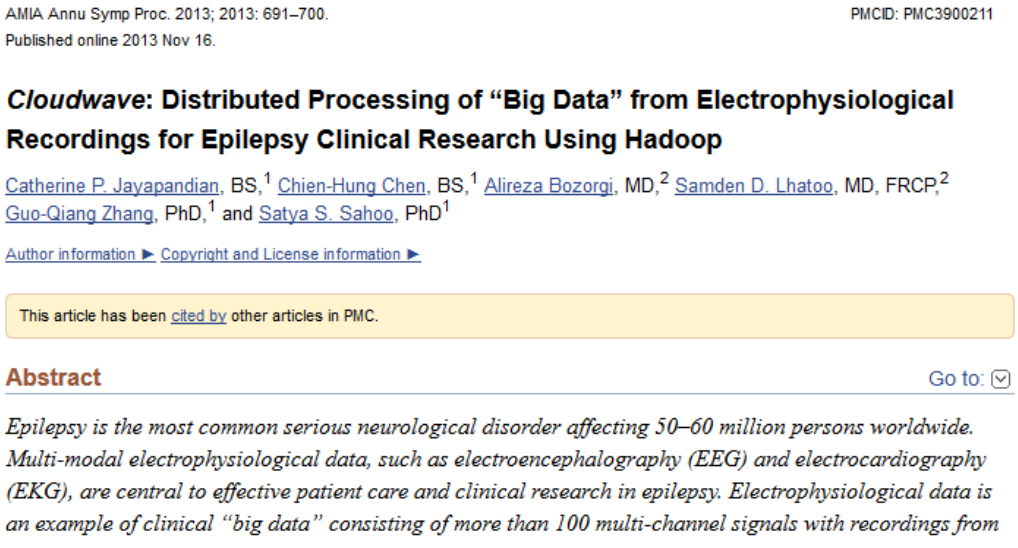
- Uses EEG
  - Clinical
    - **Demo: EEG recording synchronized with video of a patient suffering a seizure**



IOActive™

EEG / Brain Waves

- Uses EEG
  - Research
    - Clinical research



AMIA Annu Symp Proc. 2013; 2013: 691–700.
Published online 2013 Nov 16.

PMCID: PMC3900211

***Cloudwave*: Distributed Processing of "Big Data" from Electrophysiological Recordings for Epilepsy Clinical Research Using Hadoop**

Catherine P. Jayapandian, BS,[1] Chien-Hung Chen, BS,[1] Alireza Bozorgi, MD,[2] Samden D. Lhatoo, MD, FRCP,[2] Guo-Qiang Zhang, PhD,[1] and Satya S. Sahoo, PhD[1]

Author information ▶ Copyright and License information ▶

This article has been cited by other articles in PMC.

Abstract Go to:

Epilepsy is the most common serious neurological disorder affecting 50–60 million persons worldwide. Multi-modal electrophysiological data, such as electroencephalography (EEG) and electrocardiography (EKG), are central to effective patient care and clinical research in epilepsy. Electrophysiological data is an example of clinical "big data" consisting of more than 100 multi-channel signals with recordings from

http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3900211/

IOActive™

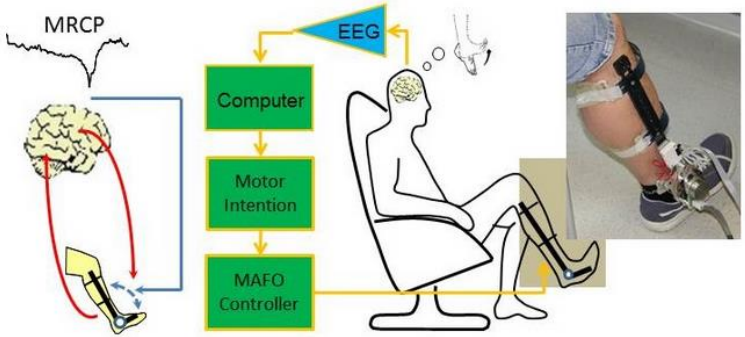
EEG / Brain Waves

- Uses EEG
  - Research

A Closed-Loop Brain-Computer Interface Triggering an Active Ankle-Foot Orthosis for Inducing Cortical Neural Plasticity

Ren Xu, Ning Jiang, Natalie Mrachacz-Kersting, Chuang Lin, Guillermo Asín Prieto, Juan C. Moreno, Jose L. Pons, Kim Dremstrup, and Dario Farina, University Medical Center Göttingen, Georg-August University, Dalian University of Technology, Aalborg University, and Consejo Superior de Investigaciones Científicas

Volume 61, Issue 7, Page:2092-2101



http://tbme.embs.org/2014/07/27/closed-loop-brain-computer-interface-triggering-active-ankle-foot-orthosis-inducing-cortical-neural-plasticity/

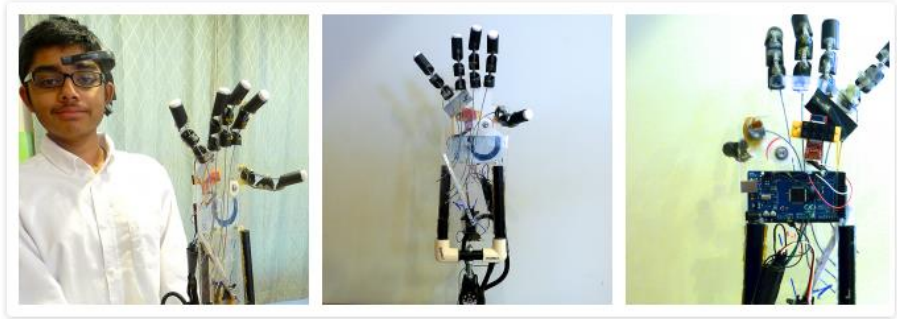
IOActive™

EEG / Brain Waves

- Uses EEG
  - Research

The Arduino Prosthesis Using the Neurosky Mindwave

Inspiration Author: Shiva Nathan



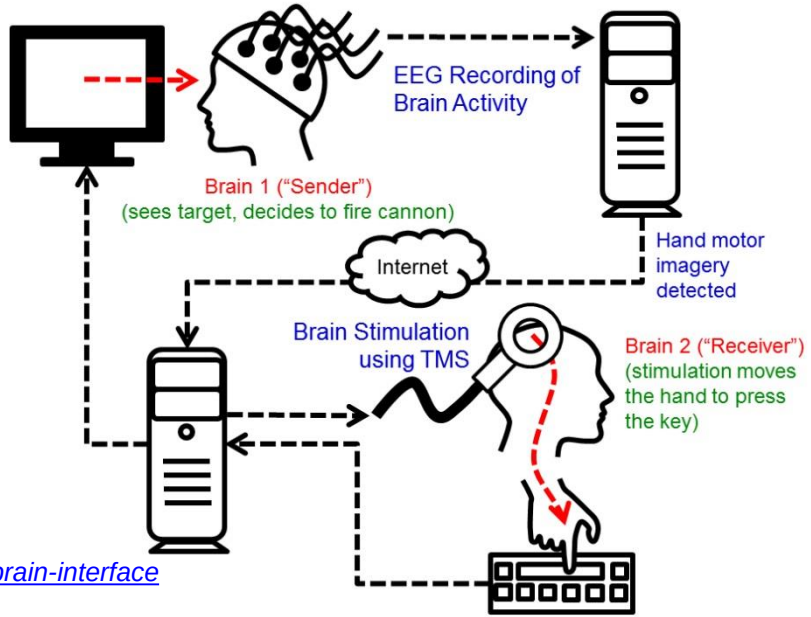
The Arduino Prosthesis is a low cost Prosthetic, a Brain Control Interface (BCI) device that can be fitted on to amputees' limbs. Mind-Waves – or more precisely the ability of the mind to focus and to concentrate – controls the Prosthetic. This is accomplished by using an inexpensive EEG (Electro-Encephalo-Gram)reader that can be worn on the head,like a pair of headphones using a headband.This external device is in contrast to current expensive devices that require an implanted electrode in the arm or leg and require training for effective usage. Also, some of the more expensive prosthetics require myo-electric impulses to control the actuators.

http://learn.parallax.com/inspiration/arduino-prosthesis-using-neurosky-mindwave

IOActive™

EEG / Brain Waves

- Uses EEG
  - Research
    - B2B - Brain-to-Brain Interface



http://www.kurzweilai.net/first-human-brain-to-brain-interface

IOActive

EEG / Brain Waves

- Uses EEG
  - Research
    - B2B - Brain-to-Brain Interface

First human brain-to-brain interface

August 28, 2013

University of Washington researcher Rajesh Rao, left, plays a computer game with his mind. Across campus, researcher Andrea Stocco, right, wears a magnetic stimulation coil over the left motor cortex region of his brain. Stocco's right index finger moved involuntarily to hit the "fire" button as part of the first human brain-to-brain interface demonstration. (Credit: University of Washington)

http://www.kurzweilai.net/first-human-brain-to-brain-interface

IOActive™

EEG / Brain Waves

- Uses EEG
  - Research
    - Babylab Research Centre

http://www.wired.co.uk/magazine/archive/2013/03/start/this-little-piggy-went-to-the-lab

IOActive™

EEG / Brain Waves

- Uses EEG
  - Research
    - Controlling stuff with mind waves

Brain-controlled drone shown off by Tekever in Lisbon

http://www.bbc.com/news/technology-31584547

IOActive™

EEG / Brain Waves

- Uses EEG
  - Research
    - Controlling stuff with mind waves

IOActive™

EEG / Brain Waves

- Uses EEG
  - Security
    - Biometric

Thanks to researchers at the UC Berkeley School of Information, you may not need to type those pesky passwords in the future. Instead, you'll only need to think them.

By measuring brainwaves with biosensor technology, researchers are able to replace passwords with "passthoughts" for computer authentication. A $100 headset wirelessly connects to a computer via Bluetooth, and the device's sensor rests against the user's forehead, providing a electroencephalogram (EEG) signal from the brain.

Other biometric authentication systems use fingerprint or retina scans for security, but they're often expensive and require extensive equipment. The NeuroSky Mindset looks just like any other Bluetooth set and is more user-friendly, researchers say. Brainwaves are also unique to each individual, so even if someone knew your passthought, their emitted EEG signals would be different.

http://mashable.com/2013/04/09/passwords-thoughts/

WHAT COULD POSSIBLY GO WRONG ?!

IOActive

EEG / Brain Waves

- Uses EEG
  - Security

Researchers studying brain activity to determine cybersecurity threats

By Julie Ferrell
Staff Writer
jferrell@amestrib.com

Three Iowa State University researchers have studied brainwaves as a way to indicate employees who may be at the highest risk of becoming a cybersecurity threat.

Qing Hu, Union Pacific Professor in information systems, along with assistant professor of marketing Laura Smarandescu and Robert West, professor in psychology, published the findings in the Journal of Management Information Systems.

Based on brain activity, the team found test subjects with lower self-control were more at risk of giving away secure company information.

Hu said roughly half of the cybersecurity incidents in the last year came from internal employees, and even external threats occasionally involved an employee unintentionally releasing information through instances like responding to spam emails.

http://amestrib.com/news/researchers-studying-brain-activity-determine-cybersecurity-threats

IOActive™

EEG / Brain Waves

- Uses EEG
  - Military

Translating Soldier Thoughts to Computer Commands

by BRYANT JORDAN on AUGUST 7, 2015

22 26 5

The Army Research Laboratory is funding research that would enable troops to communicate via a cellphone or radio without uttering a sound or moving a finger.

http://defensetech.org/2015/08/07/translating-soldier-thoughts-to-computer-commands/

IOActive

EEG / Brain Waves

- Uses EEG
  - Military

JEAN VETTEL: ARMY RESEARCH LAB TECHNOLOGY SEEKS TO DETECT BATTLEFIELD THREATS VIA BRAIN WAVES

JANE EDWARDS · MAY 26TH, 2015

Researchers at the U.S. Army Research Laboratory have demonstrated a headgear equipped with electroencephalography sensors they designed to detect threats on the battlefield via the wearer's brain waves, the Army said May 18.

Dr. Jean Vettel, a neuroscientist at the research lab, said the brain wave detection technology could be used by soldiers to tag threatening images from a collection of digital pictures captured by robotic assets on the battlefield without clicking a button or saying a word, C. Todd Lopez writes.

"And then when we have images labeled, we can take those images and give it to a machine learning algorithm that can learn to distinguish between threatening or non-threatening images," Vettel said at the Defense Department Lab Day event May 14.

http://www.executivegov.com/2015/05/jean-vettel-army-research-lab-technology-seeks-to-detect-battlefield-threats-via-brain-waves/

IOActive

EEG / Brain Waves

- Uses EEG
  - Neurofeedback
    - MUSE headband for relaxation

http://www.choosemuse.com

IOActive™

EEG / Brain Waves

- Uses EEG
  - Neurofeedback + Art
    - Environmental Disturbances by Anni Garza Lau

http://annigarzalau.com/anni-garza-lau--environmental-disturbances.html

IOActive™

EEG / Brain Waves

- Uses EEG
  - Art
    - Music created with Brainwaves

http://thecreatorsproject.vice.com/blog/eunoia-seeking-enlightenment-by-tracking-brainwaves

IOActive™

EEG / Brain Waves

- Uses EEG
  - Others

Brain scan delays sentencing hearing for convicted murderer in Brooksville

BROOKSVILLE — Murderer Byron Burch's sentencing has been delayed until late July after his defense ordered a new scan of Burch's brain, catching the prosecution off guard.

Burch was convicted of first-degree murder last week in the 2010 killing of Sarah Davis, a retired Brooksville teacher and community matriarch.

He faces either life in prison without the possibility of parole or the death penalty.

Byron Burch

The defense originally utilized a method called quantitative electroencephalography to map Burch's brain activity. However, the state raised concerns about the scan's reliability, and the court ruled it inadmissible.

http://www.tampabay.com/news/courts/brain-scan-delays-sentencing-hearing-for-convicted-murderer-in-brooksville/2233777

IOActive™

EEG / Brain Waves

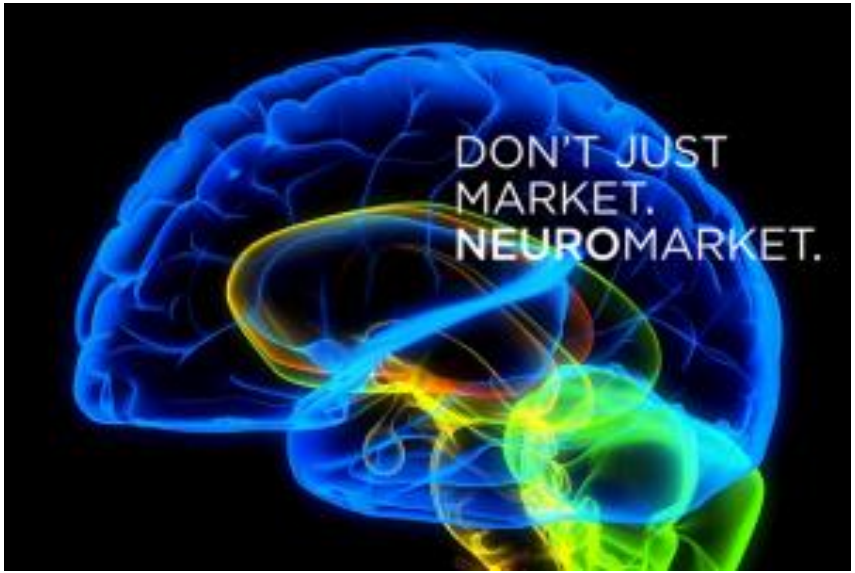
- Uses EEG
  - Others
    - NeuroGaming

http://www.neurogamingconf.com

IOActive™

EEG / Brain Waves

- Uses EEG
  - Others
    - NeuroMarketing



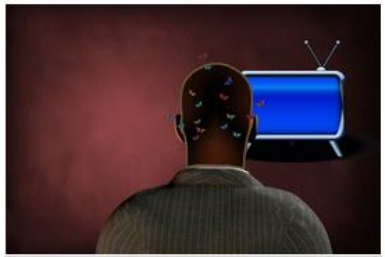
IOActive™

EEG / Brain Waves

- Uses EEG
  - Others

Blockbuster or Bust? Brain Waves May Predict Movie Success

by Rachael Rettner, Senior Writer | March 10, 2015 08:01am ET



Pin it

Credit: Bruce Rolff/Shutterstock.com

View full size image

People's brain waves may reveal which movies they like, and even predict which movies will do well at the box office, a new study suggests.

In the study, researchers had 32 college students watch 18 movie trailers each; the students had electrodes placed on their scalps to measure their brain waves, a test known as electroencephalography, or EEG.

The researchers then looked at the EEG data on certain brain waves, called beta and gamma waves. Results showed that the beta brain waves were linked with people's rankings of the movies: The more beta wave brain activity there was as a participant watched a movie, the higher that individual ranked the movie.

After they watched each trailer, the participants were asked to rate how much they liked the movie and how much they'd be willing to pay for a DVD of it. After viewing all 18 trailers, the participants were asked to rank the movies in order of preference. [10 Things You Didn't Know

http://www.livescience.com/50092-brain-waves-movie-success.html

IOActive™

EEG / Brain Waves

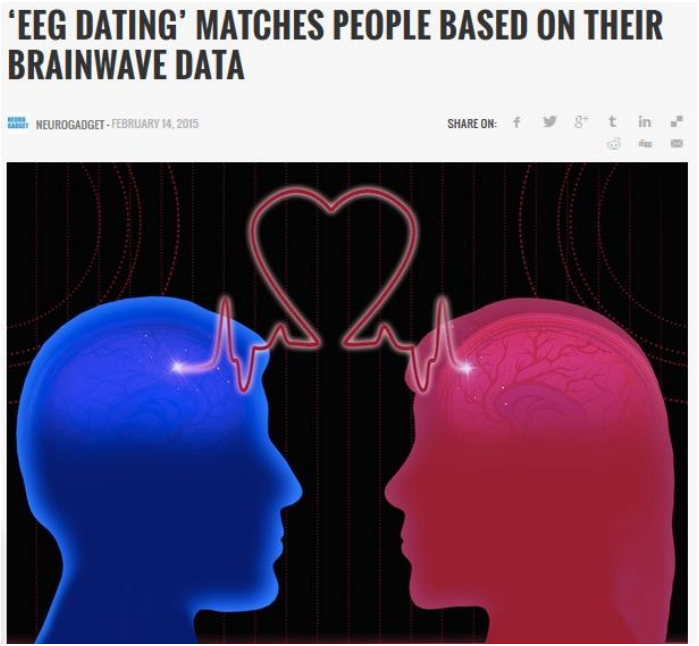
- Uses EEG
  - Others
    - Neurowear

http://www.neurowear.com

IOActive™

EEG / Brain Waves

- Uses EEG
  - Others



http://neurogadget.com/2015/02/14/eeg-dating-matches-people-based-brainwave-data

EEG / Brain Waves

- Uses EEG
  - Others

Neuroscience Gets Radical: How to Study Surfers' Brain Waves

By Eliza Strickland
Posted 28 Oct 2014 | 13:00 GMT

Share | Email | Print | Reprint

Photo: Red Bull

At Red Bull's surf camp in Salina Cruz, Mexico, Jake Marshall surfed for science.

http://spectrum.ieee.org/tech-talk/biomedical/imaging/neuroscience-gets-radical-how-to-study-surfers-brain-waves

IOActive™

EEG / Brain Waves

- Uses EEG
  - The Cloud
    - Neuroelectrics' NUBE

NE006

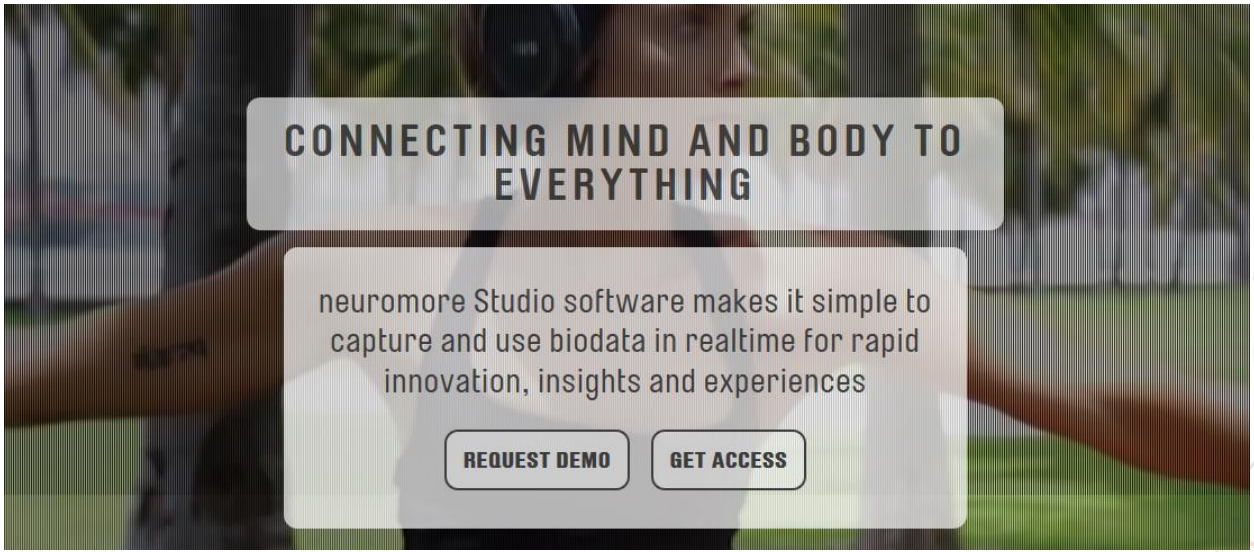
ENOBIO 32

Enobio® is a wearable, wireless electrophysiology sensor system for the recording of EEG. Using the superb Neuroelectrics Cap, Enobio 32 is ideal for high-density recording research applications. It comes integrated with an intuitive, powerful user interface for easy configuration, recording and visualization of 24 bit EEG data at 500 S/s, including Spectrogram and 3D visualization in real time of spectral features. It is ready for research or clinical use as well as telemedicine using our NUBE cloud system for experimental data collection and organization. In addition to EEG, triaxial accelerometer data is automatically collected. You can also use a microSD card to save data offline in Holter mode. Enobio is a CE medically certified product. It is currently classified as an investigational device under US federal law.

IOActive

EEG / Brain Waves

- Uses EEG
  - The Cloud
    - Neuromore



http://www.neuromore.com

IOActive

(In)security Aspects

- Attack scenarios
  - Reply attacks with saved EEG data to
    - Control things
      - Drones
      - Prosthesis
      - Etc.
    - Bypass authentication
  - Unauthorized update of EEG data from a ~~criminal~~ patient in a hospital network
  - Trade of EEG data for behavior analysis in neuromarketing
  - Client-side attacks on doctors/physicians' computers with malicious EEG (meta)data

IOActive™

(In)security Aspects

- Attack scenarios
  - Hard to achieve
    - Understand the environment
      - The EEG technology in use. Product X != Product Y
    - Understand the protocols in use, if any
    - Understand the file formats in use
    - **Special expertise required**
      - Electroencephalography
        - » What EEG data to modify, how and where
  - Feasible, though
    - See the following demos

IOActive

(In)security Aspects

- Design
  - Some of them include security

TWin Monitor 2 Remote Control/Viewing Software installed on any record or review station uses standard TCP/IP protocols to broadcast in-lab, in-hospital or over the internet.

After logging in, an image of the TWin Monitor host screen is broadcasted to the viewing computer. To the remote user TWin will operate the same as if it was installed on the remote PC.

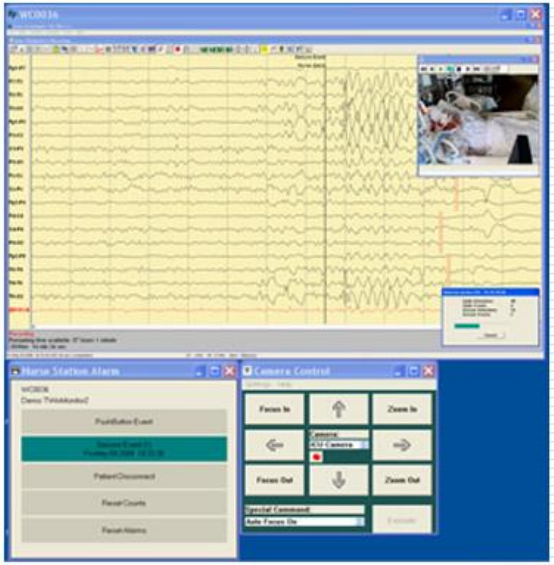
TWin Monitor 2 uses encryption and authentication for information that travels over the network, which is an added benefit to comply with HIPAA regulations

Allows the user to:

- Remote view EEG/PSG data over the local area network or over the WWW.
- Remote view the same recording system from different locations.
- Remote control and operate the EEG/PSG/LTM recording system (record or review).
- Score PSG records from home or other locations.

ORDERING INFORMATION

Model	
TWINMON-CD	TWin Monitor 2 Remote Control/Viewing Software



TWin Monitor 2 Viewer

IOActive

(In)security Aspects

- Design
  - Some of them include security
    - Neuromore
      - E.g Biodata to the cloud through a SSL channel

IOActive™

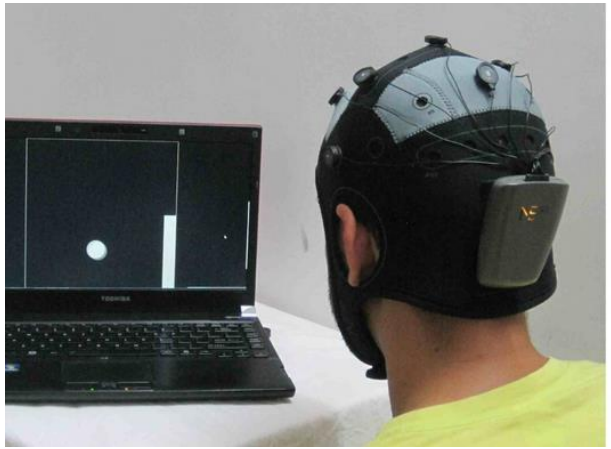
(In)security Aspects

- Design
  - However, no security keywords
    - '*secur*', *'crypt*', *'auth*', '*passw*', etc.
    - In 90% of the reviewed
      - Manuals
      - Technical specs
      - Brochures

IOActive™

(In)security Aspects

- Encryption
  - In Transit
    - Brain waves on the wire: Digital streaming over TCP/IP



0, 1, 1, 0, 0, …

internet

WHAT COULD POSSIBLY GO WRONG ?!

IOActive™

(In)security Aspects

- Encryption
  - In Transit
    - Brain waves on the wire: Digital streaming over TCP/IP
      - Google dorks:
        - » *+<product_name> +tcp +port*
        - » *neuro acquisition +tcp +port*
        - » *+eeg +tcp*

IOActive™

(In)security Aspects

- Encryption
  - In Transit
    - Brain waves on the wire: Digital streaming over TCP/IP

BRAIN VISION professional RECVIEW

BrainVision RecView:
Software for real-time data analyses

BrainVision RecView is an advanced solution designed for real-time analysis of data received over the Ethernet network via TCP/IP directly from the Recorder software. BrainVision RecView is widely used in the EEG/fMRI co-registration to remove both the gradient and the ballistocardiogram artifact permitting experimental control during the scan. The innovative Template Drift Compensation algorithm remedies template jitter caused by imperfect synchronization between the EEG amplifier and the scanner clock and thus ensures optimal data correction at any time.

IOActive

(In)security Aspects

- Encryption
  - In Transit
    - Brain waves on the wire: Digital streaming over TCP/IP

Measure biosignals reliably even outside in the Himalayas

g.MOBIlab+ In the HimalayasDuring an Austrian expedition to Chulu Far West in Nepal (6419 m) g.MOBIlab+ was used to measure the effect of high altitude on the EEG and ECG parameters. The expedition started in Besi Sahar at an altitude of 700 m near Annapurna I. The team gained each day a height between 300 and 600 m and settled basecamp at 4800 m. After one night in BC the highcamp was established in 5600 m on the Chulu glacier. At 3 p.m. in the morning the team started to climb Chulu Far West (right picture) and reached the summit at 11 a.m. g.MOBIlab+ was used to record 2 EEG channels over the sensorimotor areas and 1 ECG channel of 2 expedition members. The persons performed a self-paced finger movement every 10 seconds.The on-set and off-set of the movement was recorded by an external switch connected to g.MOBIlab.

EEG and ECG data recording at the Dachstein glacier

g.MOBIlab at Dordic Fitness Days - DachsteinAt the 2003 Nordic Fitness Days at the Dachstein glacier organized by the Planaibahnen from October 24th-26th g.MOBIlab+ was tested in measuring EEG and ECG data of skiers and mountaineers going up the Dachstein summit with the cable car. The study was part of the research program of the ARGE Alpinmed. A total of 50 data sets were acquired within 3 days. Data recordings started at a base station in 1200 m. Then physiological data of subjects were measured in the cable car and at the top station in 2700 m. The subjects had to perform a stimulus-reaction paradigm in order to test the reliability of g.MOBIlab+ under bad weather and field conditions. In all 50 sessions data quality was excellent and even EEG data displayed high signal-to-noise ratio.

IOActive™

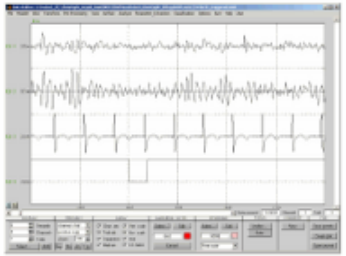
(In)security Aspects

- Encryption
  - In Transit
    - Brain waves on the wire: Digital streaming over TCP/IP

Excellent data quality

g.MOBIlab+ data in g.BSanalyzeg.MOBIlab+ is equipped with low-noise biosignal amplifiers and a 16-bit A/D converter (256 Hz) which guarantees excellent data quality and a high signal-to-noise ratio. For sophisticated data analyses g.MOBIlab-data can be imported directly into g.BSanalyze, the toolbox for advanced biosignal processing and analyses.

Data can also be converted into ASCII-format for other programs like MS-Excel or foreign toolboxes.



Remote control of g.MOBIlab+

g.MOBIlab+ can also be remote controlled over a TCP/IP network. Just plug g.MOBIlab+ to the g.tec Remote Control Unit and connect it to a standard network connection. g.MOBIlab+ will be visible on every other PC in the network and can be used as connected to the own PC.

IOActive

(In)security Aspects

- Encryption
  - In Transit
    - Case: [Neuroelectrics NIC]

Sending commands to NIC

NIC can be remotely commanded from a third-party software through a set of commands that can be sent using a TCP/IP connection. NIC listens to the **TCP/IP port 1235** for incoming connections. The clients that connect to that port can command the following actions:

Action	Device
Start EEG streaming	Enobio & StarStim
Stop EEG streaming	Enobio & StarStim
Start Stimulation	StarStim
Abort Stimulation	StarStim
Online tACS Frequency Change	StarStim
Online tACS Amplitude change	StarStim
Online tDCS Amplitude change	StarStim
Load template	StarStim
Request status	Enobio & StarStim

NIC responds to those commands with a set of status commands to indicate whether the commands are successfully processed, the stimulation is ready to be started and so on. The following table shows all the possible status value that NIC might send.

Status	Device
Remote control allowed	Enobio & StarStim
Remote control rejected	Enobio & StarStim
Device is idle	Enobio & StarStim
EEG streaming is ON	Enobio & StarStim
EEG streaming is OFF	Enobio & StarStim
Template not loaded	StarStim
Template loaded	StarStim
Stimulation is ready to be started	StarStim
Stimulation is ON	StarStim
Stimulation is OFF	StarStim

IOActive™

(In)security Aspects

- Encryption
  - In Transit
    - Case: Neuroelectrics NIC

Controlling ENOBIO

> When controlling a Enobio device only two actions might be commanded from the TCP/IP client: to sart and to stop the EEG streaming. In order to do so the client needs to successfully **connect to the TCP/IP server** port:

- **[ret, socket] = NICRemoteStimulationServerConnect(host);**

> Once connected the **starting of the EEG** streaming is asked through the following call:

- **ret = NICRemoteStimulationServerStartEEG (socket);**

> When the EEG streaming is ON the data can be captured through a separated server which runs on the port 1234. The 8/20 channel samples are sent in 4 bytes in two's complement. The MSB byte of each sample is sent first.

IOActive™

(In)security Aspects

- Encryption
  - In Transit
    - Case: [Neuroelectrics NIC]

Receiving data streams from NIC

Receiving data streams using TCP/IP

The NIC software has a TCP/IP server that streams the EEG data received from Enobio. Up to 5 clients can connect to that server simultaneously in order to receive the EEG data ans perform the desired operations in real time.

The software clients that want to receive the EEG data in real time from NIC need to connect to the **TCP/IP port 1234** of the host where the NIC software is running. Once the client software is connected to the server, it will receive the EEG data streaming according to the following format:

Channel 1				...	Channel N			
(MSB) Byte#1	Byte#2	Byte#3	(LSB) Byte#4	...	Byte#1	Byte#2	Byte#3	Byte#4

IOActive™

(In)security Aspects

- Encryption
  - In Transit
    - Case: LabStreamingLayer

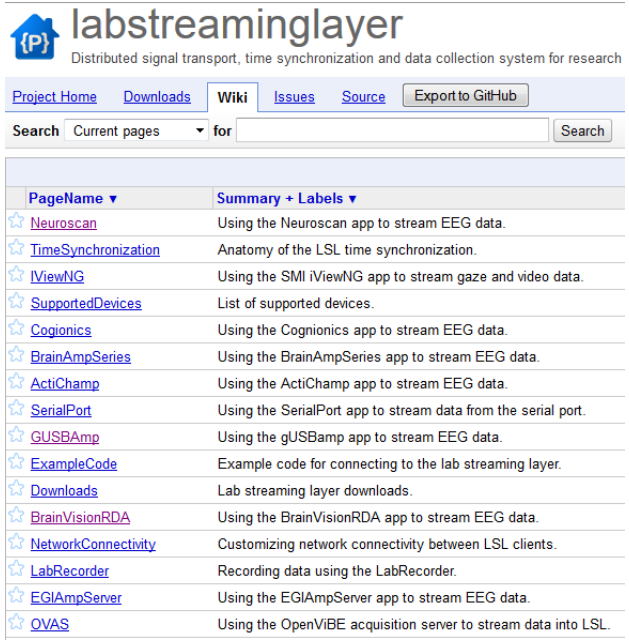
The **lab streaming layer** (LSL) is a system for the unified collection of measurement time series in research experiments that handles both the networking, time-synchronization, (near-) real-time access as well as optionally the centralized collection, viewing and disk recording of the data.

The **LSL distribution** consists of:

- The core transport library (liblsl) and its language interfaces (C, C++, Python, Java, C#, MATLAB). The library is general-purpose and cross-platform (Win/Linux/MacOS, 32/64) and forms the heart of the project.
- A suite of tools built on top of the library, including a recording program, online viewers, importers, and apps that make data from a range of acquisition hardware available on the lab network (for example audio, EEG, or motion capture).

(In)security Aspects

- Encryption
  - In Transit
    - Case: LabStreamingLayer



labstreaminglayer

Distributed signal transport, time synchronization and data collection system for research

Project Home | Downloads | Wiki | Issues | Source | Export to GitHub

Search: Current pages for: Search

PageName ▾	Summary + Labels ▾
Neuroscan	Using the Neuroscan app to stream EEG data.
TimeSynchronization	Anatomy of the LSL time synchronization.
IViewNG	Using the SMI iViewNG app to stream gaze and video data.
SupportedDevices	List of supported devices.
Cognionics	Using the Cognionics app to stream EEG data.
BrainAmpSeries	Using the BrainAmpSeries app to stream EEG data.
ActiChamp	Using the ActiChamp app to stream EEG data.
SerialPort	Using the SerialPort app to stream data from the serial port.
GUSBAmp	Using the gUSBamp app to stream EEG data.
ExampleCode	Example code for connecting to the lab streaming layer.
Downloads	Lab streaming layer downloads.
BrainVisionRDA	Using the BrainVisionRDA app to stream EEG data.
NetworkConnectivity	Customizing network connectivity between LSL clients.
LabRecorder	Recording data using the LabRecorder.
EGIAmpServer	Using the EGIAmpServer app to stream EEG data.
OVAS	Using the OpenViBE acquisition server to stream data into LSL.

https://github.com/sccn/labstreaminglayer/wiki/SupportedDevices.wiki

IOActive™

(In)security Aspects

- Encryption
  - In Transit
    - Case: LabStreamingLayer

Sending Random Data in C++

```
#include "lsl_cpp.h"
#include <stdlib.h>
using namespace lsl;

/**
 * This is an example of how a simple data stream can be offered on the network.
 * Here, the stream is named SimpleStream, has content-type EEG, and 128 channels.
 * The transmitted samples contain random numbers (and the sampling rate is irregular
 * and effectively bounded by the speed at which the program can push out samples).
 */

int main(int argc, char* argv[]) {

        // make a new stream_info (128ch) and open an outlet with it
        stream_info info("SimpleStream","EEG",128);
        stream_outlet outlet(info);

        // send data forever
        float sample[128];
        while(true) {
                // generate random data
                for (int c=0;c<128;c++)
                        sample[c] = (rand()%1500)/500.0-1.5;
                // send it
                outlet.push_sample(sample);
        }

        return 0;
}
```


IOActive™

(In)security Aspects

- Encryption
  - In Transit
    - Case: LabStreamingLayer

Receiving Data in C++

```
#include "lsl_cpp.h"

/**
 * This is a minimal example that demonstrates how a multi-channel stream (here 128ch)
 * of a particular name (here: SimpleStream) can be resolved into an inlet, and how the
 * raw sample data & time stamps are pulled from the inlet. This example does not
 * display the obtained data.
 */

int main(int argc, char* argv[]) {
        using namespace lsl;

        // resolve the stream of interest & make an inlet to get data from the first result
        std::vector<stream_info> results = resolve_stream("name","SimpleStream");
        stream_inlet inlet(results[0]);

        // receive data & time stamps forever (not displaying them here)
        float sample[128];
        while (true)
                double ts = inlet.pull_sample(&sample[0],128);

        return 0;
}
```

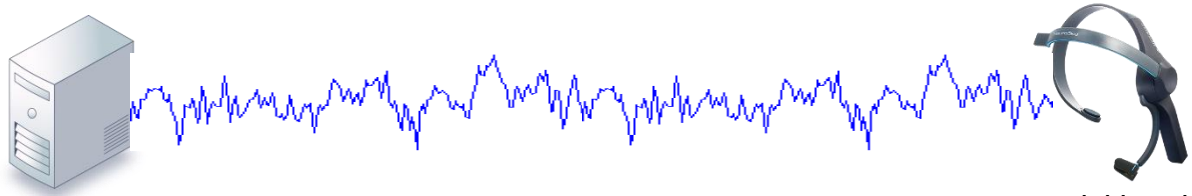
(In)security Aspects

- Encryption
  - In Transit
    - **Demo: Sniffing raw brain signals through a MITM attack between the acquisition device (NeuroSky MindWave) and a remote NeuroServer**
      - NeuroServer: EEG signal transceiver using TCP/IP and EDF format
      - Old and unmaintained
      - Still in use (mostly research)
      - Included in BrainBay

IOActive

(In)security Aspects

- Encryption
  - In Transit
    - **Demo: Sniffing raw brain signals through a MITM attack between the acquisition device (NeuroSky MindWave) and a remote NeuroServer**



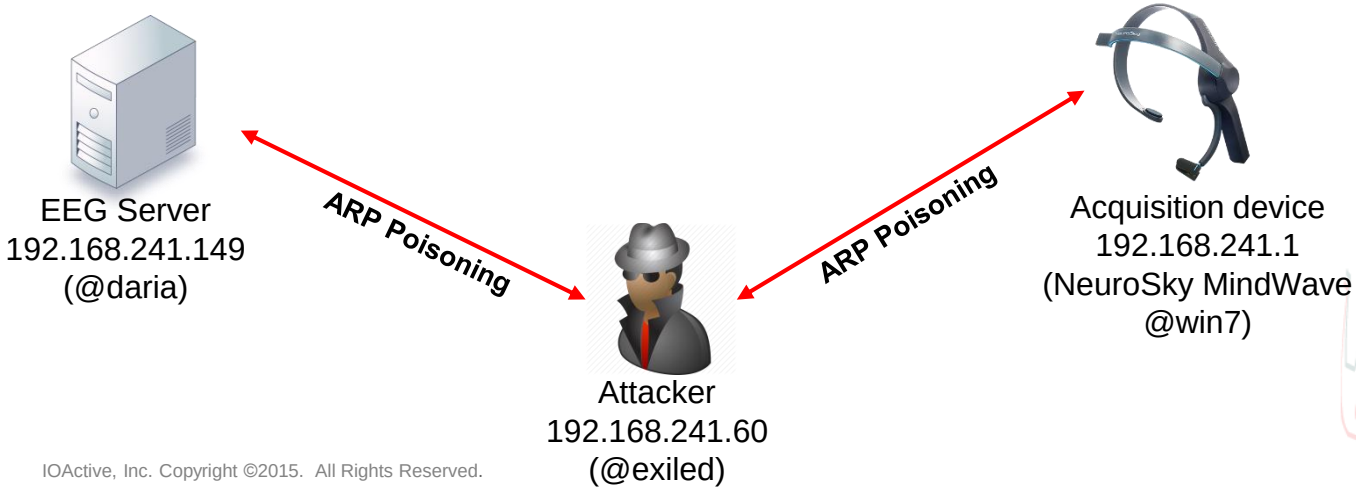
EEG Server
192.168.241.149
(@daria)

Acquisition device
192.168.241.1
(NeuroSky MindWave
@win7)

IOActive

(In)security Aspects

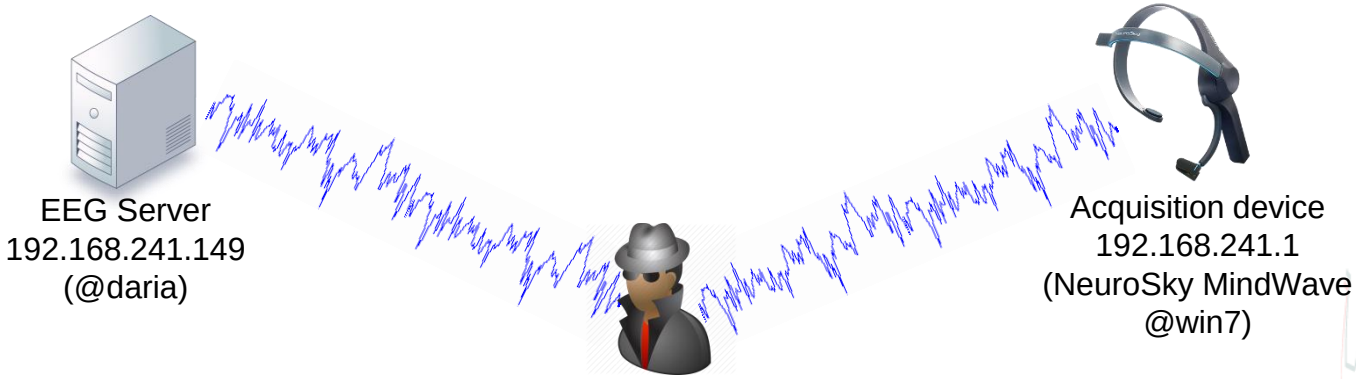
- Encryption
  - In Transit
    - **Demo: Sniffing raw brain signals through a MITM attack between the acquisition device (NeuroSky MindWave) and a remote NeuroServer**



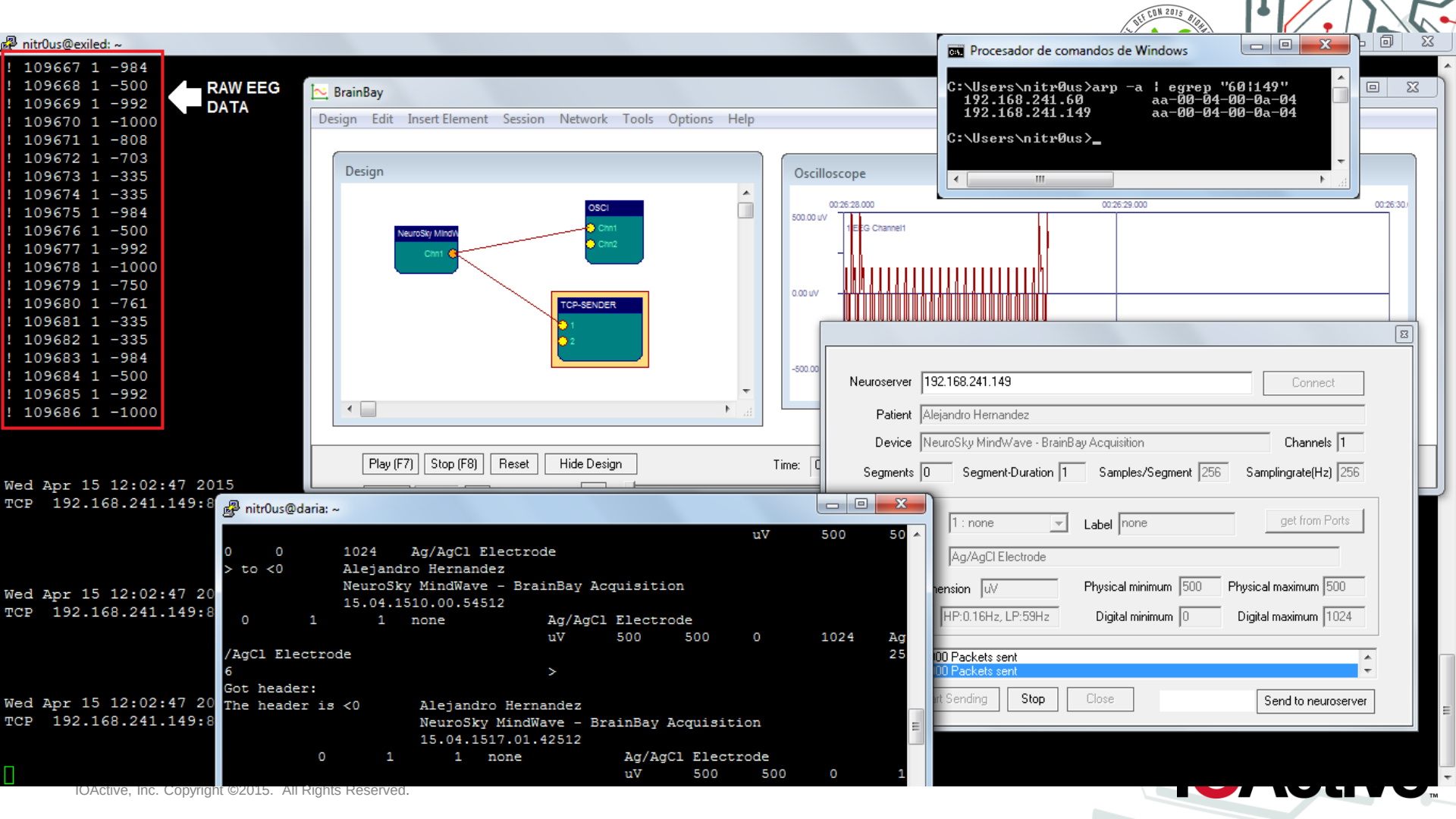
IOActive

(In)security Aspects

- Encryption
  - In Transit
    - **Demo: Sniffing raw brain signals through a MITM attack between the acquisition device (NeuroSky MindWave) and a remote NeuroServer**

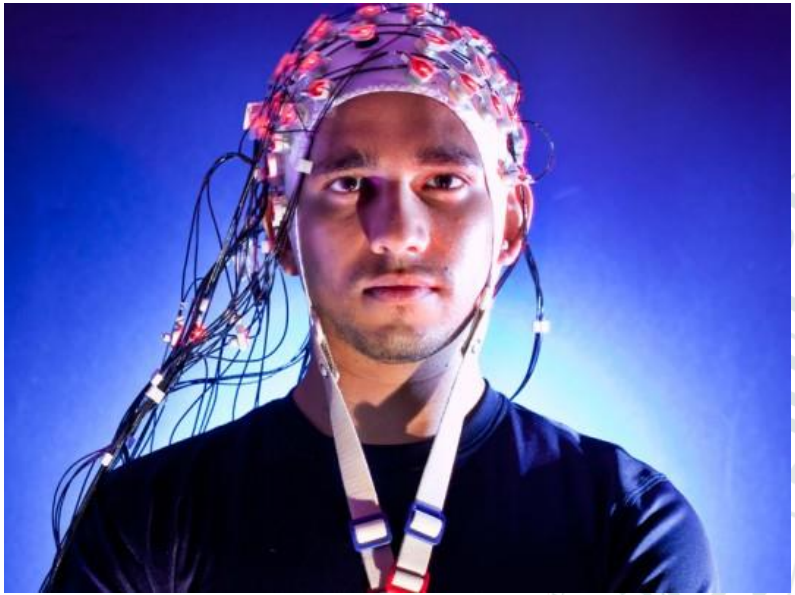


IOActive



(In)security Aspects

- Encryption
  - In Rest
    - File formats, as common files, no encryption
    - What about the cloud? How are they protecting your brain waves?



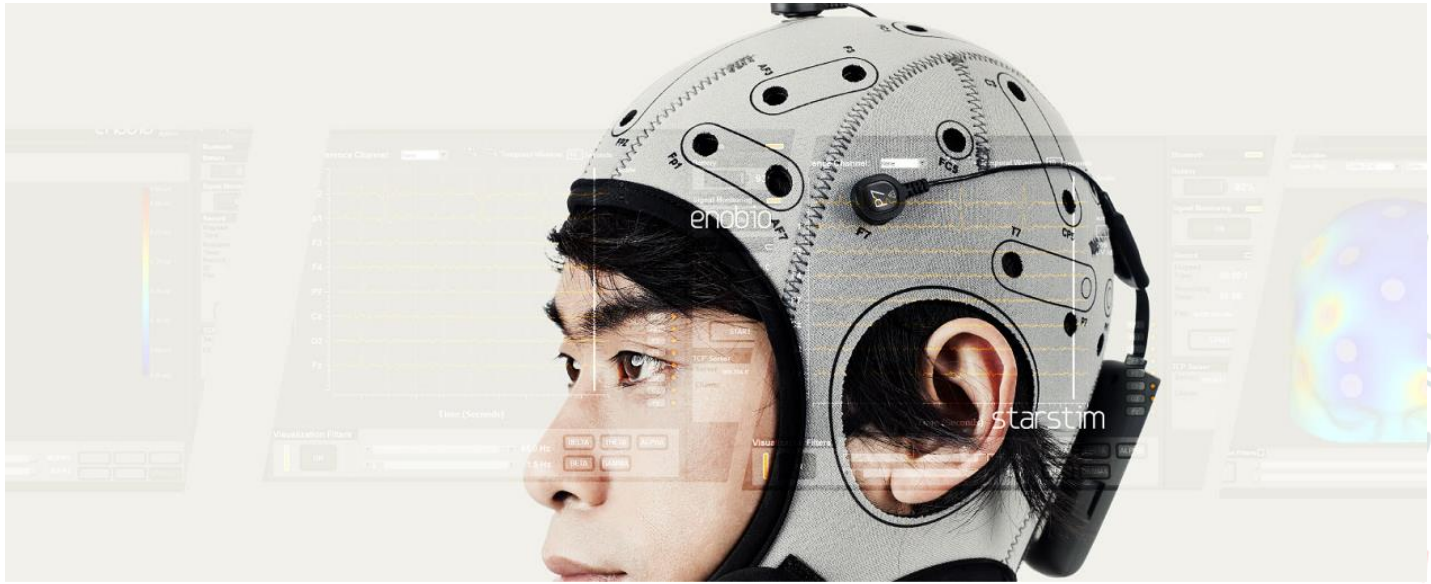
IOActive™

(In)security Aspects

- Authentication
  - The process of determining whether someone or something is who or what it is declared to be
  - Auth mechanism needed before
    - Read/Update an EEG stream/record
    - Start/Stop EEG
  - Auth mechanism between the acquisition device, EEG middleware and the endpoints
    - E.g.:
      EEG device <-> EGG Server
      <-> Drone/Prosthesis/Etc.

(In)security Aspects

- Authentication
  - Case: Neuroelectrics NIC
  - Same issue described previously (no auth to receive EEG data)



IOActive

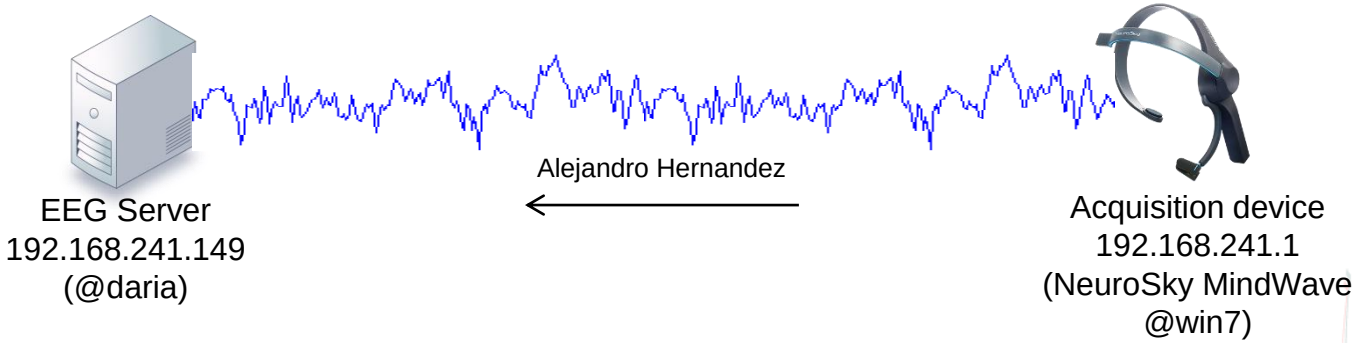
(In)security Aspects

- Authentication
  - **Demo: Patient's name is changed in a MITM attack before it reaches NeuroServer**
    - NeuroServer: EEG signal transceiver using TCP/IP and EDF format
    - Old and unmaintained
    - Still in use (mostly research)
    - Included in BrainBay

IOActive

(In)security Aspects

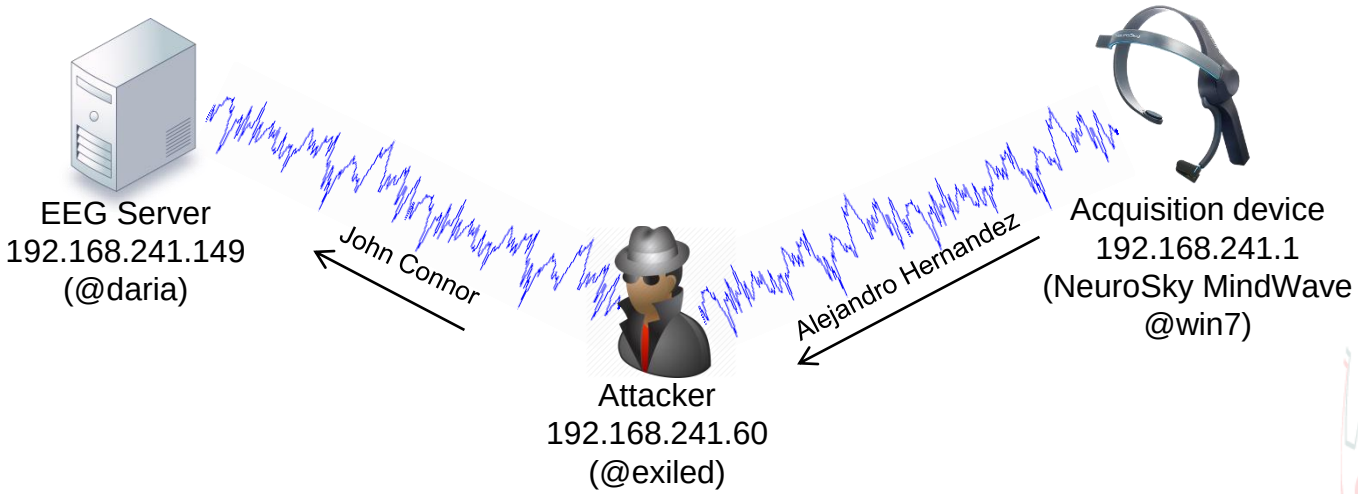
- Authentication
  - **Demo: Patient's name is changed in a MITM attack before it reaches NeuroServer**



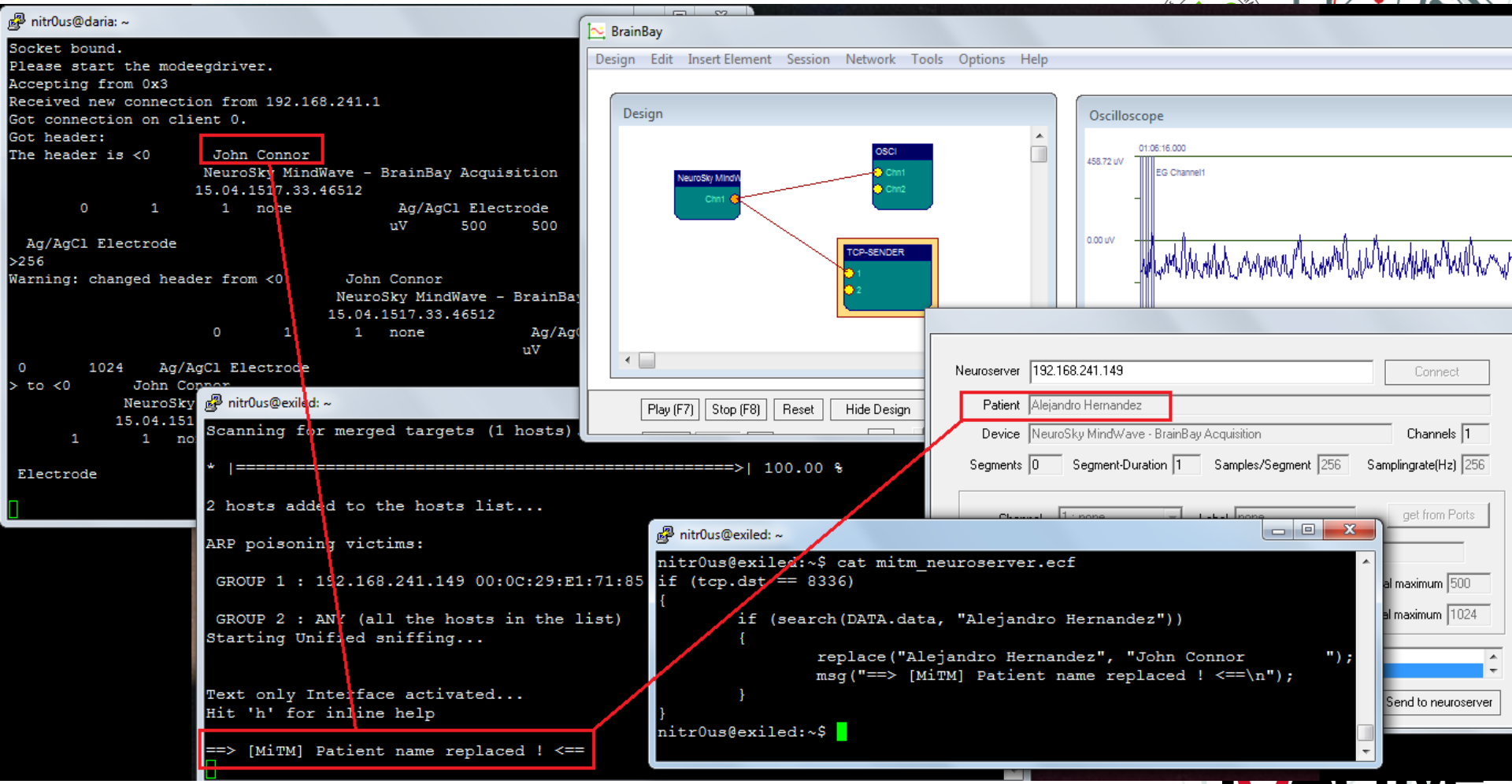
IOActive

(In)security Aspects

- Authentication
  - **Demo: Patient's name is changed in a MITM attack before it reaches NeuroServer**



IOActive™



(In)security Aspects

- Resilience
  - Ability to support or recover from adversity (Denial of Service attacks)

IOActive™

(In)security Aspects

- Resilience
  - 90's techniques still killing 21st century tech

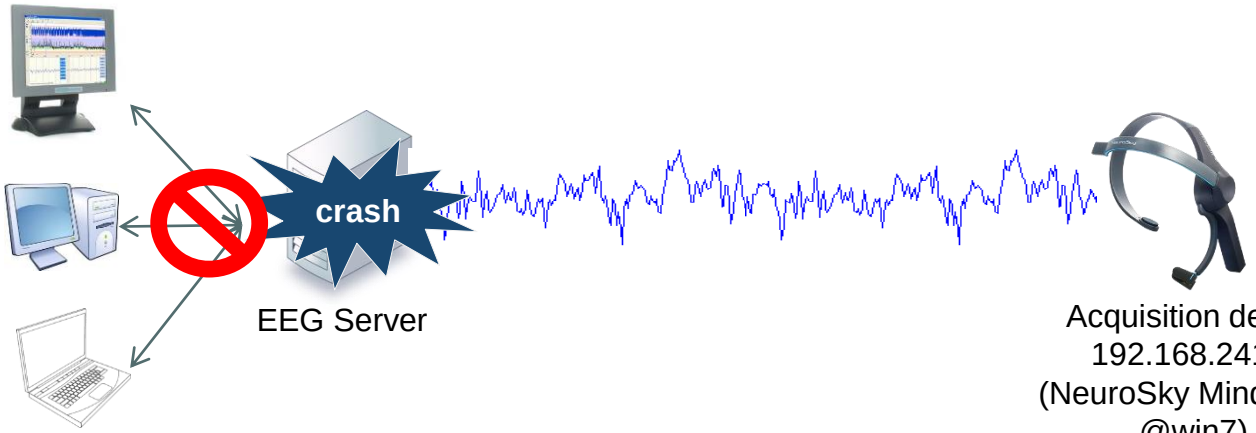
```
#define NCONNS 10000

for(k = 0; k < NCONNS; k++){
    sock = socket();
    connect();
    send("foo\n");
    sleep();
}
```


IOActive™

(In)security Aspects

- Resilience
  - Some EEG (TCP) servers
    - SPoF



EEG Server

Clients

Acquisition device
192.168.241.1
(NeuroSky MindWave
@win7)

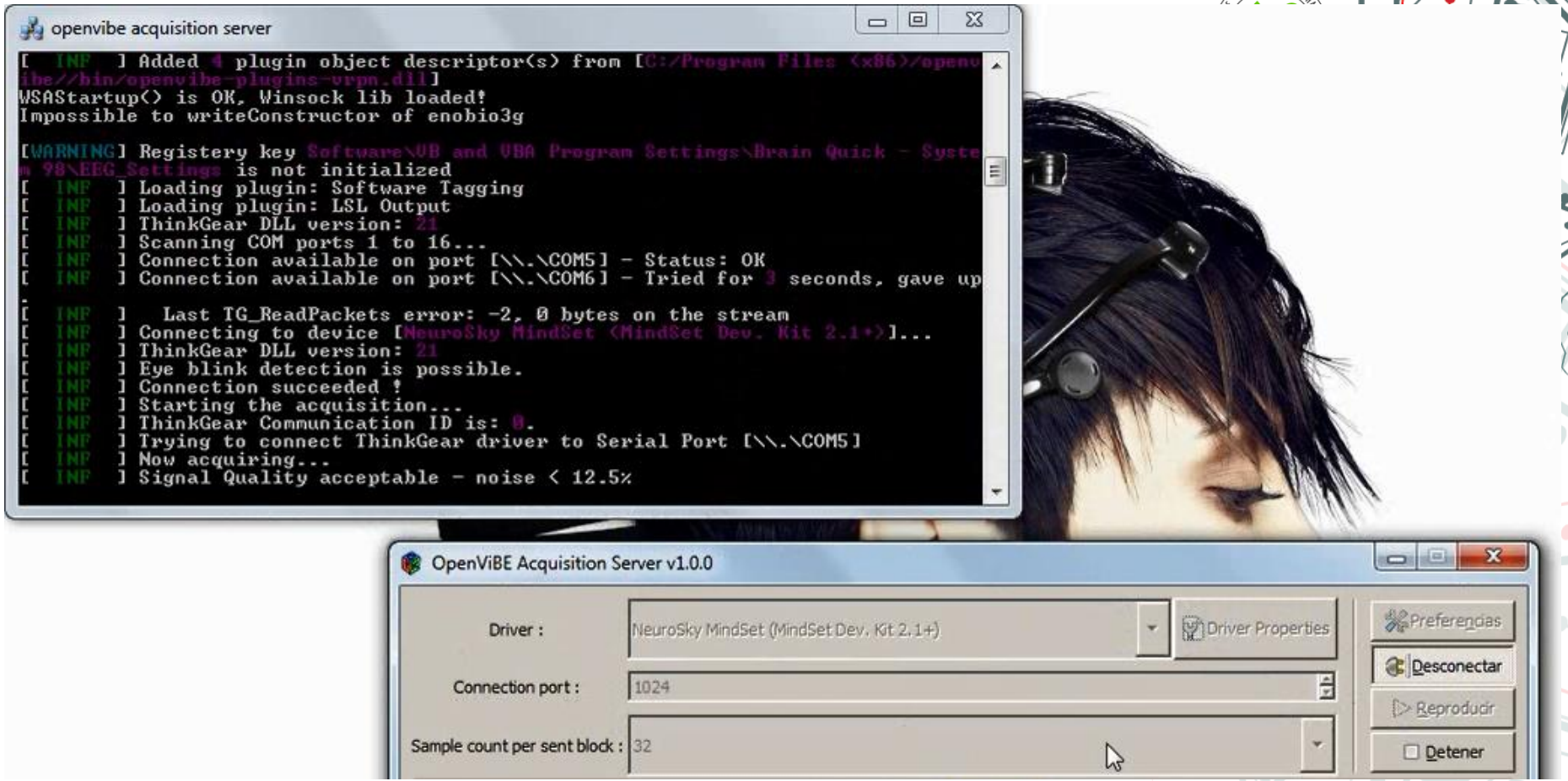
IOActive

(In)security Aspects

- Resilience
  - **Demo: OpenViBE Acquisition Server Remote DoS**

Software for Brain Computer Interfaces
and
Real Time Neurosciences

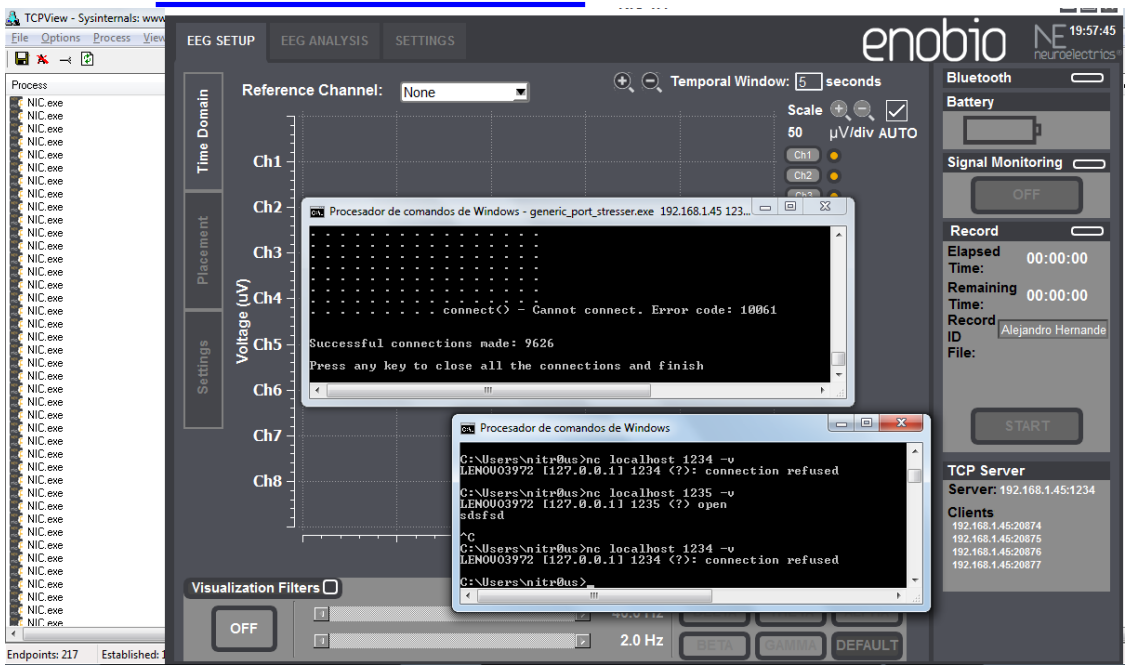
IOActive™



IOActive™

(In)security Aspects

- Resilience
  - **Demo: [Neuroelectrics NIC](#) TCP Server Remote DoS**



IOActive™

(In)security Aspects

- Resilience
  - **Demo: NeuroServer Daemon Multiple Remote DoS**

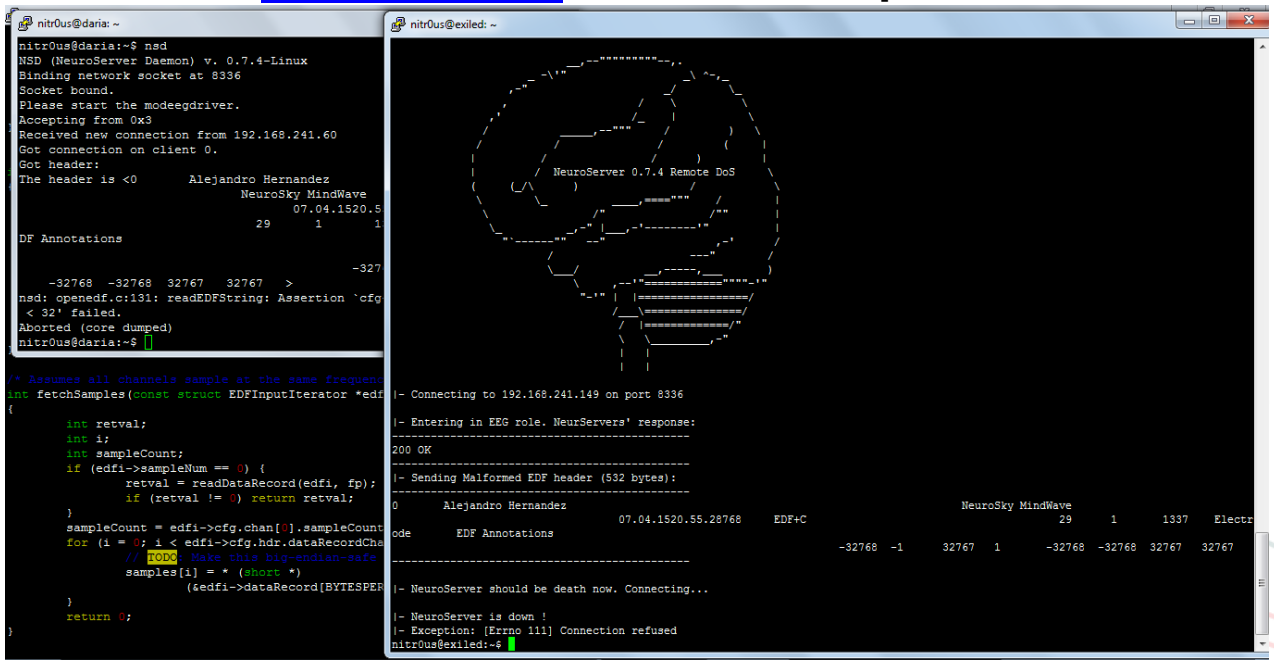
```
# Malformed EDF header
# Spec: http://www.edfplus.info/specs/edf.html
EDF  = "0       " # Version
EDF += "Alejandro Hernandez                                                    "
# Patient Identification
EDF += "NeuroSky MindWave                                                      "
# Recording Identification
EDF += "07.04.1520.55.28768     EDF+C                                  "
# Startdate of Recording
EDF += "29      " # Number of Data Records
EDF += "1       " # Duration of a Data Record in Seconds
EDF += "1337    " # Number of Signals. This value triggers the DoS: assert(cfg->hdr.dataRe
cordChannels < MAXCHANNELS);
EDF += "Electrode       EDF Annotations

                                  "      # Labels and other data per channel
EDF += "-32768  -1      32767   1       -32768  -32768  32767   32767   " # PhysiMin Physi
Max DigiMin DigiMax
```


IOActive™

(In)security Aspects

- Resilience
  - **Demo: NeuroServer Daemon Multiple Remote DoS**



(In)security Aspects

- Resilience
  - **Demo: NeuroServer Daemon Multiple Remote DoS**

```
#define MAXCLIENTS 16
...
struct Client clients[MAXCLIENTS];
...
int makeNewClient(sock_t fd) {
        int myIndex = clientCount;
        clientCount += 1;
        memset(&clients[myIndex], 0, sizeof(clients[0]));
        clients[myIndex].fd = fd;
        clients[myIndex].role = Unknown;
```

(In)security Aspects

- Resilience
  - **Demo: NeuroServer Daemon Multiple Remote DoS**

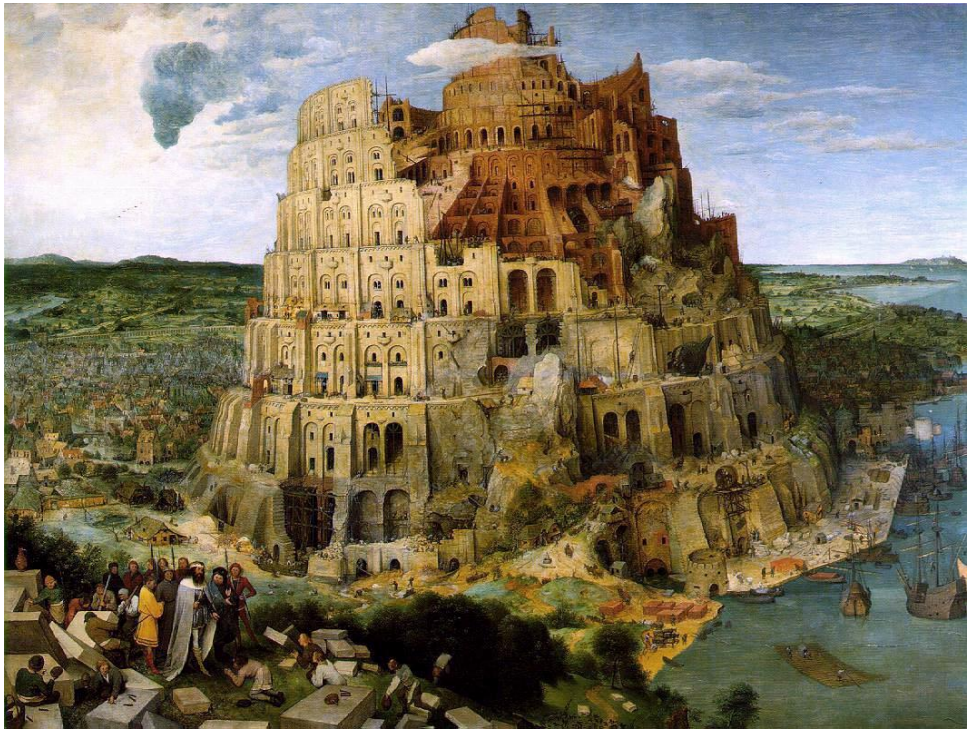
```
Program received signal SIGSEGV, Segmentation fault.
memset () at ../sysdeps/x86_64/memset.S:80
80      ../sysdeps/x86_64/memset.S: No such file or directory.
(gdb) bt
#0  memset () at ../sysdeps/x86_64/memset.S:80
#1  0x0000000000401d03 in makeNewClient (fd=92) at nsd.c:280
#2  0x000000000040235d in main () at nsd.c:363
(gdb) l nsd.c:280
275     }
276
277     int makeNewClient(sock_t fd) {
278             int myIndex = clientCount;
279             clientCount += 1;
280             memset(&clients[myIndex], 0, sizeof(clients[0]));
281             clients[myIndex].fd = fd;
282             clients[myIndex].role = Unknown;
283             clients[myIndex].markedForDeletion = 0;
284             clients[myIndex].linePos = 0;
(gdb) p clientCount
$7 = 89
(gdb) whatis clients
type = struct Client [16]
(gdb)
```

```
nitr0us@daria: ~/NeuroServer-0.7.4/src
nitr0us@daria:~/NeuroServer-0.7.4/src$ grep "struct Client" nsd.c
struct Client {
struct Client clients[MAXCLIENTS];
nitr0us@daria:~/NeuroServer-0.7.4/src$ grep MAXCLIENTS *.h
nsnet.h:#define MAXCLIENTS 16
nitr0us@daria:~/NeuroServer-0.7.4/src$
```


IOActive™

(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats



IOActive™

(In)security Aspects

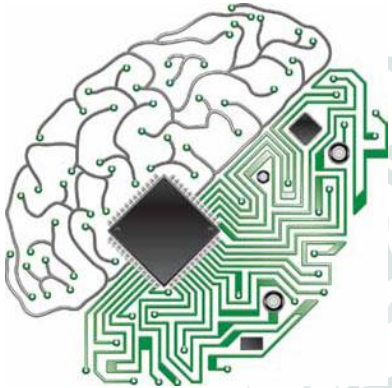
- The *"Tower of Babel"* of EEG File Formats
  - File Formats
    - *"A major difficulty with current commercial EEG systems is that they use **proprietary file formats**, which require dedicated reader systems."*
    - *"In some instances, different generation of a single vendor's system generate **incompatible file formats**"*
    - *"Some vendors of EEG systems do provide an option to save EEG data in a **standard format such as the European Data Format (EDF)** for biosignals… In addition, some vendors do not strictly adhere to the EDF specification, causing problems for some EDF reader programs."*

Krauss, G., Fisher, R., Kaplan, P. (September 1st, 2011). *The Johns Hopkins Atlas of Digital EEG: An Interactive Training Guide.* 2nd Edition. Johns Hopkins University Press.

IOActive

(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - File Formats
    - Many old specifications and implementations
      - EDF: 1992
      - EDF+: 2003
    - Many new specs and formats, though
    - Biomedical signals (time series)
      - https://en.wikipedia.org/wiki/List_of_file_formats#Biomedical_signals_.28time_series.29
    - List of *Scientific Data Formats*
      - http://pub.ist.ac.at/~schloegl/matlab/eeg/



IOActive™

(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - File Formats
    - Matrix of formats supported in different software / hardware
      - Took me weeeeeks…
        - » Brochures
        - » Manuals
        - » Specs

IOActive™

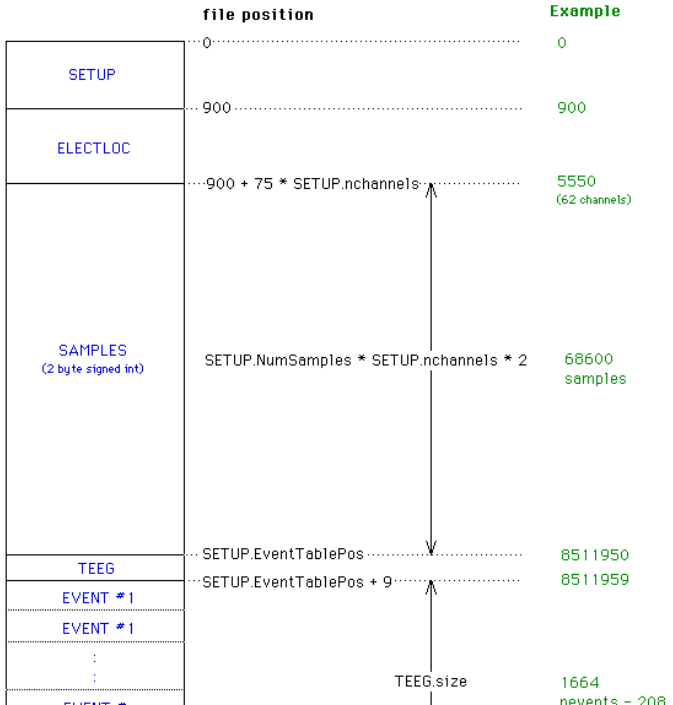
		File Formats											Networking
		EDF(+)	GDF	BDF	NeuroScan (CNT)	HL7	Persyst	Stellate	BrainVision	BCI2000	ASCII	Propietary	TCP/IP
Vendor	**Software**												
BioEra	BioEra	x											
CyberEvolution	BioExplorer												
Brain Products	BrainVision Recorder								x			x	x
Brain Products	BrainVision Analyzer								x		x	x	
Brain Products	BrainVision Rec								x			x	x
Neuro Electrics	Enobio	x									x		x
Neuro Electrics	NIC											x	x
Compumedics Neuro Scan	ProFusion EEG				x							x	
Compumedics Neuro Scan	Curry 7				x		x	x				x	
Persyst	Advanced Review (Insight II	x		x	x		x	x				x	
Grass Technologies	Twin EEG	x											
Grass Technologies	Twin Portal					x							
Grass Technologies	Twin Monitor 2												x
NeuroSky	Recorder (iOS)										x		
NeuroSky	ThinkGear Connector											x	x
BrainMaster	BrainAvatar	x		x								x	
Natus	Stellate Harmonie Viewer	x						x				x	
g.tek	g.BSanalyze	x			x						x	x	
g.tek	g.UDPinterface											x	x
OSG BVBA	BrainRT	x										x	
Pinnacle Technology	Sirenia Acquisition	x											
Pinnacle Technology	Sirenia Sleep	x											
Mitsar	WinEEG Basic											x	
Mitsar	WinEEG Advanced	x			x						x	x	
Mitsar	EEGStudio Aquisition	x									x	x	
Cadwell	Easy II EEG					x						x	x
Neurotraces	edfEdit	x											
Open Source	PhiTools PRANA	x			x			x	x		x		

IOActive™

(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - File Formats
    - Examples
      - Neuroscan

Data structure for Neuroscan continuous EEG files



IOActive™

(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - File Formats
    - Examples
      - EDF

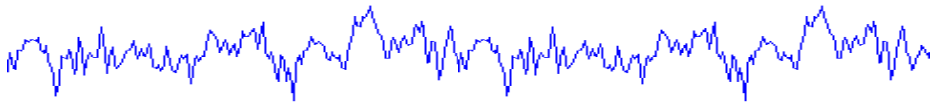
HEADER RECORD (we suggest to also adopt the 12 simple addit
8 ascii : version of this data format (0)
80 ascii : local patient identification (mind item 3 of the additional E
80 ascii : local recording identification (mind item 4 of the additiona
8 ascii : startdate of recording (dd.mm.yy) (mind item 2 of the addi
8 ascii : starttime of recording (hh.mm.ss)
8 ascii : number of bytes in header record
44 ascii : reserved
8 ascii : number of data records (-1 if unknown, obey item 10 of th
8 ascii : duration of a data record, in seconds
4 ascii : number of signals (ns) in data record
ns * 16 ascii : ns * label (e.g. EEG Fpz-Cz or Body temp) (mind ite
ns * 80 ascii : ns * transducer type (e.g. AgAgCl electrode)
ns * 8 ascii : ns * physical dimension (e.g. uV or degreeC)
ns * 8 ascii : ns * physical minimum (e.g. -500 or 34)
ns * 8 ascii : ns * physical maximum (e.g. 500 or 40)
ns * 8 ascii : ns * digital minimum (e.g. -2048)
ns * 8 ascii : ns * digital maximum (e.g. 2047)
ns * 80 ascii : ns * prefiltering (e.g. HP:0.1Hz LP:75Hz)
ns * 8 ascii : ns * nr of samples in each data record
ns * 32 ascii : ns * reserved

DATA RECORD
nr of samples[1] * integer : first signal in the data record
nr of samples[2] * integer : second signal
..
..
nr of samples[ns] * integer : last signal

IOActive™

(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - Parsing
    - Parsing is parsing !
      - Bytes in data structures
    - As any other file format
      - PDF, JPG, GIF, PE, ELF, etc. etc.
    - EEG data and its metadata



IOActive™

(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - Parsing
    - Memory corruption / Buffer overflows
    - Boundary checking problems (e.g. indexes in arrays)
    - Loops copying data more times than expected
    - Invalid memory derefs
    - Arithmetic calculations
    - Unexplored file formats
      - A new terrain to play
    - Attack surface reduced
      - Specialized formats, not mainstream

IOActive™

(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - Parsing
    - (Perhaps) developers with different backgrounds
      - Not fully aware of (in)secure programming

IOActive™

(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - Bug hunting
    - (In)secure programming
      - *(haven't corroborated if are real security vulnerabilities)*

```
$ egrep -nr "strcpy|sprintf" ~/labstreaminglayer/LSL/ | wc -l
63
$ egrep -nr "memcpy|memset|bzero" ~/labstreaminglayer/LSL/ | wc -l
519
$ egrep -nr "strcpy|sprintf" ~/biosig4c++-1.6.4/ | wc -l
361
$ egrep -nr "memcpy|memset|bzero" ~/biosig4c++-1.6.4/ | wc -l
254
$ egrep -nr "strcpy|sprintf" ~/NeuroServer-0.7.4/src/ | wc -l
47
$ egrep -nr "memcpy|memset|bzero" ~/NeuroServer-0.7.4/src/ | wc -l
20
```

(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - Bug hunting
    - (In)secure programming
      - *(haven't corroborated if are real security vulnerabilities)*

```
$ flawfinder --quiet --minlevel=3 --falsepositive ~/labstreaminglayer/LSL/
...
ANALYSIS SUMMARY:

Hits = 329
Lines analyzed = 1115455 in approximately 47.91 seconds (23281
lines/second)
Physical Source Lines of Code (SLOC) = 958265
Hits@level = [0]   0 [1]   0 [2]   0 [3] 306 [4]  20 [5]   3
```


IOActive™

(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - Bug hunting
    - (In)secure programming
      - *(haven't corroborated if are real security vulnerabilities)*

```
$ flawfinder --quiet --minlevel=3 --falsepositive ~/biosig4c++-1.6.4/
...
ANALYSIS SUMMARY:

Hits = 117
Lines analyzed = 95048 in approximately 3.63 seconds (26188 lines/second)
Physical Source Lines of Code (SLOC) = 71225
Hits@level = [0]   0 [1]   0 [2]   0 [3]   4 [4] 113 [5]   0
```

(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - Bug hunting
    - (In)secure programming
      - *(haven't corroborated if are real security vulnerabilities)*

```
$ flawfinder --quiet --minlevel=3 --falsepositive ~/NeuroServer-0.7.4/src/
...
ANALYSIS SUMMARY:

Hits = 17
Lines analyzed = 2938 in approximately 0.08 seconds (35282 lines/second)
Physical Source Lines of Code (SLOC) = 2481
Hits@level = [0]   0 [1]   0 [2]   0 [3]   0 [4]  17 [5]   0
```

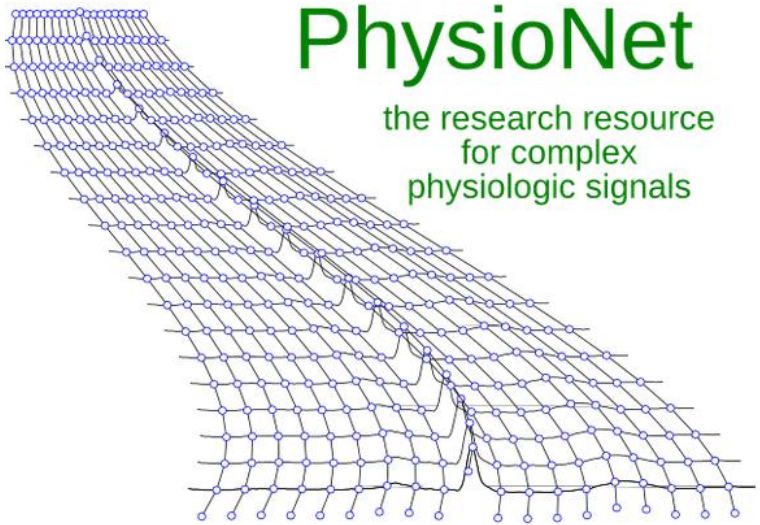
(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - Bug hunting
    - Fuzzing
      - Only the EDF format was approached
        - » Most supported amongst EEG software/hardware
      - Trivial fuzzing
        - » mangle.c
          by Ilja van Sprundel
        - » Microsoft MiniFuzz

IOActive™

(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - Bug hunting
    - Fuzzing
      - Sample EDF recordings
        - » My own brain waves in EDF
        - » PhysioNet



PhysioNet offers free web access to large collections of recorded physiologic signals (PhysioBank) and related open-source software (PhysioToolkit).

IOActive

(In)security Aspects

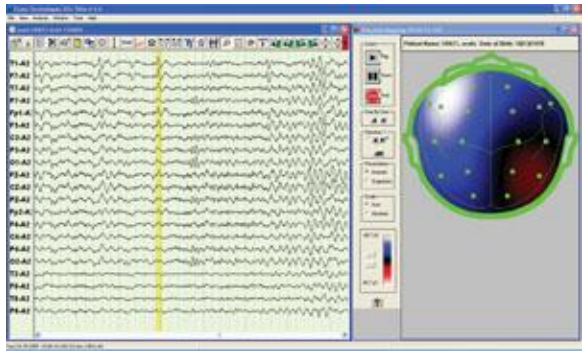
- The *"Tower of Babel"* of EEG File Formats

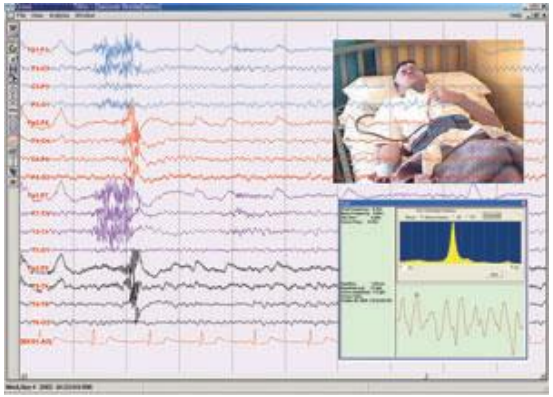
Sample	Fuzzer	Header Bytes	% Fuzzed	Output Folder	Test Cases Created
neurosky_mindwave_Alejandro_10apr15_12secs_2channels.edf	mangle	236	33%	mangle_33_236_1	100
neurosky_mindwave_Alejandro_10apr15_40secs_13channel.edf	mangle	236	33%	mangle_33_236_2	100
eegmmidb_S001R01.edf	mangle	236	33%	mangle_33_236_3	100
sleep-edfx_SC4112E0-PSG.edf	mangle	236	33%	mangle_33_236_4	50
neurosky_mindwave_Alejandro_10apr15_12secs_2channels.edf	mangle	256	33%	mangle_33_256_1	100
neurosky_mindwave_Alejandro_10apr15_40secs_13channel.edf	mangle	256	33%	mangle_33_256_2	100
eegmmidb_S001R01.edf	mangle	256	33%	mangle_33_256_3	100
sleep-edfx_SC4112E0-PSG.edf	mangle	256	33%	mangle_33_256_4	50
neurosky_mindwave_Alejandro_10apr15_12secs_2channels.edf	mangle	768	20%	mangle_33_768_1	100
neurosky_mindwave_Alejandro_10apr15_40secs_13channel.edf	mangle	768	20%	mangle_33_768_2	100
eegmmidb_S001R01.edf	mangle	768	20%	mangle_33_768_3	100
sleep-edfx_SC4112E0-PSG.edf	mangle	768	20%	mangle_33_768_4	50
neurosky_mindwave_Alejandro_10apr15_12secs_2channels.edf	MS SDL MiniFuzz	x	10%	x	x
neurosky_mindwave_Alejandro_10apr15_40secs_13channel.edf	MS SDL MiniFuzz	x	10%	x	x
eegmmidb_S001R01.edf	MS SDL MiniFuzz	x	10%	x	x
sleep-edfx_SC4112E0-PSG.edf	MS SDL MiniFuzz	x	10%	x	x
neurosky_mindwave_Alejandro_10apr15_12secs_2channels.edf	MS SDL MiniFuzz	x	5%	x	x
neurosky_mindwave_Alejandro_10apr15_40secs_13channel.edf	MS SDL MiniFuzz	x	5%	x	x
eegmmidb_S001R01.edf	MS SDL MiniFuzz	x	5%	x	x
sleep-edfx_SC4112E0-PSG.edf	MS SDL MiniFuzz	x	5%	x	x

IOActive™

(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - Bug hunting
    - **Demos: Flaws discovered in well-known EEG analysis software**
      - Unhandled exceptions / Seg faults
      - Potential memory corruption bugs
      - Still in the bug discovery phase



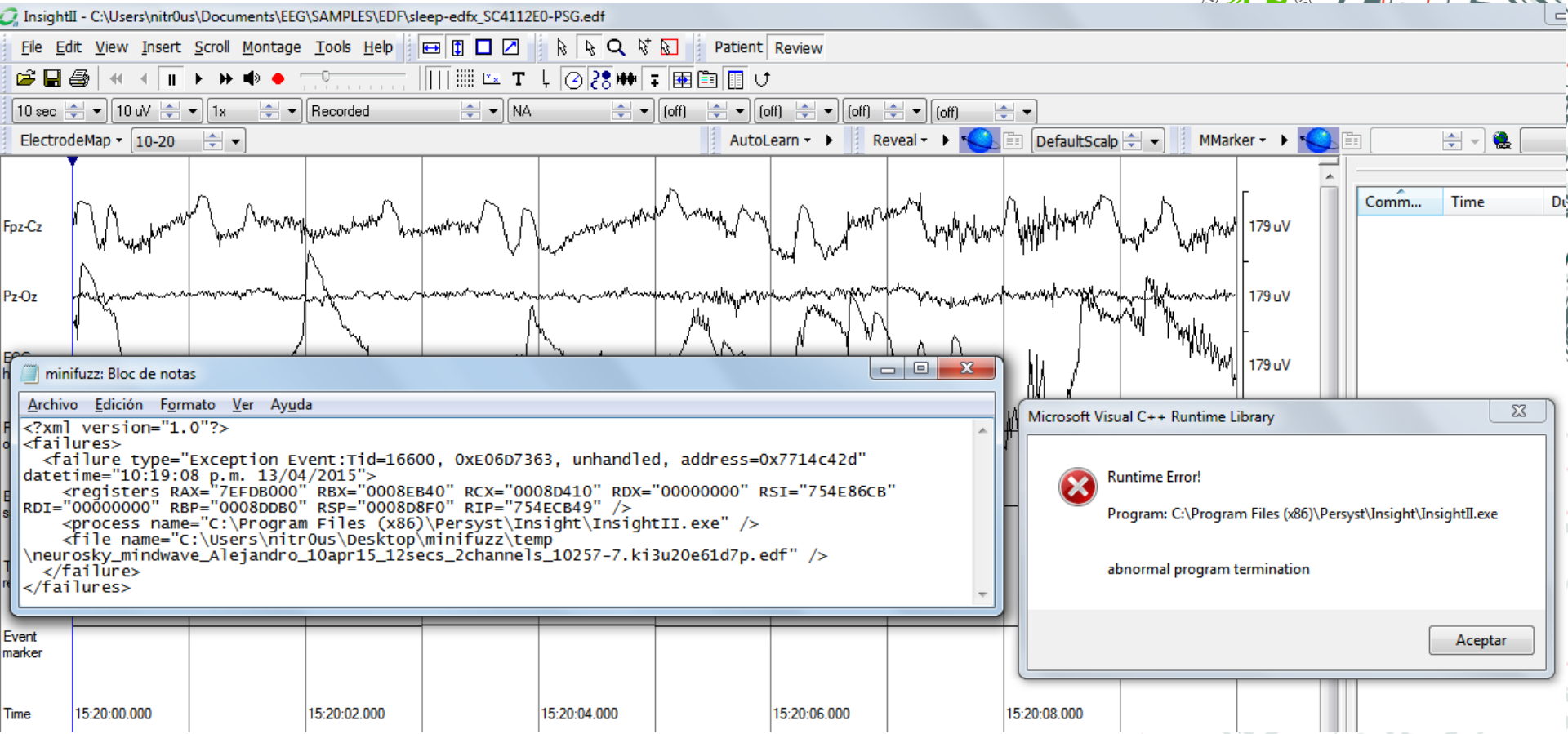


IOActive™

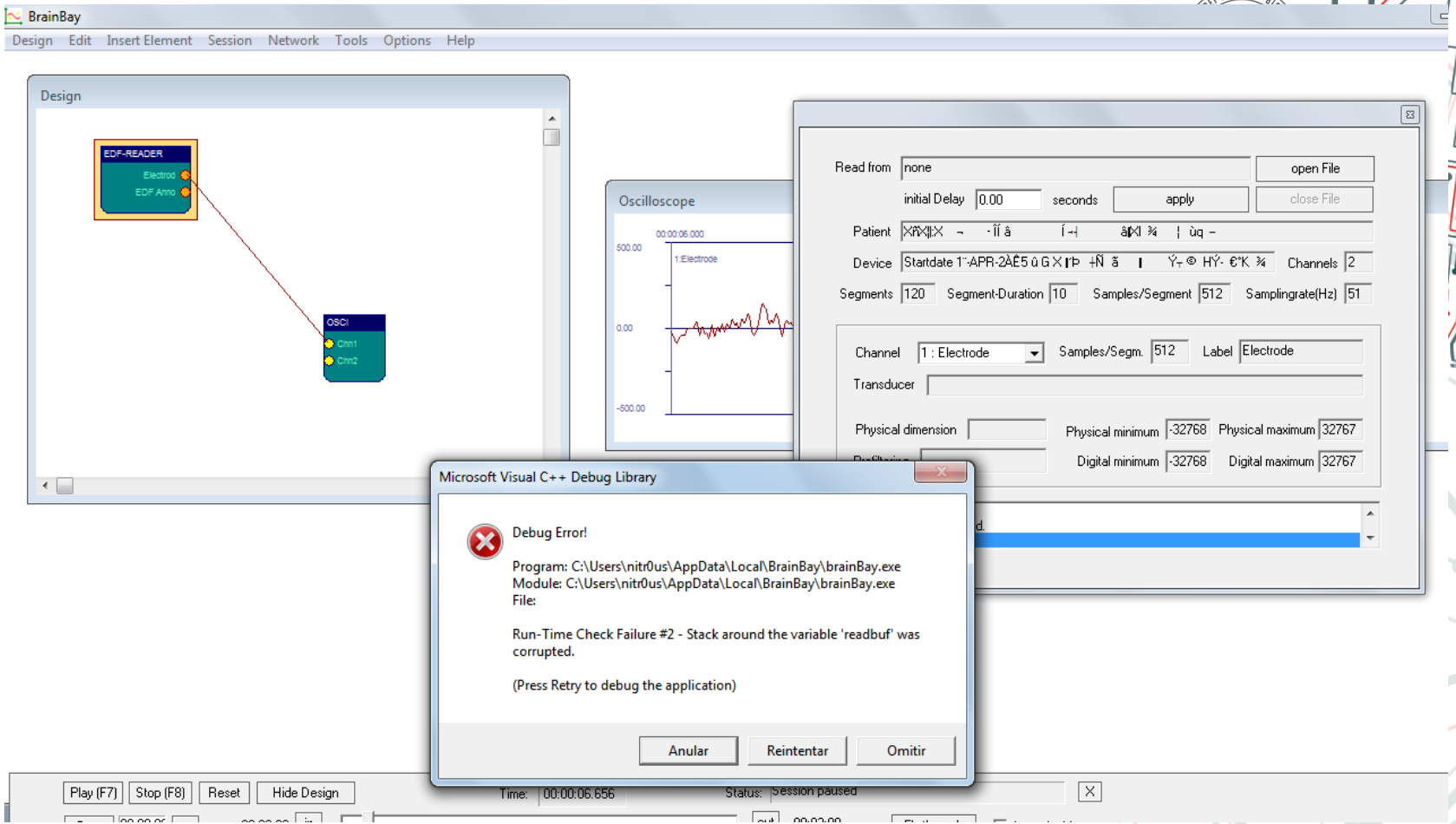
(In)security Aspects

- The *"Tower of Babel"* of EEG File Formats
  - Bug hunting
    - **Demos: Flaws discovered in well-known EEG analysis software**
      - Persyst Advanced Review (Insight II)
      - Natus Stellate Harmonie Viewer
      - BrainBay
      - SigViewer (uses libbiosig)

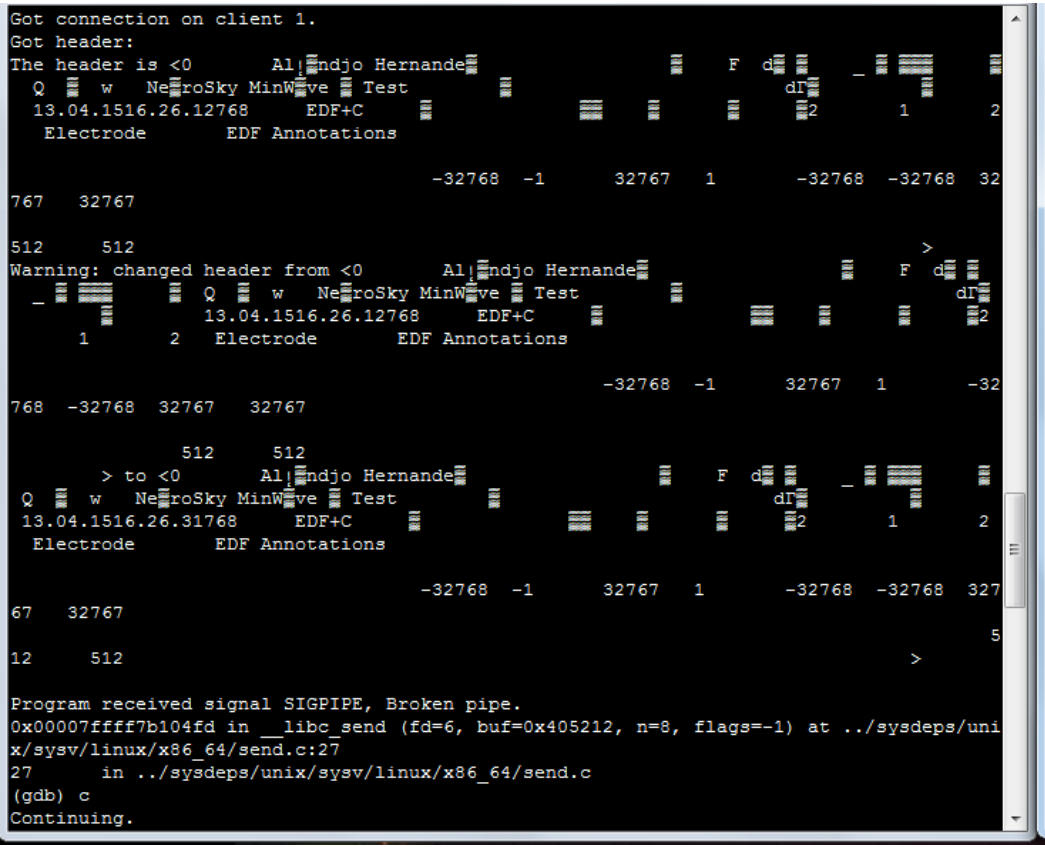
IOActive™

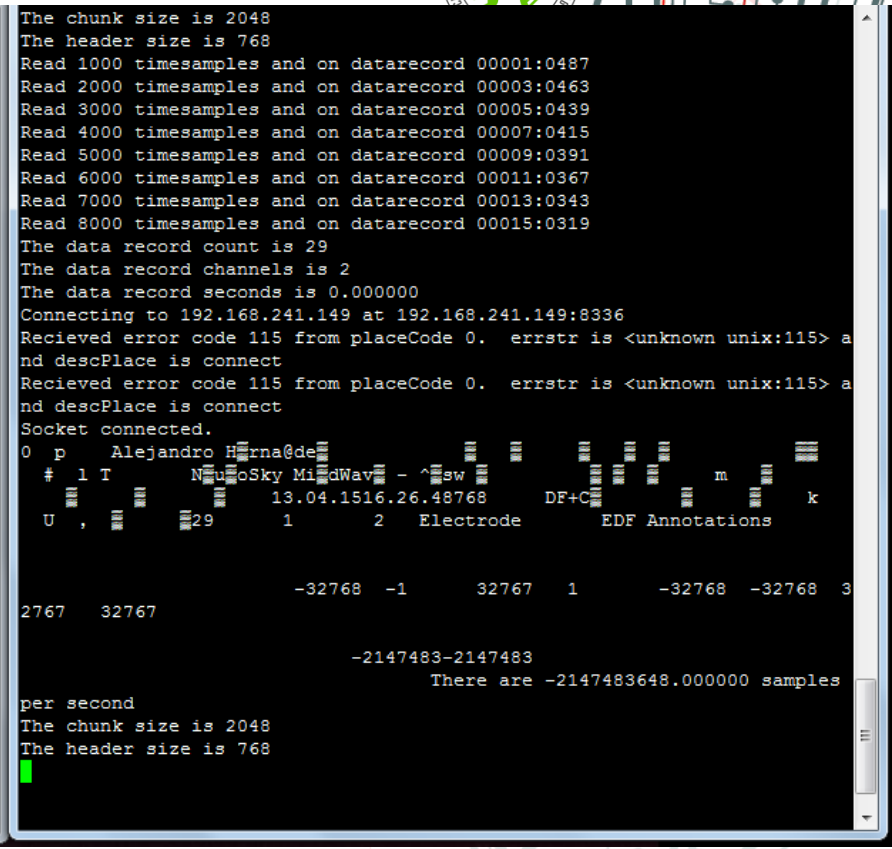


IOActive™

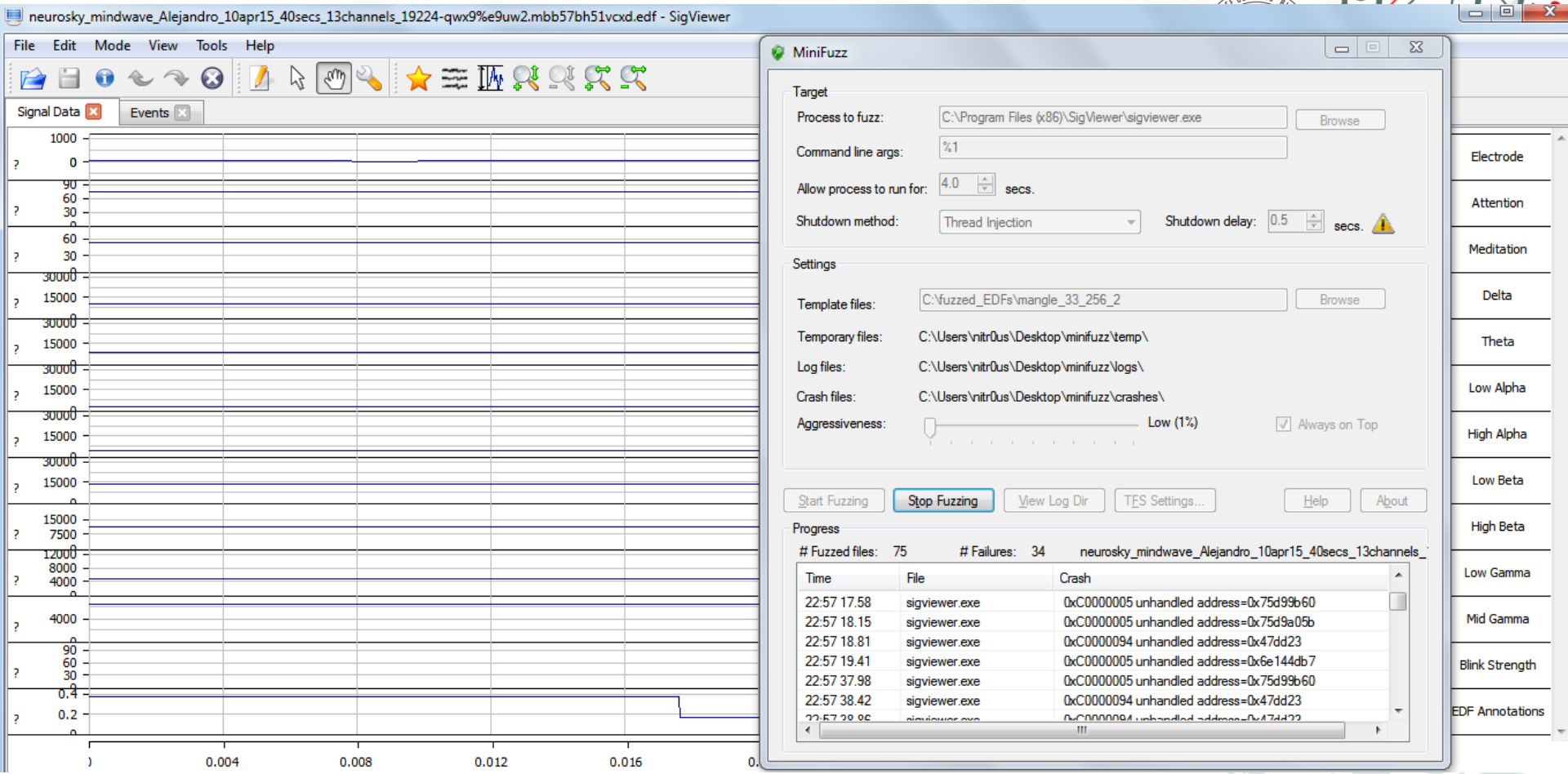


IOActive™





IOActive™



IOActive™

(In)security Aspects

- Misc
  - Brain waves in the air
    - Bluetooth / WiFi

Home ▶ Neurology Diagnostics ▶ Ambulatory EEG Solution ▶ Wireless Ambulatory EEG ▶ Siesta802 EEG

IOActive™

(In)security Aspects

- Misc
  - Brain waves in the air
    - Bluetooth / WiFi

Radio LAN

TCP/IP wireless
2.4 GHz, 802.11b compliant
Maximum Range: 30 to 50 meters in hospital environment (RF transmission is affected by environmental and architectural factors)
Communication via 802.11 access points
Up to four Siesta units may communicate via one access point
Network consultation may be required to support more than four Siesta's in a facility
Wireless Security Options: WEP (40 and 128 bit), WPA1-PSK, WPA2-PSK.

IOActive

(In)security Aspects

- Misc
  - Brain waves in the air
    - Bluetooth / WiFi

The Siesta is a revolutionary wireless data recorder.

This software programmable amplifier/data acquisition system has low noise, high gain and high input impedance features. It provides state of the art amplification and digitization of physiological signals from electrodes, sensors and transducers. Additionally, Siesta features real-time data transmission via an 802.11 compatible wireless radio link to the host computer or network. The Siesta offers up to 52 total available signals. Advanced processor technology allows sampling rates up to 1024 Hz per channel with a 16 bit vertical A to D resolution. Siesta's integrated radio-linked IP protocol allows simple interfacing to most current computers.

This technology enables any single computer, or all computers on a LAN, to easily monitor multiple Siesta recorders simultaneously on the network.

IOActive™

(In)security Aspects

- Misc
  - Brain waves in the air
    - Bluetooth / WiFi
      - Jamming

IOActive™

(In)security Aspects

- Misc
  - Brain waves in the air
    - Bluetooth
      - Fuzz the stack (BSS – Bluetooth Stack Smasher)

IOActive

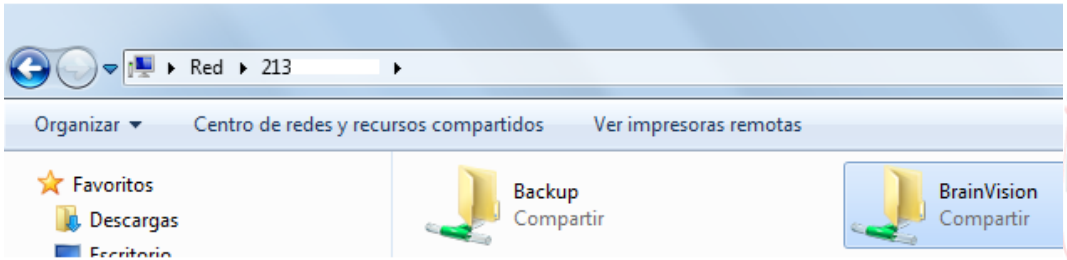
(In)security Aspects

- Misc
  - Internet accessible
    - SHODAN + NetBIOS shares

f3.cuni.cz
Charles University
Added on 2015-03-23 03:08:42 GMT
Czech Republic, Prague
Details

```
NetBIOS Response
Servername: EEG-BRAINVISION
MAC: d4:3d:7e:50:2d:5c

Names:
EEG-BRAINVISION <0x0>
PCP             <0x0>
AladinHaspV01.2 <0x30>
EEG-BRAINVISION <0x20>
```



IOActive

(In)security Aspects

- Misc
  - Internet accessible
    - SHODAN + NetBIOS shares

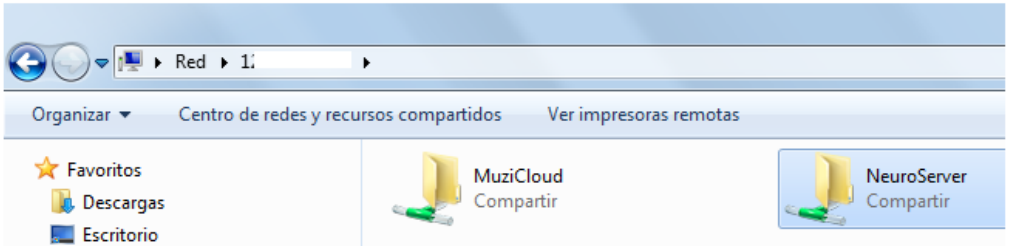
t.net.br
Global Village Telecom
Added on 2015-03-24 06:57:40 GMT
Brazil, Gramado
Details

NetBIOS Response
Servername: NEUROSERVER
MAC: 00:08:54:45:4b:c2

Names:
NEUROSERVER <0x0>
SNNMC <0x0>
NEUROSERVER <0x20>
SNNMC <0x1e>
SNNMC <0x1d>
__MSBROWSE__ <0x1>

University of Washington
Added on 2015-03-22 19:50:46 GMT
United States, Seattle
Details

Sharename	Type	Comment
MuziCloud	Disk	
QIN	Disk	
NeuroServer	Disk	
IPC$	IPC	IPC Servi



IOActive

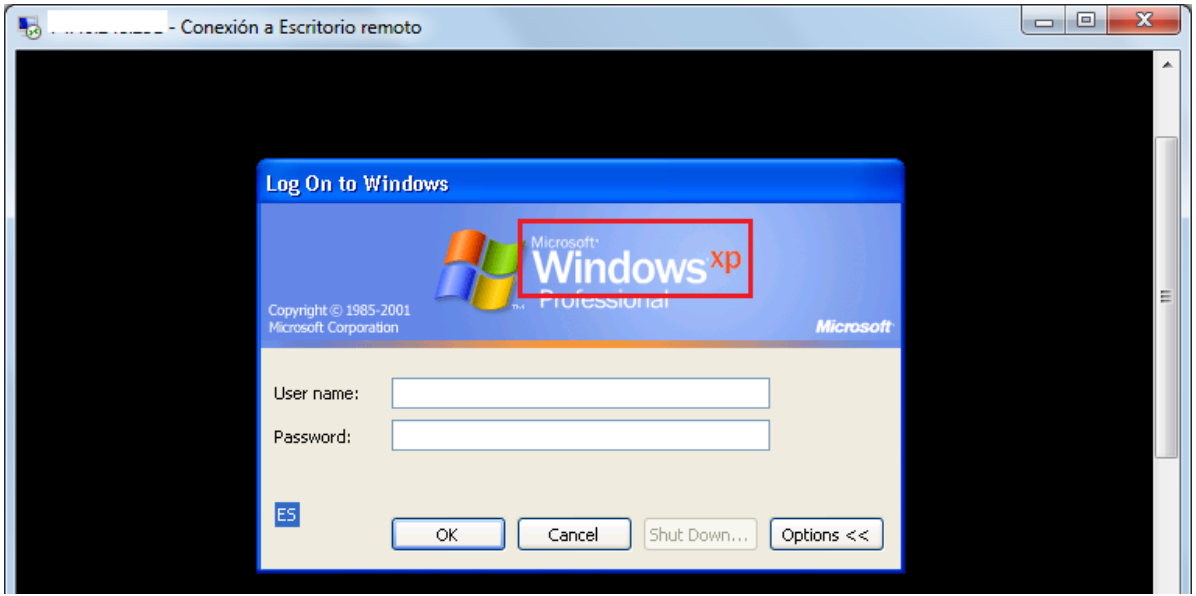
(In)security Aspects

- Misc
  - Internet accessible
    - SHODAN + RDP

IOActive™

(In)security Aspects

- Misc
  - Internet accessible
    - SHODAN + RDP



IOActive

(In)security Aspects

- Misc

On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces

Ivan Martinovic*, Doug Davies†, Mario Frank†, Daniele Perito†, Tomas Ros‡, Dawn Song†
*University of Oxford** *UC Berkeley†* *University of Geneva‡*

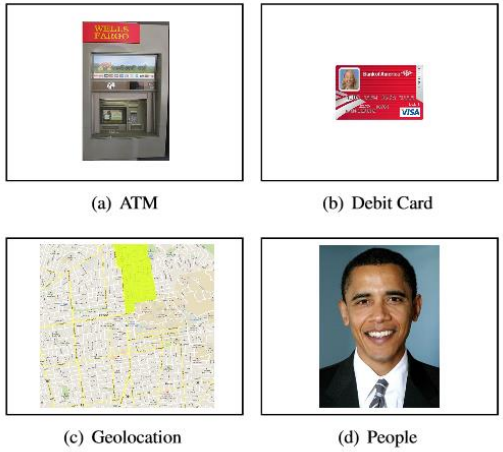


Figure 5: Layout of four of the experiments: Bank ATMs, Debit Cards, Geolocation and People.

https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf

IOActive

(In)security Aspects

- Misc
  - *"We use inexpensive electroencephalography (EEG) based BCI devices to test the feasibility of simple, yet effective, attacks.* ***The captured EEG signal could reveal the user's private information about, e.g., bank cards, PIN numbers, area of living, the knowledge of the known persons****. This is the first attempt to study the security implications of consumer grade BCI devices. We show that* ***the entropy of the private information is decreased on the average by approximately 15 % - 40 % compared to random guessing attacks.****"*

https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf

IOActive™

Regulatory Compliance / Best Practices for digital EEG

- Privacy

Medical devices have serious risks beyond data protection failures

Though HIPAA certainly seems to have made the healthcare community stand up and take notice of information security, it may have had an unintended side effect. You see, HIPAA is all about keeping private medical records private. You remember that form with

http://searchsecurity.techtarget.com/opinion/McGraw-asks-whos-in-charge-of-medical-device-security

IOActive

Regulatory Compliance / Best Practices for digital EEG

- Privacy

Hospitals have no CSO and too little security kung fu

There is another point that came up during the ISPAB panel that relates directly to medical device security. It boils down to some simple questions. Who is in charge of information security at most hospitals? And what kinds of expertise do these people generally have?

http://searchsecurity.techtarget.com/opinion/McGraw-asks-whos-in-charge-of-medical-device-security

IOActive™

Regulatory Compliance / Best Practices for digital EEG

- Privacy

Under the pressure of Sarbanes-Oxley and other financial regulations, CISOs in financial services grew up quickly (actually, in most cases the early CISOs were simply swapped out). The same sort of thing needs to happen to the CISO role in hospitals so that attention turns from patient record protection and network security to patient safety concerns and building security in.

http://searchsecurity.techtarget.com/opinion/McGraw-asks-whos-in-charge-of-medical-device-security

IOActive™

Regulatory Compliance / Best Practices for digital EEG

- Privacy

FDA and the Cybersecurity Community: Working Together to Protect the Public Health

Posted on **October 8, 2014** by **FDA Voice**

By: Suzanne Schwartz, M.D., M.B.A.

Medical devices that contain computer hardware or software or that connect to computer networks are subject to the same types of cyber vulnerabilities as consumer devices. The consequences of medical device breaches include impairing patient safety, care, and privacy. And as in the case of consumer devices, strengthening the cybersecurity of medical devices requires collaboration and coordination among many stakeholders, as well as a shared sense of responsibility for reducing the cybersecurity vulnerabilities.

http://blogs.fda.gov/fdavoice/index.php/tag/collaborative-approaches-for-medical-device-and-healthcare-cybersecurity/

IOActive™

Regulatory Compliance / Best Practices for digital EEG

- Guidelines by the ACNS (American Clinical Neurophysiology Society)

Practice

Guidelines

- Introduction
- Electroencephalography
- Evoked Potentials
- Neurophysiologic Intraoperative Monitoring
- Long Term EEG Monitoring for Epilepsy
- Long Term EEG Monitoring in Neonates
- Continuous EEG Monitoring in Critical Care
- Quantitative EEG
- Technical Standards for Digital EEG Formats
- Neurodiagnostic Personnel
- Magnetoencephalography

Guidelines

Clinical Neurophysiology Topic

Title	Guideline	#	Date Revised
Introduction			
	Introduction to the 2006 Revisions		
Electroencephalography			
	Minimum Technical Requirements for Performing Clinical EEG	1	2/10/06
	Minimum Technical Standards for Pediatric EEG	2	2/10/06
	Minimum Technical Standards for EEG Recording in Suspected Cerebral Death	3	2/10/06
	Standards of Practice in Clinical EEG	4	2/10/06
	Guidelines for Standard Electrode Position Nomenclature	5	2/10/06
	A Proposal for Standard Montages to Be Used in Clinical EEG	6	2/10/06
	Guidelines for Writing EEG Reports	7	2/10/06
	Guidelines for Recording Clinical EEG on Digital Media	8	2/10/06

IOActive

Regulatory Compliance / Best Practices for digital EEG

- Guidelines by the ACNS (American Clinical Neurophysiology Society)
  - (2008) *Standard for Transferring Digital Neurophysiological Data Between Independent Computer Systems*
  - (2006) *Guideline 8: Guidelines for Recording Clinical EEG on Digital Media*
    - Magnetic storage and CD-ROMs
  - *Clinical Practice Guideline 1: Recording and Analysis of Spontaneous Cerebral Activity*
    - *"Long-term storage should be of sufficient capacity to handle the projected annual volume of data with appropriate information security, backup, and data recovery."*

IOActive

Conclusion / Further Research

- We need more security *"in mind"* for brain signals treatment
- Efforts in file format standardization
- More secure programming practices
- Create or update the guidelines / best practices
- A new terrain to play: Networking + parsing

IOActive™

Conclusion / Further Research

- Test your medical devices and software

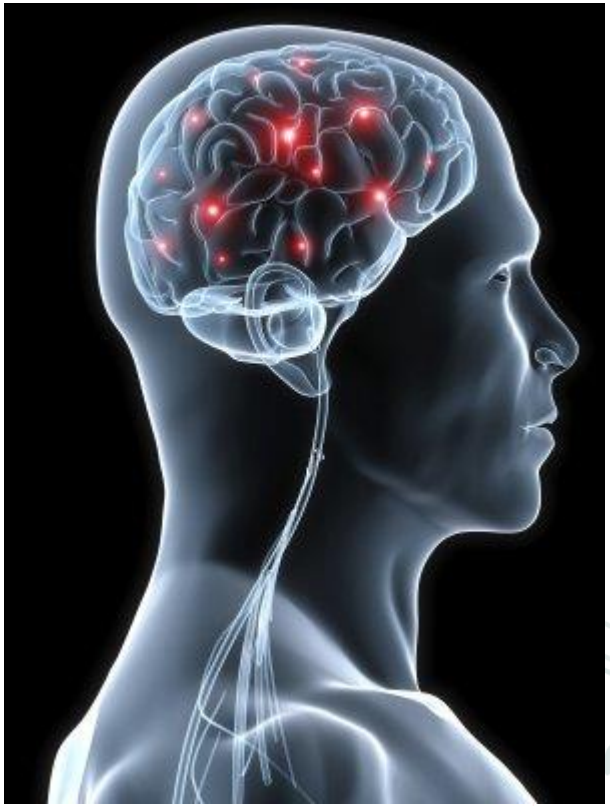
- Brain signals exposed on the Internet?
  - Zmap scannings of ports used by known EEG acquisition software / hardware (who is in? ☺)

- By now, security could be improved by implementing controls surrounding the EEG tech
  - SSL tunnels
  - Like in ICS/SCADA networks… Bio-signals firewalls / IPSs with DPI in L7? In the ~~near~~ future perhaps?

IOActive™

Thanks !

Alejandro Hernández
http://www.brainoverflow.org
http://chatsubo-labs.blogspot.mx
@nitr0usmx



IOActive