Brains Can be Hacked. Why Should You Care?

Tamara Bonaci
Department of Electrical Engineering
University of Washington
The Era of Devices Attached to Us

New and upcoming products make brain malware possible!
Hackers backdoor the human brain, successfully extract sensitive data

By Sebastian Anthony on August 17, 2012 at 1:29 pm  |  95 Comments

Our Brains Will Be Hacked, Tracked and Data-Mined

Written by JORDAN PEARSON | June 3, 2014 // 12:22 PM EST

How Hackers Could Get Inside Your Head With ‘Brain Malware’

WRITTEN BY VICTORIA TURK (/AUTHOR/VICTORIATURK) | August 3, 2016 // 07:50 AM EST
What is Brain Spyware?

Any malicious application that extracts private information about users from their neural signals [Martinovic et al., 2012]
Why Does Brain Spyware Work?

ENGINEERING PERSPECTIVE

BRAIN-COMPUTER INTERFACE

SIGNAL ACQUISITION

Digitized signal

Feature extraction

Classification algorithm

Neuroprosthesis control

Neural spelling

Neurogame control

Neuroprosthesis

P300 Speller

Neurogame

Sensory feedback

Neural signals

SIGNAL PROCESSING
Why Does Brain Spyware Work?

ENGINEERING PERSPECTIVE

BRAIN-COMPUTER INTERFACE

SIGNAL ACQUISITION

Digitized signal

Neural signals

SIGNAL PROCESSING

Feature extraction

Classification algorithm

Malicious feature extraction

Malicious classification algorithm

Extracted private information

Neuroprosthesis control

Neural spelling

Neurogame control

Neuroprosthesis

P300 Speller

Neurogame

Sensory feedback

Malicious sensory feedback

Malicious BCI application

1/31/17
Why Does Brain Spyware Work?

NEURO-SCIENTIFIC PERSPECTIVE

Event Related Potentials (ERPs) - responses associated with specific sensory, cognitive and motor events
Subliminal Brain Spyware?
“What we do not see and what we do not know can hurt us”

Brannon, 1994
Subliminal Stimulation

- Process of affecting people with stimuli of which they are not aware
How Feasible is Subliminal Brain Spyware?

**Approach:** Experimental analysis with human subjects using specially developed BCI-game, *Flappy whale*
How Feasible is Subliminal Brain Spyware?

- During the game:
  - 5 different stimuli presented on the screen for 7 ms
  - Each stimulus repeated 10 times
  - Users’ EEG signals recorded using 7 electrodes
Data Preparation and Analysis
Data Preparation and Analysis

EEG signal [scaled μV]

Time [ms]
Data Preparation and Analysis

![Graph showing EEG signals and averaged channels over time](image)

**EEG Signal (scaled µV)**

-2000 to 2000

**Time (ms)**

-200 to 600

**Averaged Channels**
Feasibility of Subliminal Attacks

Training data

Testing data

Time sync EEG & stimuli; epoch data

Feature extraction (Principal Component Analysis)

SVM classifier for private data extraction

Comparison with users’ self-reported post-game surveys

Subliminal information extraction result

Flappy Whale, BCI-controlled game
Feasibility of Subliminal Attacks

- Target stimulus recognized
- Target stimulus reported by a subject

![Graph showing target stimulus recognition and report across subjects.](image)
Mitigation - BCI Anonymizer

_Idea:_ Neural signals should be treated as a user’s personally identifiable information (PII)

[Picture credit: NeuroFocus]

vs.

[Picture credit: The Verge]
Brains Can be Hacked. What Can We Do?

Understand system

Develop non-technical approaches

Develop technical approaches

Understand threats
Brains Can be Hacked. What Can We Do?

- Understand system
- Understand threats
- Develop technical approaches
- Develop non-technical approaches
Acknowledgement

• This project is a collaborative work with:
  • Professors: Ryan Calo, Howard Jay Chizeck, and Tadayoshi Kohno
  • Doctors: Jeffrey Herron, Charlie Matlack, and Rad Roberts
  • Graduate students: Tim Brown, Brady Houston, Tyler Libey, Brian Mogen, Patrick Moore, Katherine Pratt, and Margaret Thompson
  • Other collaborators: Matthew Ehlert, Emily McReynolds, and Hannah Werbel

• Thank you to the members of the UW BioRobotics Lab, Tech Policy Lab, and the NSF Center for Sensorimotor Neural Engineering

This project is supported by the NSF Engineering Research Center for Sensorimotor Neural Engineering (Award # EEC1028725) and the grant from the UW Tech Policy Lab.
Thank you

Contact: Tamara Bonaci
tbonaci@uw.edu
@tbonaci