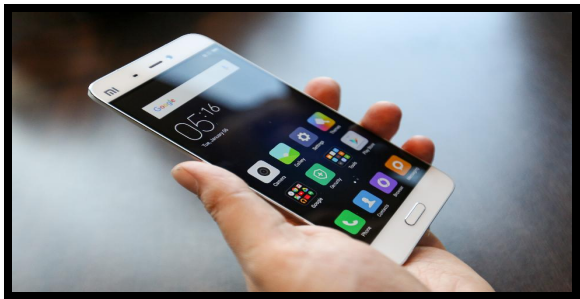# Brains Can be Hacked. Why Should You Care?

Tamara Bonaci

Department of Electrical Engineering

University of Washington

The Era of Devices Devices Attached to Us

[Pictures credit: Forbes, US News, Wired]
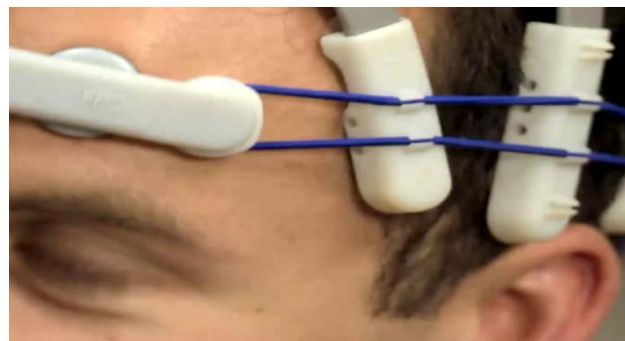
Devices Attached to Our Brains

EPOC
Emotiv

NECOMIMI
NeuroSky

Nielsen
Consumer Neuroscience

[Picture credit: Lucid]

[Picture credit: mindtecstore]

[Picture credit: forbes.com]

New and upcoming products make brain malware possible!

How Hackers Could Get Inside Your Head With 'Brain Malware'

WRITTEN BY VICTORIA TURK (/AUTHOR/VICTORIATURK)

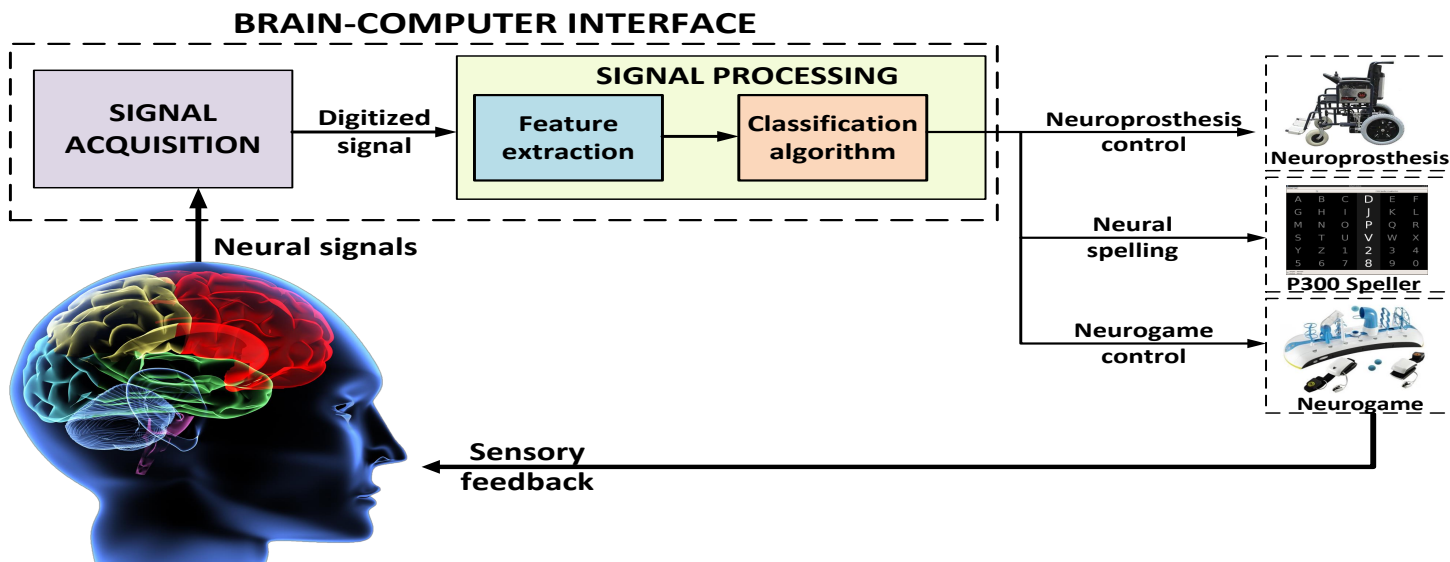August 3, 2016 // 07:50 AM EST

What is Brain Spyware?

Any malicious application that extracts private information about users from their neural signals [Martinovic *et al.*, 2012]

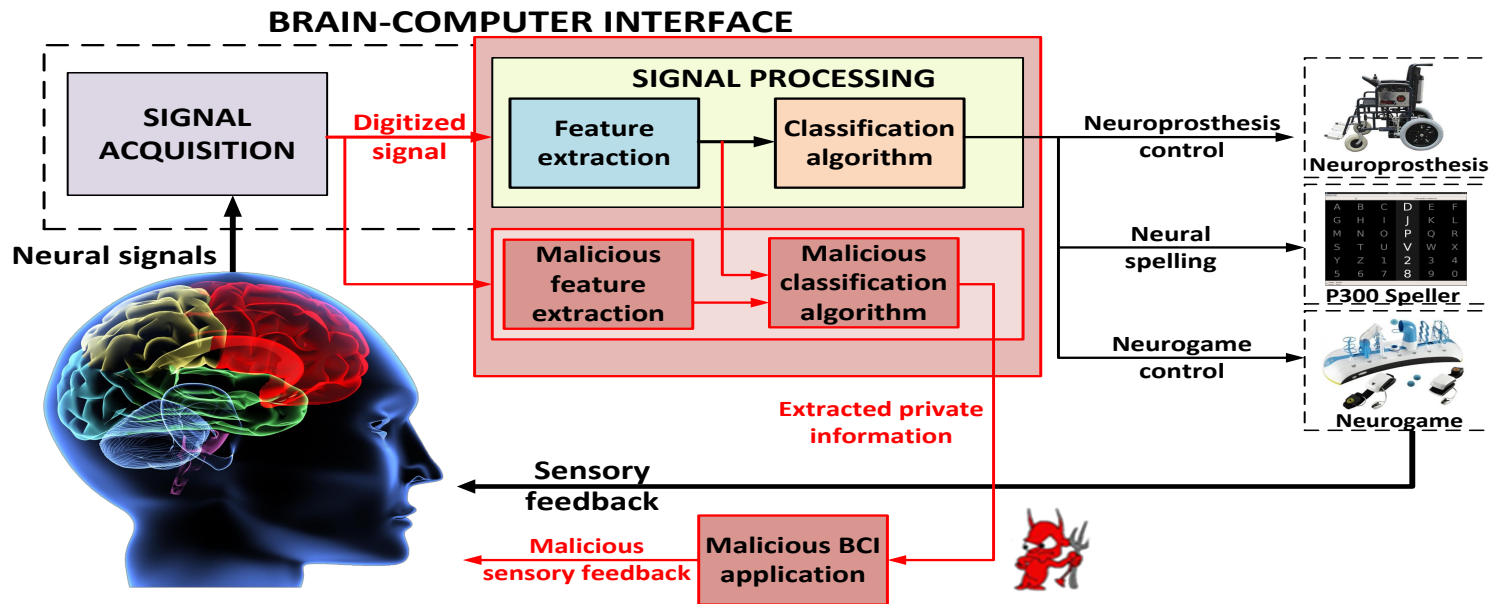[Picture credit: University of Washington]

Why Does Brain Spyware Work?

ENGINEERING PERSPECTIVE

Why Does Brain Spyware Work?

ENGINEERING PERSPECTIVE

BRAIN-COMPUTER INTERFACE

SIGNAL ACQUISITION

Digitized signal

SIGNAL PROCESSING

Feature extraction → Classification algorithm

Neural signals

Malicious feature extraction → Malicious classification algorithm

Neuroprosthesis control → Neuroprosthesis

Neural spelling → P300 Speller

Neurogame control → Neurogame

Extracted private information

Sensory feedback

Malicious sensory feedback ← Malicious BCI application

Why Does Brain Spyware Work?

NEURO-SCIENTIFIC PERSPECTIVE

Event Related Potentials (ERPs) - responses associated with specific sensory, cognitive and motor events
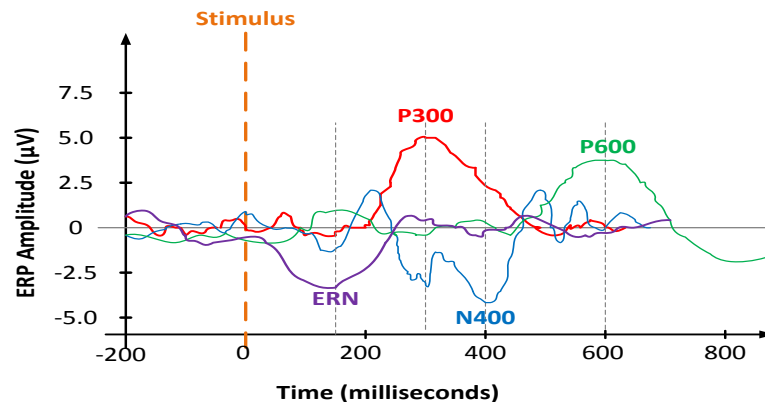
Subliminal Brain Spyware?

"What we do not see and what we do not know can hurt us"

Brannon, 1994

Subliminal Stimulation

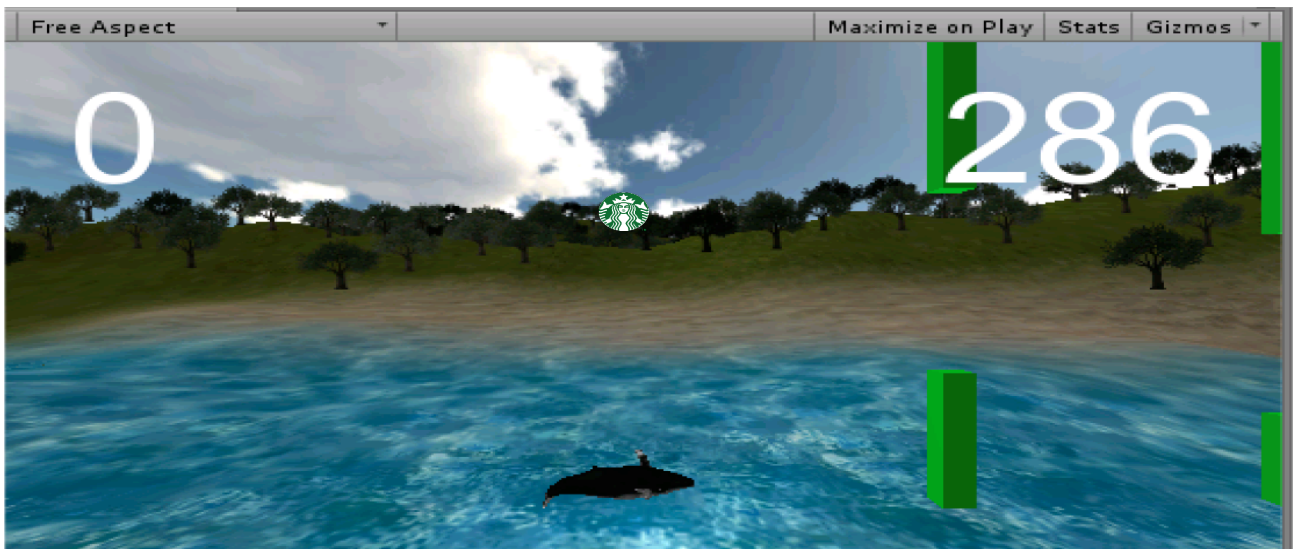- Process of affecting people with stimuli of which they are not aware
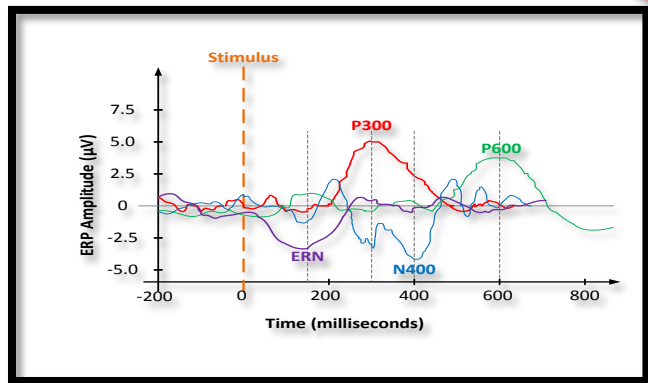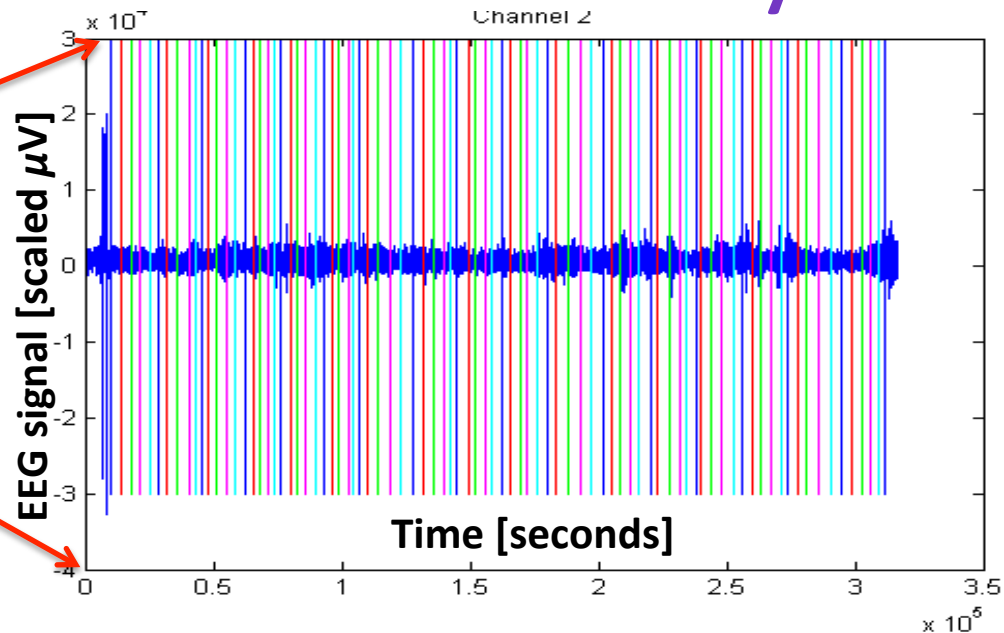
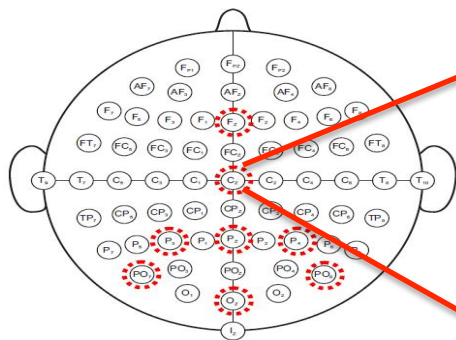# How Feasible is Subliminal Brain Spyware?

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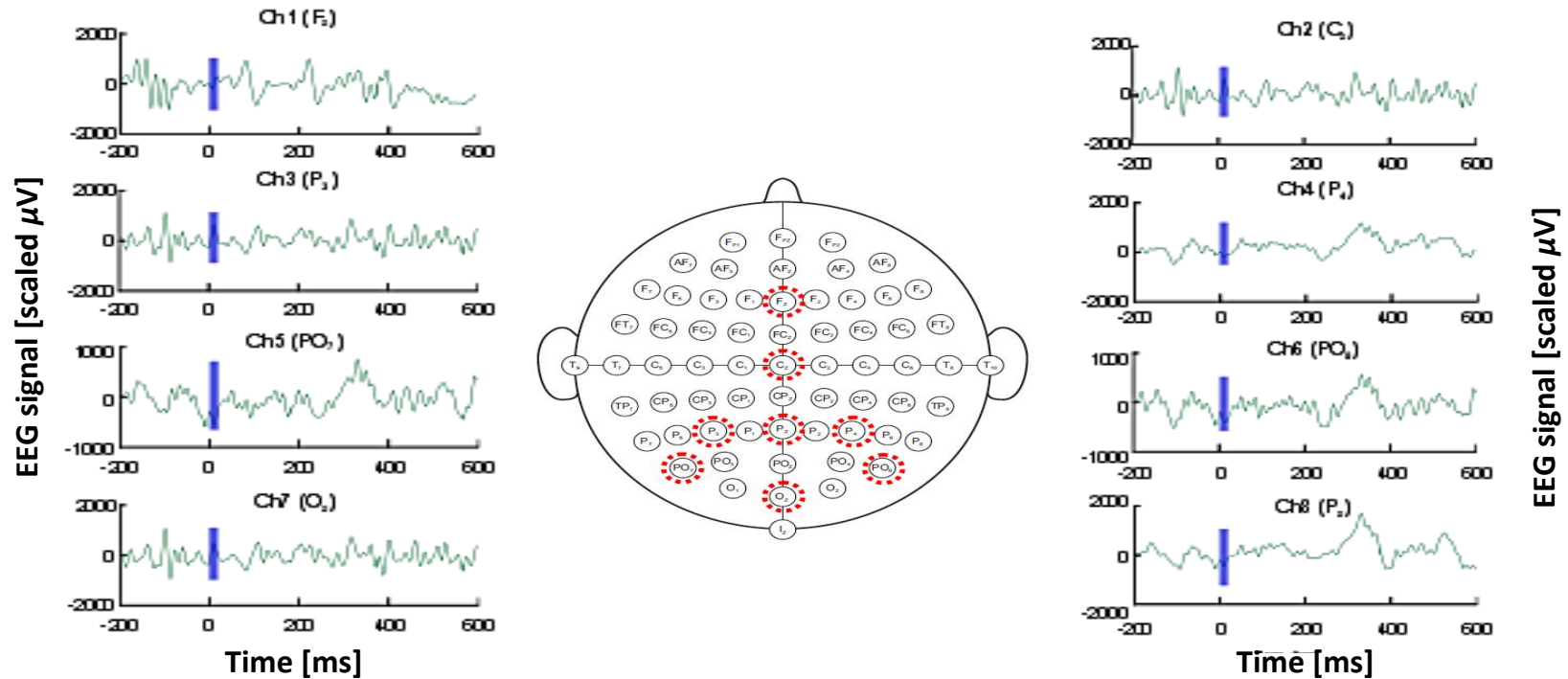
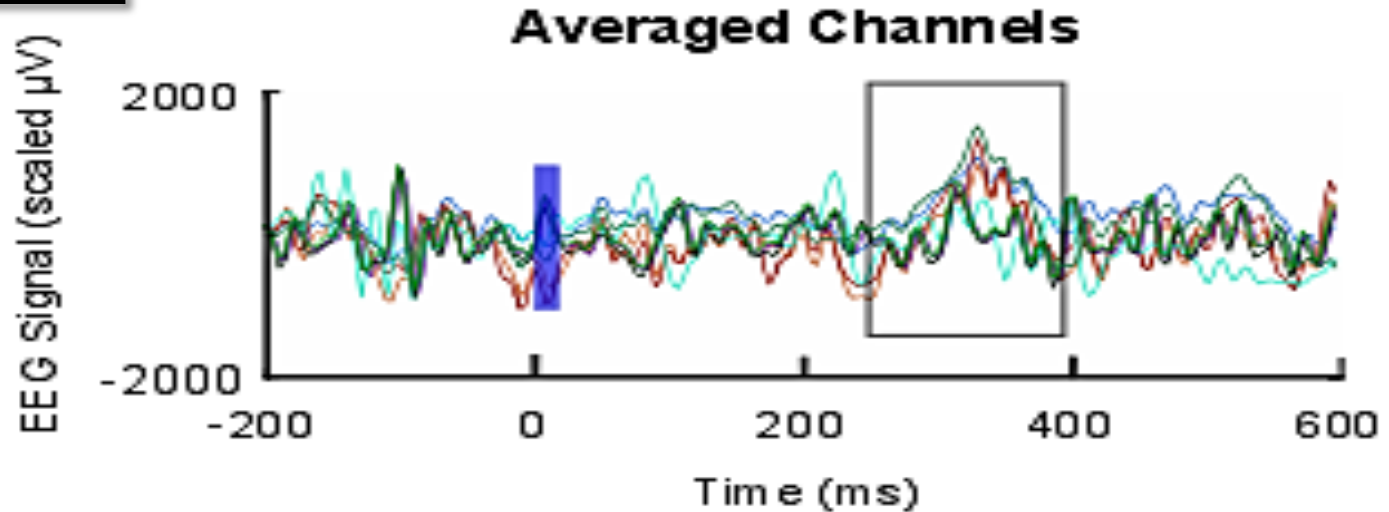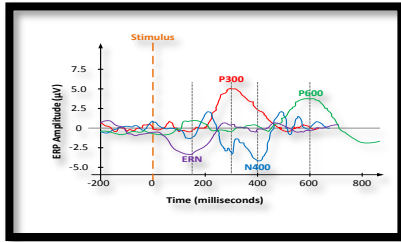# How Feasible is Subliminal Brain Spyware?

- **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

Data Preparation and Analysis

Feasibility of Subliminal Attacks

Flappy Whale, BCI-controlled game

Training data

Testing data

Time sync EEG & stimuli; epoch data

Feature extraction (Principal Component Analysis)

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

Feasibility of Subliminal Attacks

Legend:
- **Target stimulus recognized** (blue)
- **Target stimulus reported by a subjects** (green)

Y-axis: **Games** (0, 2, 4, 6, 8, 10)
X-axis: **Subjects** (1, 2, 3, 4, 5, 6, 7)

Mitigation - BCI Anonymizer

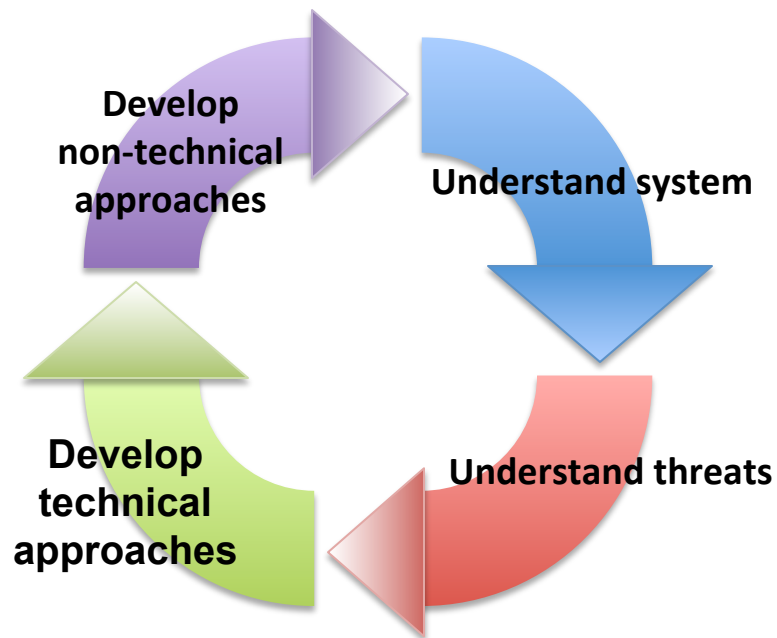**Idea:** Neural signals should be treated as a user's personally identifiable information (PII)
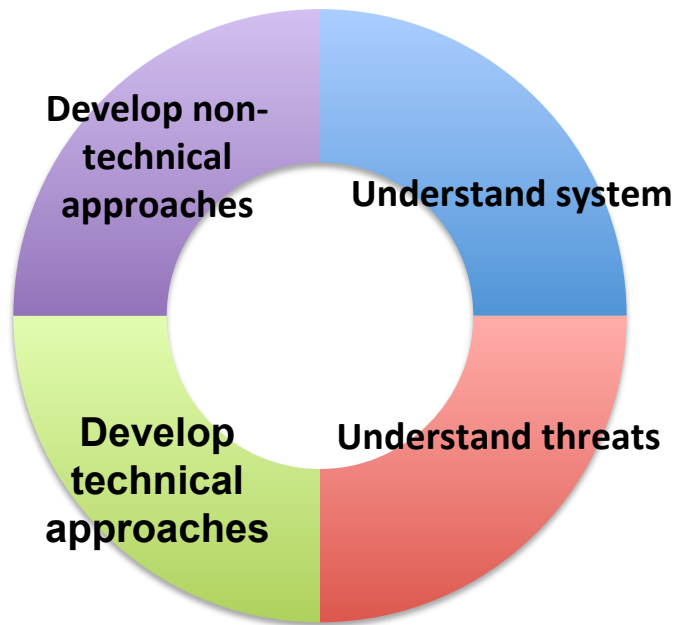

[Picture credit: NeuroFocus]

vs.

[Picture credit: The Verge]

Brains Can be Hacked. What Can We Do?

Develop non-technical approaches → Understand system → Understand threats → Develop technical approaches → (cycle)

Brains Can be Hacked. What Can We Do?

Develop non-technical approaches

Understand system

Develop technical approaches

Understand threats

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**

BioRobotics Laboratory

Thank you

Contact: Tamara Bonaci

tbonaci@uw.edu

@tbonaci