Embedded security is needed in BMI devices

Yoshiyasu Takefuji, Professor,
Keio University

(20 July 2017)

Jens Xlausen, et al., mentioned security problems of brain-machine interfaces (BMIs) in the paper entitled "Help, hope, and hype: Ethical dimensions of neuroprosthetics: Accountability, responsibility, privacy, and security are key" published in Science on June 30, 2017 (1). The BMI control technology and the computer network capability allow paralyzed people to enhance the human abilities using sensors and actuators where some of the abilities may be more than normal. Connected BMI devices are called IoT (internet of things) devices. Connected BMI devices and connected vehicles have faced the same security problem where we must protect against jamming/spoofing sensor attacks.. The connected (autonomous) vehicle uses sensors including GPS for location, millimeter wave (MMW) radar sensor for detection, LiDAR (light detection and ranging) sensor, ultrasonic sensor for distance, and camera sensor for imaging (2). Those sensors will be also embedded in BMI devices. Sensor attacking includes GPS jamming/spoofing attacking, millimeter wave radar jamming/spoofing attacking, LiDAR sensor relay/spoofing attacking, ultrasonic sensor jamming/spoofing attacking, and camera sensor blinding attacking (2). The connected BMI devices must be also protected against wireless BMI-jacking. Therefore, embedded security is needed in BMI devices. Otherwise, the connected BMI devices will become the next crime frontier.

1. Jens Xlausen, et al., Help, hope, and hype: Ethical dimensions of neuroprosthetics: Accountability, responsibility, privacy, and security are key, Science, Vol. 356, Issue 6345, pp. 1338-1339 , June 30, 2017
2. Y. Takefuji, connected vehicle security, private paper, 2017