Include Security in Brain Interfaces

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

My wife, Dr Deborah N. Black, MD, is an expert in neural feedback (NF) for improving the attention of patients with attention-deficit / hyperactivity disorder (ADHD). There's an interesting news story about the technique on National Public Radio (NPR)< http://www.npr.org/templates/story/story.php?storyId=130896102 > This approach to retraining disorderly brains monitors electroencephalographic (EEG) data as the subjects learn to focus better by playing video games or controlling the visibility of a favourite movie being played on a special DVD player or computer. There are many sites in the United Kingdom which advertise NF treatments; try search string "neural feedback adhd uk" in a search engine. For example, "Learning with neural feedback"< http://www.learningwithneurofeedback.co.uk/ > has useful information about the technique.

Deborah's work has gotten me interested in following developments in the entire field of direct neural interfaces. Back in 1995, the film "Johnny Mnemonic"< http://www.imdb.com/title/tt0113481/ > imagined a world in which people had what appeared to be standard female phono jacks in their head; the character would plug a male phono jack< http://upload.wikimedia.org/wikipedia/commons/thumb/9/93/Jack_plug.png/300px-Jack_plug.png > into his head to transfer data. The film mentioned that his brain could hold – gasp – 4GB of data! In recent years, a company called NeuroSky®< http://www.neurosky.com/ > has been developing an increasingly wide range of applications of neural interfaces. They are particularly interested in increasing EEG-sensor availability to the research community< http://www.neurosky.com/Academics/WhatWeDo.aspx >.

The future of such systems includes direct neural control of computer-equipped systems such as artificial limbs. In a recent article by Ian Sample entitled "Brain implant allows paralysed woman to control a robot with her thoughts,"< http://www.guardian.co.uk/science/2012/may/16/brain-implant-paralysed-woman-robot-thoughts > published in *The Guardian* on 16 May 2012, the author describes the ineffable joy of a woman identified only as "S3" when she managed to control a robotic arm mentally so that she was able to serve herself a cup of coffee for the first time since her stroke fifteen years ago. Another report< http://news.sciencemag.org/sciencenow/2012/05/paralyzed-patients-control-robot.html > from *Science Now* has additional details.

The studies described in the *Guardian* and *Science Now* articles use implanted electrodes in the brain; NeuroSky devices look more like earphones or headbands. I think we are only a few years away from seeing NeuroSky equipment and other lightweight, non-invasive systems for neural interfacing. There is great hope not only for disabled people who may regain control of their limbs or voices, but also for more general applications. For example, in 2008, there was news< http://www.newscientist.com/article/dn13449-nervetapping-neckband-used-in-telepathic-chat.html > of a "neckband that translates thought into speech by picking up nerve signals" that was "used to demonstrate a 'voiceless' phone call for the first time."

If a neckband can translate neural input (thinking about what we want to say) into sound, it can eventually also be used for silent dictation and for controlling computers by programs similar to Dragon Dictation®.< http://www.nuance.com/talk/ > Eventually, it should be possible to achieve that staple of science fiction, the silent "phone" conversation: the sender's neural interface for interpreting imaged speech sends data to the recipient's neural interface for interpreting digital data to brain patterns corresponding to hearing a voice. Voilà! Artificial telepathy!

At this point, we turn to the issue of integrating security into new systems using thorough analysis of potential vulnerabilities and effective quality assurance methods. Anyone interested in seeing the consequences of trying to patch security into inadequately designed and implemented products need merely consult the extensive archives of the RISKS Forum: *Forum on risks to the public in computers and related systems*< http://catless.ncl.ac.uk/Risks/ >. I've aggregated< http://www.mekabay.com/overviews/risks/index.htm > the first 25 volumes of the RISKS Digest into PDF files for convenience of readers and also generated an Acrobat PDX global index for searching the PDF files. The *RISKS Digest* site has an excellent search engine ("swish-e") that finds keywords in less than a second.

For example, the latest issue of the *RISKS Digest* [26(84)]< http://catless.ncl.ac.uk/Risks/26.84.html > includes these and other reports on breaches of security principles resulting from inadequate analysis and testing:

- Availability: Delays in billing U$1.6M in parking fines< http://catless.ncl.ac.uk/Risks/26.84.html#subj1 >
- Availability: Closing down a department of motor vehicles office< http://catless.ncl.ac.uk/Risks/26.84.html#subj2 >
- Integrity: University students received payments for tuition they never paid< http://catless.ncl.ac.uk/Risks/26.84.html#subj4.1 >
- Integrity: Flash crowd develops at a courthouse< http://catless.ncl.ac.uk/Risks/26.84.html#subj6.1 >
- Authenticity: Sliding fingers over number pads ("gestures") on mobile phones as an authentication method will fail if users have greasy fingers < http://catless.ncl.ac.uk/Risks/26.84.html#subj14.1 >

My guess is that one of the most serious threats to neural interface systems is going to be man-in-the-middle attacks (MITMAs). Examples from *RISKS Digest* include the following (note that I used my own descriptions, not the actual article titles):

- Clipper chip was susceptible to MITMA< http://catless.ncl.ac.uk/Risks/14.64.html#subj6.1 >
- HotJava 1.0 alpha 3 security issues allowed MITMAs< http://catless.ncl.ac.uk/Risks/17.43.html#subj8.1 >
- A teenaged boy used a stolen pager to send faked medical instructions to hospital staff< http://catless.ncl.ac.uk/Risks/21.19.html#subj6.1 >
- Exploding mobile phone chips by remote control – perfect situation for MITMAs< http://catless.ncl.ac.uk/Risks/21.87.html#subj1.1 >
- Home-banking online sessions were susceptible to MITMAs< http://catless.ncl.ac.uk/Risks/22.37.html#subj6.1 >
- A proxy Web service was vulnerable to MITMAs< http://catless.ncl.ac.uk/Risks/23.79.html#subj9.1 >
- Spyware program used fake certificates for potential MITMAs<

http://catless.ncl.ac.uk/Risks/23.88.html#subj5.1 >

- A firewall used fake certificates for potential MITMAs< http://catless.ncl.ac.uk/Risks/25.50.html#subj10.1 >
- A Syrian MITMA against Facebook used fake certificates< http://catless.ncl.ac.uk/Risks/26.45.html#subj10.1 >
- A forged certificate claiming to be for Google.com supports MITMAs against GMAIL users and others< http://catless.ncl.ac.uk/Risks/26.56.html#subj12.1 >

A recent summary of mobile phone weaknesses< http://www.nytimes.com/2012/01/26/technology/personaltech/protecting-a-cellphone-against-hackers.html > includes several examples of MITMAs on poorly secured phones.

So what can we envisage from neural interfaces controlling, say, computers, human prosthetic limbs, industrial robots and communications devices? How about these?

- The neighbour's kid intercepts your neural dictation signals and inserts rude words into your memo to the boss;
- A nasty pervert makes amputees dump their soda all over themselves – or punches someone in the head using the victim's prosthetic arm;
- A murderer causes an innocent user of a neutrally controlled prosthetic leg to jump into heavy traffic;
- The industrial saboteurs from our favourite hacker haven intercept the neural-interface signals in a competitor's factory to make the industrial robot go berserk, leading to several deaths, many injuries and a murder conviction for the innocent controller;
- In the near future, when neural interfaces are the standard method for communicating silently through artificial telepathy, industrial spies intercept private communications and pranksters insert inappropriate content into conversations.

Failing to include security into the design of systems – any systems – leads to serious vulnerabilities – and in some cases, serious exploits. All communications between neural interfaces and actuators *must* be designed to resist MITMAs from the very start of design.

I will be contacting manufacturers of the current generation of neural interfaces for their comments on how they are integrating security into their systems and will summarize the results for readers in a later article – assuming any of the manufacturers are willing to discuss the issue.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *