On the Security and Privacy Risks in Cochlear Implants

Daniel Bodmer
Clinic for Otorhinolaryngology
Head and Neck Surgery
University Hospital Basel, Switzerland
dbodmer@uhbs.ch

Srdjan Čapkun
Department of Computer Science
ETH Zürich
Switzerland
capkuns@inf.ethz.ch

Abstract

We analyze the security and privacy implications of cochlear implants (CI). We discuss possible attacks on CI systems and their implications for CI users, their security and privacy.

1 Introduction

Hearing loss is a common medical problem. Approximately one out of 1000 babies suffer from hearing loss. In the elderly population, hearing loss is a common complaint. It is estimated that around 30% of all persons over 65 years old and about 50% of all persons over 80 years old suffer from hearing loss. While people with problems in either the external ear or the middle ear suffer from the so called conductive hearing loss which can be treated well either medically or surgically, people with problems in the inner ear (cochlea) suffer from sensorineural hearing loss which can only be alleviated using prosthetic devices. Persons with mild to moderate sensorineural hearing loss profit from a hearing aid, while patients with profound hearing loss or deafness profit from a cochlear implant (CI). Cochlear implantation has revolutionized the treatment for severe hearing loss and has become the treatment of choice for both children and adults with this affliction. The majority of patients report enhanced quality of life and a high number of patients can understand speech without visual information (Lip reading). Cochlear implantation requires a 2-3 hour long operation and after that a fitting period in order to optimize the implants performance to the patients needs.

Implantation of CIs can also have complications. Complications after cochlear implantation can be categorized as major or minor depending whether these require surgery or not. Early major complications include facial nerve paralysis, incorrect electrode placement, and wound infection. There are also late complications such as flap problems, device malfunction or infection of the middle ear cleft to name a few [6, 4, 5].

2 Cochlear Implants

Modern CIs [2, 3, 1] share three basic components, namely a microphone, a speech processor, and an implanted receiver-stimulator. Sound is first detected by a microphone (worn behind the ear as a conventional hearing aid) and converted into an analog electrical signal. This signal is then sent to the (external) speech processor where it is processed. The processor extracts features from the signals, which determine how the implanted stimulator will stimulate the cochlea. The processor communicates with the implanted stimulator through the skin via a wireless link, using a transmitting coil that is held externally over the implanted receiver-stimulator. Typically, magnetic induction is used for this communication. This equally allows the speech processor to power the implant. The received signal is processed by the stimulator which then outputs electrical impulses to the electrodes on a coil implanted within the cochlea (inner ear). When current is applied to the electrodes, this generates an electrical field which in turn stimulates the auditory nerve fibers.

Cochlear implants are programmed (fitted) individually for each user. This is done by setting the intensity of stimulation i.e., the current level outputs of the electrodes, based on patient's report. During this procedure, speech processing program and parameters are also set. Some recent CIs come with remote control devices that allow the users to control some settings of the CI, e.g., to change the program or the parameters.

3 Security and Privacy Implications

One aspect of cochlear implantation has not been so far widely discussed: the security and the privacy implications of the implants. As stated above, cochlear implants are highly specialized devices which require and enable remote programming after the surgical procedure in order to fit the implant with the needs of the individual pa-

tient. The speech processor, the stimulator and the remote devices are therefore embedded devices that allow remote access and reprogramming.

If these devices are left unprotected from unauthorized access or can be compromised, they can become vulnerable to malicious remote reprogramming attacks. The result of the attack might be that the implant is turned off, resulting in deafness, or in reprogramming of the implant. The implant can be reprogrammed such that the intensity of the stimulation within the cochlea is increased, resulting in tinnitus and a painful perception of acoustic signals. More sophisticated attacks include the compromise of the operation of the speech processor such that it ignores the input from the microphone, and instead stimulates the user to hear the sounds generated by the attacker. Unlike the attacks that result in deafness or pain, which are quickly noticed by the user, this latter attack might be undetected by the user, especially in situations in which the user has no other (e.g., visual) means of verifying what she hears. Although the communication channel between the speech processor and the implant is a short-range channel, if it is not protected from active attackers (i.e., message insertion attacks), it can enable attacks by unauthorized speech processors which would send messages to the stimulator, effectively controlling it. It is not clear if this attack could be easy to mount remotely, given the short-range communication link between the processor and the stimulator. It is, however, well conceivable that the attacker replaces user's speech processor by a clone that then modifies what the user hears. In order to prevent this attacks, the processor and the stimulator need to be securely paired (e.g., would need to share a secret key); this would allow them to mutually authenticate and to protect the integrity of their communication. Equally, it would require that the stimulator can be securely paired with another processor even after it has been implanted, to account for the situations when the original speech processor is lost. This motivates the deployment of appropriate key management solutions for cochlear implants. Another set of attacks includes the compromise/replacement of CI's remote control device and of the link between the remote control and the speech processor.

Although at first it might seem that there are little privacy implications of CIs, not only the privacy of the user but of other people in her environment might be violated. A compromised/replaced CI system essentially acts as a microphone, storage and potentially as a real-time relay device that records and processes sounds in the environment of the user, enabling the attacker not only to record the communication between the user and others but also potentially enables the attacker to reconstruct users activities during the day and even during the night (e.g., if the attacker sets the speech processor to covertly remain *on* even if the user believes that it is *off*). The reconstruction of user's activities includes detecting user's movements (location), encounters with other people, profiling the user and his friends/family/colleagues, etc. Another privacy aspect of CIs and their remote control devices is the fact that they can be discovered (by scanning for these devices within their operating frequency band), and tracked if they use static identifiers. The scenarios in which devices are involuntarily discovered are relevant since user's might not necessarily want to disclose that they are wearing a CI device; the reasons are typically that this might have social and economic implications. If CI devices use static identifiers, or even carry some information related to the user's name, date of birth, etc, the users could be tracked and easily identified. This is a concern that is not unique to these devices, but it is more an issue since the stimulator is always implanted and is rarely changed and the speech processors are typically always worn by the users.

4 Conclusion

Cochlear implants are systems that enabled significant improvements in hearing for people with profound hearing loss. However, these devices are wireless embedded platforms that raise security and privacy concerns some of which we outlined in this paper. Given that they are composed of both implantable and wearable components, these devices pose interesting challenges for the security community. To the best of our knowledge, the attacks that we discuss were not yet demonstrated in practice, but are plausible, and unless appropriate cryptographic and security measures are deployed in CI systems, they might be exploited in the near future.

References

[1] Advanced Bionics. *http://www.advancedbionics.com/.*

[2] Cochlear Limited. *http://www.cochlear.com/.*

[3] MED-EL. *http://www.medel.com/.*

[4] COHEN, N., AND HOFMAN, R. Complications of cochlear implant surgery in adults and children. *Ann Otol Rhinol Laryngol, 100:708-711* (1991).

[5] KEMPF, H., JOHANN, K., AND LENARZ, T. Complications in pediatric cochlear implant surgery. *Eur Arch Otorhinolaryngol, 256:128-132* (1999).

[6] PROOPS, D., STODDART, R., AND DONALDSON, I. Medical, surgical and audiological complications of the first 100 adult cochlear implant patients in birmingham. *Birmingham. J Laryngol Otol, 113:14-17* (1999).

Acknowledgements

This work was supported (in part) by the Hasler Foundation, Switzerland. It represents the views of the authors.