DESIGN AND IMPLEMENTATION OF A SOFTWARE APPLICATION FOR SECURE WEB-BASED COMMUNICATION FOR PEOPLE WITH SPEECH DISORDERS

Abstract:
All people need to communicate with their families, friends, neighbours, and physicians through various communication means. However, there are common barriers to communication needs of mute or/deaf people, most importantly in terms of the declining sensory and physical abilities. On the other hand, technological advances have led to the development of a variety of new tools and technologies through various communication medium including the Internet for assistive and augmentative communication for individuals with disabilities. Although communication through the Internet seems highly attractive, it poses privacy and security issues. In this paper a web-based secure message transfer application is proposed to address privacy related information security threats directed to software-based communication of mute and deaf people. The proposed application is practical and easy-to-implement, and is based on the integration of cryptology and steganography. With its easy-to-use graphical user interface suitable for different devices, it can easily be used by its potential users for ensuring the privacy and security of their message transfers. The main limitation of the proposed application is that the application requires a public web server and hence may be vulnerable against attacks directed to web servers if required precautions are not taken.

Keywords:
Security threats; message security; cryptology; steganography.

JEL Classification: L86, C88
Introduction

The ability to communicate is essential for all people. However, it is more essential for mute or/and deaf people since in addition to communicating with their families, friends, and neighbours, they need assistance with daily living activities and enjoy intergenerational contacts with family members, gain access to health and legal information, and fulfil lifelong learning goals. On the other hand, they have major barriers to their communication including sensory and physical abilities.

Deaf people use a variety of methods of communication such as sign language (SL) and lip reading (LR). Therefore, many deaf people communicate quite well with other deaf people and with people that can hear well. However, although many deaf people communicate with SL, many hearing people do not know SL. Also, some deaf people do not know SL and rely on LR. Moreover, all people who know SL do not use the same form of SL. Similarly, some mute people use SL to communicate. Others use alternative methods of communication including written notes, flash cards, Bliss symbols, pictures, words, helper pages, speech recording and replaying, vocalization, and LR lip-reading by the communication partner. In addition, some mute patients have adapted to their disability by using machines which can vibrate their vocal cords and this way allows them to speak.

In the last decade, due to the increasing interest in new technologies for assistive and augmentative communication for individuals with disabilities, new ways of communication has been developed. Especially due to the advances in information and communication technologies, computers, smart phones and the Internet has together offered alternative methods of communication to deaf and mute people. Nowadays, there are many augmentative and alternative communication devices which allow deaf and mute people to communicate such as hardware or software-based text-to-speech solutions. Nowadays, there are some practical and low/no-cost solutions provided by the Internet. Deaf and mute people use can us e-mail programs, chat applications, social media platforms and the Internet to interact with mute and deaf people and with hearing people.

Although some secure options for sending and receiving e-mails and information are available, most of the founding technologies and protocols which transfer data in clear text are still used and therefore the e-mails are insecurely transferred through the Internet. On the other hand, due to the increasing availability of the Internet, this becomes a more severe issue as the data can be captured by eavesdroppers or hackers while it is moving through the Internet (Wong, Gouda and Lam, 2000; Dolev and Yao, 1981; Bloch et al., 2008). Basically, there are two main concerns which can be applied to both message senders and recipients. As well as the security of communication links, the security of messages and attachments must be provided. For these goals, in order to provide confidentiality, integrity and authenticity of messages delivered between Internet
users, secure protocols and encryption techniques can be employed to ensure the 
security of e-mail communications and data transfers (Zhou, Fang and Zhang, 2008; Karlof and Wagner, 2003; Yang et al., 2004; Avancha et al., 2002).

In this paper, a web-based secure message transfer application is proposed to address 
common information security risks encountered during message transfers, and in this 
way ensure the integrity and privacy of private user messages.

**Proposed Web-Based Communication Framework**

The proposed application shown in Figure 1 and Figure 2 has two user types: member 
and non-member. While members can create and send messages, non-members can 
receive messages. The proposed application is based on the integration of cryptology 
(Dzung et al., 2005) and steganography (Provos and Honeyman, 2003), and operates in 
three main steps. In the first step, the message typed by the user is encrypted using AES 
(Daemen and Vincent, 2003; Murphy, 1999). Cryptanalysis studies showed that AES is 
strong against different kinds of attacks (Bogdanov, Khovratovich and Rechberger, 2011; Biryukov and Khovratovich, 2009). Then, the encrypted message is embedded in a cover 
image. Finally, a code to be used to reach the encrypted message is created by the 
algorithm and sent to the intended recipient. Using the code, the recipient can get the 
original message. The member users can also stop receiving hidden messages.

**Figure 1: Homepage of the proposed application**
Figure 2: Creating a secure e-mail using the proposed application

Figure 3: Steps used by the proposed framework to send an e-mail

Begin

Type the mail address  
Select image

Encrypt message with AES

Type message

Hide message into the image

Encrypt username, Message ID and E-mail with MD5

Change the image name with encrypted text

Send mail

End
After the user enters the recipient’s e-mail address, he/she selects an image which will be used in the encryption of the message. Then, he/she types the message and clicks Send button. Flowchart shown in Figure 3 shows all the steps used by the proposed framework to send an e-mail. After the recipient’s enter the code shared between the two parties, if the code is correct, then the server allows extracting the message text from the image. Then, the message is decrypted and displayed to the recipient. Flowchart shown in Figure 4 shows all the steps of the reverse process used by the proposed framework to receive an e-mail.

To analyze and prove the effectiveness of the proposed approach in protecting the privacy and security of message transfers, a sample case study was realized. As shown in Figure 5 and Figure 6, the case study consisting of a packet tracking using Wireshark (Wireshark.org, 2016) and an analysis with Fiddler (Telerik.com, 2016) showed that the proposed application ensured the privacy of the user message.
Figure 5: Packet tracking using Wireshark

Figure 6: Web debugging proxy - Fiddler
Conclusion

In this paper, to address potential information security risks encountered during message transfers of mute and deaf people, a web-based secure message transfer application is proposed. The proposed application is simple and easy-to-implement. Basically, it is based on the integration of cryptology and steganography, and is an efficient tool for ensuring the communication security of private user messages. The proposed application’s member users can encrypt messages and embed them in cover images. They can also send codes to enable the others to receive the altered cover images which contain embedded messages and look at their own inboxes to see whether they have unread messages or not. On the other hand, the non-member users can only receive their messages by means of the codes they have received.

References


