Print This Article

<< Return to Steganography harnesses VoIP networks

Steganography harnesses VoIP networks

Wojciech Mazurczyk and Krzysztof Szczypiorski
July 04 2008
The main aim of network steganography is to hide secret data inside users' normal data transmissions, ideally so it can't be detected by third parties.

One of the most popular steganographic techniques is to use a covert channel, which offers an opportunity to "manipulate certain properties of the communications medium in an unexpected, unconventional, or unforeseen way, in order to transmit information through the medium without detection by anyone other than the entities operating the covert channel," to quote Wikipedia.

Covert channels may be dangerous to company networks as they can lead to the leakage of confidential information. However, it is hard to assess what bandwidth of a covert channel poses a serious threat. Generally, it depends on the security policy that is implemented by the organisation concerned. The ideal case will be to eliminate all possibilities of hidden communication, but practically it is not possible as the number of steganographic techniques is high and still growing rapidly.

The dangers of VoIP

Voice over IP, or IP telephony, is one of the most popular services in the IP world and it is influencing and changing the entire telecommunications landscape. Because of its popularity, it is increasingly becoming a target in which to hide communications.

We propose to name steganographic techniques applied to VoIP traffic "steganophony". This term includes information-hiding techniques like those described below but also methods such as audio watermarking, or techniques applied to speech codecs.

To explain IP telephony steganography, it is important to understand that IP telephony connections may be divided into two phases: a signalling phase and a conversation phase. In both those phases certain types of traffic are exchanged between calling parties. Both types of traffic may be used for information hiding.

At Warsaw University of Technology, we have experimented with selected steganographic techniques to see how much hidden information can be sent in an average VoIP call. Our results showed that more than 1.3Mbps can be sent in one direction.

Three new steganophonic techniques

We are contributing to the steganophony field by proposing the following three, new steganographic techniques for VoIP.

These are:

- LACK (Lost Audio Packet Steganography) which uses intentionally delayed audio packets;
- HICCUPS (Hidden Communication System for Corrupted Networks) which is a medium-

dependent steganographic technique for VoWLAN (Voice over Wireless LAN);
- SIP/SDP (Session Initiation/Description Protocol - protocols from the signalling phase of the call) and RTP/RTCP (Real-Time Transport/Control Protocol - protocols from the conversation phase) steganography, which utilises the syntax and semantics of those protocols, such as free/unused fields.

LACK

The proposed method utilises a feature of VoIP where excessively delayed packets are not used for reconstruction of the conversation at the receiver (the packets are considered useless and discarded).

To take advantage of this technique, some packets are selected from the audio stream and intentionally delayed before transmitting. If we are sure that the delay of such packets is considered excessive at the receiver (which is not aware of the hidden communication), the payload of the intentionally delayed packets may be used to transmit secret information to other receivers which are aware of the procedure.

HICCUPS

HICCUPS is a generic steganographic framework for wireless LAN and it can be used in voice over wireless LAN (VoWLAN) deployments. In HICCUPS, information is exchanged in data payloads of frames with intentionally created bad checksums. Normally, stations, which do not belong to the hidden group, discard corrupted frames with bad frame checksums, but in HICCUPS these frames carry hidden data. This method gives the opportunity of creating additional on-demand bandwidth for steganographic purposes.

RTP/RTCP/SIP/SDP steganography

This type of steganography covers a wide range of information hiding techniques including popular techniques based on IP or TCP protocols, for which the main idea is to use free or unused fields of these protocols.

We have shown how these techniques may be applied to VoIP signalling protocols (like SIP/SDP) or protocols used in the conversation phase of the call (RTP/RTCP). This information hiding technique can be detected, for example, by using active wardens. An active warden is a system or process similar to a firewall which attempts to eliminate hidden communications.

We propose a technique, which we have called security mechanism steganography, for which security countermeasures like active wardens do not work. The main aim of security mechanism steganography is to exploit the fields in VoIP protocols which carry security information that is utilised to provide security services, for example authentication.

By altering the security data, such as authentication tags, in each RTP packet, hidden communication is possible. Moreover, because data in these fields is almost random, it is hard to detect whether they carry real security data, or hidden information. Thus most steganalysis methods will fail to uncover this type of secret communication.

No real-world steganographic method is perfect: whatever the method, the hidden information can be potentially discovered. In general, the more hidden information is inserted into the normally transmitted data, the greater the chance it will be detected. But because the number of steganographic methods is high, and there is no single method to detect them, we should consider steganography in VoIP as a threat to organisations' security.

About the authors

Wojciech Mazurczyk holds a BSc and MSc in telecommunications, both from Warsaw University of Technology. He is now pursuing a PhD at WUT in network security focusing on information hiding

techniques, network security and multimedia services.

Krzysztof Szczypiorski has received an MSc and PhD in telecommunications from the Warsaw University of Technology and is now an assistant professor at WUT. His main research interests are network security and steganography, wireless networks and privacy in virtual society.