# Secure Voice over Internet Protocol

## Prototype

EUROPEAN UNION
European Regional Development Fund

*Investing in the future by working together for a sustainable and competitive region*

The Interreg IVB North Sea Region Programme

Content



# 1. Summary

The idea to this project came up in the Laboratory for Communication Networks and Transmission Technology of the Jade Hochschule in Wilhelmshaven. In 2009, the first steps for a public, highly secured server for incoming and outgoing calls were taken within a bachelor's thesis.

Since years, we are exploring the possibilities and risks of the communication via public data networks, also known as Voice over Internet Protocol (VoIP).

During these examinations, which were supported in forms of projects and diploma respectively bachelor theses, several server solutions were set up, configurated und analysed.

Next to the proprietary solutions as Cisco Callmanager, Callmanager Express and the Panasonic Unified Communication Server we also tried open source projects as Asterisk and FreeSWITCH.

As a little side work, we analysed the packet based transmission of the with VoIP upcoming stream of data and speech in a Local Area Network. It turned out, that one can easily use software-tools to redirect the streams to an own computer (man in the middle attack). On this computer, you can save and decode the streams in real-time – (Big Brother is watching you). Neither the person who called nor the one who accepted the call will recognize that a third person is listening.

A similar way to attack is also possible in Wide Area Networks (internet), but not without breaking the laws, which may not be a point of interest to some entities.

Only few providers offer secured VoIP. At the beginning of the Security VoIP project we only had informations about a provider from Düsseldorf in Germany, but they only provided SRTP, not SIPS.

We wanted to fix this.

If you are concerned about your privacy, register with our system and download the free software PhonerLite or buy a SNOM320 IP Telephone to use SecVoIP. First you have to

registrate at our FreeSWITCH (see next section), installed on a powerful machine, which is located in our server maintenance centre.

Then you can talk to other registered customers without being wire taped.

A further step in the future will be enabling of routing into the public communication network. This feature cannot be offered for free, unfortunately.

# 2. Intention to be used

Conventional VoIP-connections (talking via internet) transmit using the protocols SIP (Session Initiation Protocol) and the RTP (Real-Time Transport Protocol). Every provider in the market is using these standards. It is barely known – or not as important as it should be – that it is very easy to redirect RTP data streams to another computer where they can be decrypted and saved in real-time.

To solve this issue, we use Open Source Software "FreeSWITCH". FreeSWITCH is capable to encrypt VoIP calls. Encoding the stream keeps the „man in the middle“ away from secretly intervening the call.

It is possible to enable the encoding by enhance the RTP to it’s secure version SRTP (Secure RTP). The data will be encrypted by a high efficient encrypting algorithm called AES. To encrypt the key and data during initiation of the call, an enhancement of SIP is used: SIPS (session initiation protocol security). Encrypting is done with TLS/SSL. TLS/SSL is also used on secured internet connections (https).

The basic algorithms are so complex, that decryption cannot be done in time, regarding to days knowledge.

***Which Hardware can be used?***

Unfortunately, not every VoIP-telephone or soft-client is capable to perform these encryptions. After numerous tests we found two telephony solutions that satisfy the high demands. We recommend fully encrypted communications that use VoIP phone solutions:

1. Hardware Phone: SNOM 320 (SNOM 370)

2. Software phone: PhonerLite

Also possible is unencrypted use of our server as a "normal" SIP server. In this case all market available SIP-based telephony clients are functional.

# 3. Geographical scope

Due to the application of providing a telephone server we do not have any geographical

restrictions. The SecVoIP server is located in Wilhelmshaven and available via internet (www.secvoip.de) from everywhere.

# 4. Project partner involved

We built SecVoIP at the UAS Wilhelmshaven. Everybody throughout the world is invited to use and test our system. Especially Compare Karlstad Foundation showed interest and we will cooperate in order to improve our prototype.

# 5. Illustration of the prototype

A first illustration of SecVoIP´s internet presence shows the picture below.

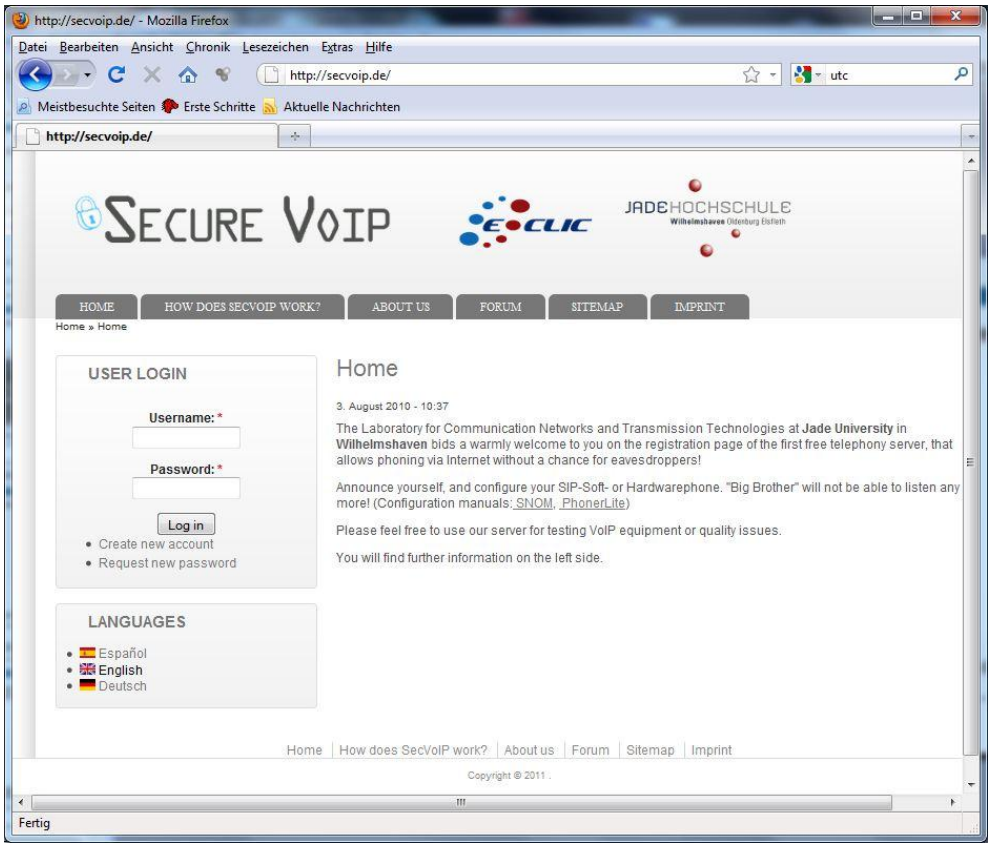


Figure 1: Internet presence of SecVoIP

For use or detailed illustration visit the website www.secvoip.de.