

# Secure-voIP

*Better safe than sorry...*

## Symbian / Windows Mobile (PDA and SmartPhone) support

### Introducción

Es la era de las soluciones de Voz sobre IP. La mayor parte de las empresas de telecomunicaciones en el mundo ofrecen o se están preparando para el despliegue de los servicios VOIP. Esto demuestra claramente que la Telefonía IP tiene un futuro brillante por delante. Sin embargo, el generalizado despliegue de telefonía IP ha traído aparejado desafíos y riesgos adicionales en materia de violaciones de seguridad. Ha habido ejemplos de escucha y otras violaciones que han creado una urgencia de tapar estos agujeros de seguridad. Secure-voIP trata los desafíos en materia de seguridad de VOIP al proveer lo siguiente:

- Autorización
- Autenticación
- Seguridad de la capa de transporte (TLS)
- Codificación de medios de doble capa

### Seguridad

Secure-voIP utiliza una protección de doble capa, de codificación Simétrica y Asimétrica.

- El primer nivel cubre la seguridad según el Protocolo de seguridad de la capa de transporte
- El Segundo nivel usa un mecanismo de seguridad inherente disponible en el protocolo de comunicación de medios.

La arquitectura completa de seguridad está construida con el único propósito de tratar las siguientes necesidades:

- Autenticación – Ambas partes en la comunicación deberían poder autenticar e identificarse a sí mismos de manera apropiada.
- Confidencial – La comunicación debe ser segura y confidencial entre las partes.
- Integridad- La comunicación no debería sufrir cambios en medio del camino. La Parte A debería escuchar lo que la Parte B quiere comunicar.
- Secreto de reenvío – Se espera que las claves de seguridad que se utilizan para una llamada particular se intercambien con frecuencia para que no se utilicen para ninguna llamada futura.

## Técnica

Secure-voIP utiliza la siguiente técnica:

Antes de que se realice la llamada, Secure-voIP se identifica con el servidor. Ésta es una comunicación SSL HTTP con una clave de 2048 bits. El algoritmo RSA se utiliza para la generación de Claves. Estas claves de 2048 bits de longitud se utilizan al momento de la autenticación. El Servidor provee su certificado al Cliente para asegurarse de que todas las comunicaciones futuras se cifren. La clave de sesión de 256 bits se genera entre el cliente de Secure-voIP y el Servidor para su cifrado utilizando claves simétricas. Esta clave de sesión se reemplaza para cada llamada telefónica.

Una vez que se ha intercambiado la clave de sesión entre el Cliente y el servidor, todas las comunicaciones futuras se cifran. No hay credenciales fijas para el Cliente. Estas credenciales se generan para cada llamada telefónica para asegurar que el Servidor y el Cliente no se vean comprometidos. Hay un secreto generado por el servidor que se comparte con el cliente sobre HTTPS. El cliente utiliza este secreto para generar credenciales sobre la marcha que a su vez se utilizan para realizar llamadas VOIP.

Al menos que y hasta que el cliente se haya identificado con el servidor, no se puede intercambiar un secreto para generar credenciales y sin estas credenciales no se pueden realizar llamadas. Estas credenciales son válidas para una llamada en particular. Una vez que se realiza la llamada, el servidor se despoja de este secreto y las credenciales. Todos los mensajes de señal VOIP y los paquetes de voz se cifran utilizando un cifrado simétrico que se acuerda durante el protocolo de intercambio TLS. Es un cifrado simétrico AES de 256 bits que se utiliza para el cifrado.

Los datos cifrados se vuelven a cifrar utilizando un mecanismo de seguridad SRTP. Se utiliza el protocolo de Gestión de claves (ZRTP) para generar las claves de sesiones. Los paquetes de voz cifrados se descifran por medio del algoritmo de cifrado simétrico AES. Entonces los paquetes de voz sufren un cifrado de doble capa.

Secure-voIP ofrece confidencialidad para los paquetes de voz por medio del cifrado de las respectivas cargas; integridad para la voz y los paquetes de señalización, junto con la protección de repetición; actualización periódica de las claves de sesión, las cuales limitan la cantidad de texto cifrado que produce una sola clave, disponible para un adversario para descifrar; una derivación de clave de sesión segura con una función pseudo al azar en ambas terminales, el uso de claves con sal para proteger contra ataques pre-computados. Secure-voIP logra alto rendimiento y baja expansión de paquetes al usar rápidos cifradores de flujo para su cifrado, un índice implícito para la sincronización y funciones universales de hash para la autenticación del mensaje.

## Características

- Fácil de usar No se necesita una configuración importante para el cliente. Solo instale y comience a realizar llamadas Secure VOIP.
- Alta calidad de audio
- Casi sin eco durante las llamadas
- Baja latencia
- Sin credenciales fijas Credenciales automáticamente generadas y suministradas por el servidor para cada llamada conexión Secured HTTP con clave de longitud de 2048 bits.
- Clave RSA de 2048 bits para autenticación
- Generación automática de claves AES
- Función de derivación de clave que se aplica para generar las claves de sesiones
- Claves de sesiones de 256 bits que se actualizan periódicamente
- Cifrado de voz de doble capa
- Se usa ZRTP para la gestión de claves en SRTP
- Clave AES de 256 bits para cifrado de voz
- Mensaje de texto invisible cifrado RC4 desde el emisor hasta el receptor para proveer el SIP URL del emisor
- Mensaje SIP IM AES 256 cifrado desde el receptor al emisor para compartir el SIP URL del receptor
- Habilidad para funcionar más allá de la mayoría de los NAT y los firewalls. Funciona a la perfección en WiFi, GPRS y 3G ofreciendo comunicación entre dispositivos móviles detrás de NAT.