Jorge Penya Sordo, Igor Ruiz Agúndez,
Juan López de Uralde Huarte y Pablo García Bringas
DeustoTech Computing, Tecnológico Fundación Deusto

El **proyecto ZIURFONE** hace más seguras nuestras comunicaciones de VoIP

ZIURFONE consiste en un software seguro para terminales telefónicos siguiendo el estándar SIP (VoIP) integrado con certificados digitales software y hardware (smart-cards).

Introducción

Las telecomunicaciones mediante VoIP (*Voice over the Internet Protocol*) están ganando cada día más y más terreno a las líneas de voz tradicionales. El despliegue de redes de banda ancha, el desarrollo de nuevos terminales móviles y el éxito de los protocolos que habilitan la VoIP han hecho posible que surjan nuevas formas de comunicación. Sin embargo, y tal y como ocurre en muchas otras áreas de la ingeniería, la seguridad de la VoIP ha sido un aspecto poco estudiado.

Es por ello que el proyecto ZIURFONE persigue mejorar, en la medida de lo posible, la seguridad de la VoIP. En concreto, se pretende desarrollar un terminal de comunicación seguro. Esto es, un «teléfono *software*» (ejecutable en un ordenador) que sea robusto y que garantice nuestras comunicaciones. Para ello, se autenticará y validará la identidad del usuario utilizando certificados digitales, y se garantizará un uso seguro de los servicios de red detectando y previniendo usos fraudulentos.

Al finalizar el proyecto, ZIURFONE será el primer terminal del mundo en utilizar certificados digitales para hacer más seguras las tecnologías de VoIP. Además, este proyecto podrá utilizarse en múltiples ámbitos, como el doméstico, empresarial o administrativo. Para el doméstico, por ejemplo, podremos utilizar nuestro DNIe para llamar por teléfono a través del ordenador con las máximas garantías de seguridad posibles. Este terminal también podrá adaptarse a las necesidades de las empresas y administraciones que necesiten garantizar sus comunicaciones de VoIP, mejorando de esta forma sus servicios a clientes y ciudadanos.

Figura 1
Uno de los primeros modelos de terminal telefónico

Téléphone - by zigazou76 - license cc attribution

Conceptos relacionados

VoIP

La telefonía sobre IP ha captado la atención de los proveedores de servicios de Internet (ISPs) en todo el mundo, ofreciendo una amplia gama de servicios nuevos y reduciendo al mismo tiempo sus costes de infraestructura. La voz sobre IP está cambiando el paradigma de acceso a la información a través de la fusión de voz, datos, fax y funciones multimedia en una sola infraestructura de acceso convergente (Red IP). Dado que IP es una norma abierta, la VoIP brinda a los proveedores de servicios flexibilidad para personalizar sus servicios existentes e implementar nuevos servicios con mayor rapidez y eficiencia.

Las centralitas de VoIP y los callcenters

Las centralitas telefónicas VoIP sustituyen a las centralitas telefónicas tradicionales y proporcionan un número de extensión a cada empleado. Todas las llamadas se envían mediante paquetes de datos en lugar de sobre la red telefónica tradicional. Mediante el uso de una pasarela VoIP se pueden conectar líneas telefónicas existentes a la centralita IP, y hacer y recibir llamadas telefónicas mediante una línea tradicional.

De este modo los *callcenters*, ante el crecimiento explosivo de sus necesidades, disponen de una solución para lograr un equilibrio entre la eficiencia operativa y la calidad del servicio. En los servicios telefónicos este reto es a menudo llevado al extremo ya que un centro de llamadas sirve miles de llamadas diarias, cada una de ellas exige una respuesta en el plazo según dos modelos analíticos que buscan el codiciado equilibrio.

En concreto, este proyecto utiliza la centralita de *software* libre *Asterisk*. Debido a su gran versatilidad y flexibilidad a ha sido considerada como la plataforma perfecta para la integración de pasarelas y centralitas de VoIP. Permite llevar a cabo tareas de transcodificación (paso de un *codec* de voz a otro), *bridging* entre diferentes tecnologías o control y monitorización de la red.

Session Initiation Protocol (SIP)

Fue desarrollado con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia (video, voz, mensajería instantánea...). En el año 2000 fue aceptado como protocolo de señalización de 3GPP y elemento permanente de la arquitectura IMS (*IP Multimedia Subsystem*)

Debido a su simple y rápido mecanismo de establecimiento de sesión, SIP se ha introducido con gran rapidez en el mercado de VoIP. Previamente, el mercado estaba dominado por implementaciones adheridas al complejo estándar telefónico H.323. Mientras que H.323 es un modelo muy cercano a la tradicional 3.ª capa de establecimiento de llamada de RDSI y usa mensajes codificados en binario ASN.1 para la señalización, SIP está basado en el modelo de transacción petición/respuesta como en HTTP por medio de mensajes legibles ASCII con una sintaxis casi idéntica a HTTP/1.1.

Mecanismos de seguridad SIP

Por una parte, dado que la estructura del mensaje SIP es una derivación directa del modelo petición/respuesta de HTTP, todos los mecanismos válidos para HTTP pueden ser también aplicados a las sesiones SIP. Por otra parte, el uso de contenedores MIME en los mensajes SIP sugiere el uso potencial de los mecanismos de seguridad de correo electrónico como PGP o S/MIME. Y por supuesto es similar a HTTPS con la construcción de túneles seguros de transporte usando TLS. Y por último, la seguridad IP (IPsec) puede ser usada como un mecanismo de propósito general para cifrar todas las comunicaciones basadas en IP sobre la capa de red.

Métodos de autenticación: PSK (Pre-Shared keys) PKI (Public Key Infraestructure)	Autenticación	Integridad de datos	Confidencialidad	
Autenticación básica HTTP 1.0	PSK	–	–	Obsoleto para SIPv2. Transmisión insegura del *pass*.
Autenticación implícita HTTP 1.1	PSK	–	–	Basado en *hash* MD5 de contraseña fuerte
Pretty Good Privacy (PGP)	PKI	√	√	Obsoleto para SIPv2
MIME Seguro (S/MIME)	PKI	√	√	Para el cifrado, la clave pública debe ser conocida por el receptor
SIPS URI (TLS)	PKI	√	√	Aplicación SIP y los *proxys* deben integrar TLS

Fraude

En las empresas de telecomunicaciones que proveen servicios globales se pueden encontrar escenarios de fraude. En la actualidad todas las empresas disponen de un departamento de fraude específico, así como de las herramientas de análisis necesarias para minimizar y prevenir dichos escenarios. A continuación se detallan una serie de posibles fraudes:

- *SIM Boxing:* Operadores fraudulentos que consiguen saltarse los costes elevados de interconexión entre operadores internacionales mediante el encaminamiento de llamadas internacionales como locales, usando para ello redes públicas como Internet.
- *Hacking* de centralitas telefónicas: Si la configuración de seguridad no es correcta, un usuario externo podría utilizarlas ilícitamente para encaminar llamadas de forma fraudulenta a costa de la empresa.
- *Dialers:* Programas a modo virus que modificaban las propiedades de conexión de acceso a redes en los que equipos infectados y cambiaban el número telefónico del nodo de acceso por un número de tarificación especial. Eran capaces de activarse automáticamente sin intervención del usuario.
- Fraude interno: A pesar de que estadísticamente la mayoría de los ataques proceden de fuera, los ataques internos tienen un impacto ostensiblemente superior. Proceden en su mayoría de roles privilegiados como son los administradores de sistemas pero en segundo lugar se encuentran empleados sin roles privilegiados.

Sistemas de gestión de fraude

Los sistemas de gestión del fraude (*Fraud Management System* [FMS]) son un conjunto de herramientas que ayudan a detectar señales de fraude. Estas señales suelen ser comportamientos anormales en las operaciones realizadas por los usuarios. El objetivo de los FMS es automatizar el procesado de información en busca de estos comportamientos anómalos, definidos normalmente mediante reglas, y notificar a los operadores del servicio en aras de reducir el impacto del fraude.

Identidad digital

El concepto de Identidad Digital, o Gestión de Identidad Digital, hace referencia al sistema integrado de políticas y procesos organizacionales que pretenden facilitar y controlar el acceso a los sistemas de información y a las instalaciones. Para ello, por lo general, dicho concepto aglutina toda una colección de funcionalidades, entre las que aparecen por lo general las siguientes:

- Gestión de Identidades, con el objetivo de proporcionar servicios de provisión/desprovisión de cuentas, de automatización del flujo de trabajo,

de administración remota delegada, de sincronización de contraseñas, y de reemplazo automático de contraseñas.

- Control de acceso, con el objeto de implementar servicios de políticas de control de acceso, dar capacidades de *Enterprise/Legacy Single Sign-On* (SSO) así como *Web Single Sign On* (SSO), o *Reduced Sign On*.
- Servicios de directorio, con el objeto de proporcionar capacidades de repositorio de identidades (servicios de directorio para la administración de los atributos de cuentas de usuario), sincronización y/o réplica de metadatos, virtualización de directorios, sistemas de directorio de escala *de e-Business*, servicios de directorio compuestos (CADS, CADS SDP).
- Otras categorías, como pueden ser control de acceso basado en perfiles —o roles— (RBAC), federación de derechos de acceso a los usuarios de aplicaciones *web*, dentro de redes en un principio no fiables, *Networking* basado en directorio (802.1X EAP), etcétera.

La gestión de la identidad es especialmente importante para el proyecto ya que su objetivo es poder identificar digitalmente a los usuarios de una centralita telefónica o de un *callcenter* de manera inequívoca.

Solución técnica propuesta

Tal y como muestra la Figura 2, la solución técnica propuesta está formada por cinco elementos principales:

- Gestión de certificados digitales: Administra la infraestructura de certificados digitales de clave pública. Se utilizará la experiencia y garantías de una entidad certificadora que garantizará la autenticidad de las identidades de usuario.
- Gestión central de la telefonía: Ofrece toda la infraestructura de VoIP en sí misma. Permite realizar llamadas, redirigirlas, gestionar usuarios y buzones de voz, salas de conferencias y muchas otras opciones. Se comunica con la gestión de certificados digitales para garantizar la seguridad de los usuarios.
- Terminal telefónico *software* seguro: Este elemento es la innovación más importante del proyecto, ya que es el elemento que utiliza el usuario para utilizar los servicios de VoIP. Aporta una capa de seguridad extra entre el usuario y el servidor utilizando certificados para autenticar y cifrar las comunicaciones.
- Sistema de gestión de fraude: Permite hacer frente a posibles fraudes en el uso de los servicios de VoIP. Utilizando sistemas de reglas y modelos matemáticos, el sistema de gestión de fraude permite identificar comportamientos anómalos y, si es preciso, detener su uso.
- Protocolo de comunicación segura: La comunicación entre los distintos elementos del proyecto se realiza de forma segura, protegiendo las comunicaciones entre los distintos puntos del sistema.

Agradecimientos

Agradecemos su trabajo y colaboración al resto de los participantes del proyecto: IRONTEC, BZERO e IZENPE.

Eusko Jaurlaritzak diruz lagundutakoa

Subvencionado por el Gobierno Vasco

Figura 2

Diseño general del proyecto