Segunda Conferencia de Directores de Tecnología de Información, TICAL 2012
Gestión de las TICs para la Investigación y la Colaboración, Lima ,2 y 3 de Julio

Problemas y herramientas en la seguridad de redes de transmisión de datos universitarias. El caso de la Universidad Nacional de Cuyo.

Roberto Cutuli[1] Carlos Catania[2], Carlos García Garino[2,3]

[1] Centro Informático Tecnológico, [2] ITIC, [3] Facultad de Ingeniería
Universidad Nacional de Cuyo, Centro Universitario, 5500 Mendoza, Argentina
rcutuli@uncu.edu.ar, {ccatania, cgarcia@itu.uncu.edu.ar}

Resumen. Los desarrollos relacionados con las Tecnologías de la Información y las Comunicaciones, han dado lugar a una paulatina convergencia de redes de infraestructura y servicios de valor agregado. Esto plantea crecientes demandas a los administradores de las redes en general y por supuesto a los responsables de las redes universitarias. Sin embargo, los recursos muchas veces son escasos en términos de infraestructura o de recursos humanos para su despliegue, operación y administración. Por otro lado resulta necesario implementar de manera adecuada servicios y equipos para Educación a distancia; Repositorios Digitales o e-ciencia en general. En este contexto las comunicaciones constituyen un elemento central para la interacción de una universidad con otros centros de I+D, la sociedad y los integrantes de la comunidad. En particular, la telefonía IP juega un rol central las comunicaciones actuales y ha sido objeto de atención durante TICAL 2011. El trabajo presenta los antecedentes de telefonía IP en la Universidad Nacional de Cuyo, describe la infraestructura actual y discute un problema de seguridad relacionado con la misma. Se enfatiza la necesidad de contar con herramientas de seguridad habituales en las redes de datos, que quizás no son el foco de los administradores de sistemas telefónicos.

Palabras Clave: Telefonía IP; Redes de transmisión de datos; seguridad; integración de información

1 Introducción

La Universidad Nacional de Cuyo (UNCuyo) [1] es la más grande del centro oeste de Argentina con cerca de 4000 puestos de trabajos y múltiples enlaces hacia otras redes institucionales y la propia Internet.

En un trabajo anterior presentado en TICAL 2011 [2] los autores describieron las características de la red de la Universidad, se hizo énfasis en la seguridad de la misma y se analizaron diferentes herramientas de seguridad para la misma.

Además del tráfico de datos, típico de una red universitaria existen diferentes demandas como telefonía o servicios de valor agregado como Educación a distancia; Repositorios Digitales y también servicios relacionados con la e-ciencia que plantean nuevas necesidades y requisitos a los administradores de la infraestructura y servicios.

En este trabajo se presenta la infraestructura de telefonía IP, sus elementos y el impacto de la misma en la seguridad de la red.

El trabajo esta organizado de la siguiente manera: en la sección 2 se brinda un breve panorama acerca de la UNCuyo. En la sección 3 se presenta una síntesis de la red de la universidad. En la sección 4 se discuten la red de Telefonía IP. Finalmente, en la sección 5 se presentan las conclusiones de este trabajo.

2 La Universidad Nacional de Cuyo

La Universidad Nacional de Cuyo (UNCuyo) [1] se fundó en Mendoza, Argentina en 1939. Actualmente es la casa de estudios superiores más grande del centro oeste argentino. Originalmente sus unidades académicas estaban ubicadas en las provincias de San Luis, San Juan y Mendoza, las cuales conforman la región de Cuyo, de la cual proviene el nombre de la universidad. Desde 1973, año en que se crearon las Universidades Nacionales de San Luis y San Juan, la UNCuyo lleva a cabo su labor en la provincia de Mendoza

Actualmente conforman la Universidad 11 facultades, varias de ellas ubicadas fuera del campus e incluso algunas en ciudades lejanas. Un panorama completo de las actividades de la universidad puede verse en la referencia [1].

Actualmente cursan sus estudios de grado unos 38 mil estudiantes que alcanzan unos 50 mil si se suman los estudiantes de postgrado y los alumnos de los colegios secundarios de la universidad.

La UNCuyo posee una importante valoración social en Mendoza y su zona de influencia que se ha plasmado en el liderazgo y/o participación de diferentes emprendimientos asociativos: la Fundación Escuela de Medicina Nuclear (FUESMEN) pionera en Latinoamérica en Medicina por Imágenes; la Fundación del Instituto Tecnológico Universitario (FITU); el Instituto de Desarrollo Industrial, Tecnológico y de Servicios (IDITS) y el Instituto Balseiro en convenio con la Comisión Nacional de Energía Atómica (CONEA), así como relaciones con otras instituciones. Recientemente ha liderado la conformación de la Asociación de Universidades SurAndinas (AUSA) que reúne a distintas casas de estudios cercanas a la cordillera de los Andes.

El cúmulo de relaciones institucionales y académicas, conlleva importante actividad intrainstitucional (que se desarrolla en la distintas unidades académicas dentro o fuera del campus) y extrainstitucional, que en la práctica ha dado lugar a una compleja topología de red de transmisión de datos que se discute en la próxima sección.

3 La red de transmisión de datos. Topología y consideraciones de seguridad

La red de la Universidad Nacional de Cuyo posee unos 4000 puestos de trabajo conectados a la misma. Estos recursos están distribuidos a lo largo de la red que interconecta a las facultades e institutos dentro o fuera del campus Universitario. A estos equipos que hay que adicionarle al menos unos 100 servidores de los cuales la mitad están instalados sobre equipos físicos y los restantes están virtualizados. Una

descripción detallada de la misma puede verse en un trabajo previo de los autores presentado a TICAL 2011 [2]. En esta sección se presenta un esquema de la red a manera ilustrativa para contextualizar la infraestructura de telefonía que se discute en la sección 4.

En la figura 1 puede verse un esquema de la red de la universidad. La red interna del campus se basa en un esquema de interconexión tipo estrella, materializado por un switch. En cada unidad académica se dispone un router que se conecta de manera punto a punto al switch central mediante enlaces de fibra óptica en la mayoría de los casos. Desde el punto de vista de los protocolos de redes, se emplea IPV4 y se disponen redes privadas en cada unidad académica. Estas redes privadas se rutean dentro del campus. El switch central ya mencionado se conecta a un router central que administra los enlaces hacia el exterior.

Hacia el exterior la red tiene un complejo sistema de interconectividad con el mundo que está fuera del campus universitario al cual se puede acceder, como se observa en el gráfico de la figura 1, por más de un camino o enlace de red.

Existen varias conexiones a Internet con tecnología de fibra óptica. Mediante las mismas se provee conectividad a Internet 1 por intermedio de distintos ISP y también a Internet 2 a través del enlace a tal efecto provisto a la Red de Interconexión Universitaria (RIU) [3] que se basa en servicios brindados por InnovaRed [4]. RIU también provee a la UNCuyo, así como a las demás Universidades Nacionales servicios de I1 e I2, sobre la cual se ha implementado una red universitaria de telefonía IP.

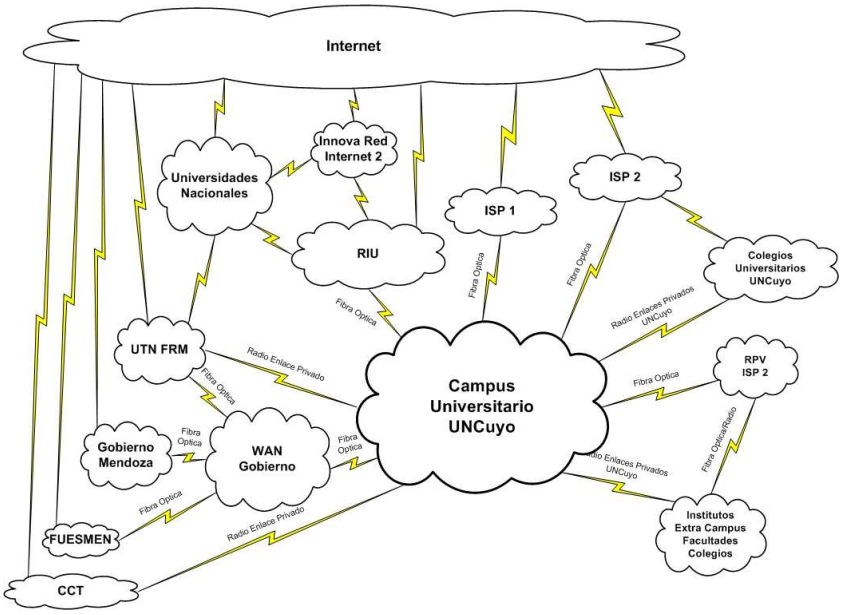

Fig. 1. Esquema de los enlaces de la Red de transmisión de datos de la Universidad Nacional de Cuyo.

4 El Proyecto de Telefonía IP en la UNCuyo

4.1 Antecedentes

En junio de 2010 se lleva a cabo en Buenos Aires la reunión anual de los representantes técnicos de las Universidades Nacionales de Argentina. Durante la misma se conforma un grupo de trabajo de VoIP liderado por el Ing. Mariano Martín y el Lic. Fernando Aversa de las universidades nacionales de Villa María y San Luis, respectivamente. Un resumen de los avances de la tecnología IP en la red de las Universidades Nacionales de Argentina puede verse en un trabajo de Martín y Aversa [5] presentado en TICAL 2011. En la reunión citada se pone en marcha un proyecto para integrar la telefonía de todas las Universidades Nacionales Argentinas mediante telefonía IP y centrales basadas en Asterisk [6].

A partir de la iniciativa descrita en la UNCuyo se decide implementar un prototipo de central Asterisk con la distribución Elastix [7], Se seleccionó esta distribución por razones de confiabilidad, amplio uso y porque además ofrece un entorno de administración web, que constituye una interfaz amigable para mantener y administrar el sistema de telefonía IP. Durante la implementación se contó con la colaboración del Ing. Miguel Morandi de la Universidad Nacional de San Juan, que contaba con mucha experiencia en el tema.

A manera de experiencia inicial se instaló la distribución Elastix sobre un equipo personal bajo una plataforma virtualizada con Virtual Box [8], mediante la versión 2.0.3 de 32 bits. Posteriormente se vinculó este Elastix a la PBX Asterisk de RIU, se verificó el funcionamiento y las nuevas posibilidades del sistema de VoIP.

Posteriormente se decidió escalar la instalación a una plataforma virtual en producción, para lo cual se utilizó el sistema operativo huésped de virtualización utilizado PROXMOX [9], el cual ofrece un entorno de administración web para virtualización con KVM [10] u OpenVZ [11].

De esta manera se instala la primer central Asterisk de la UNCuyo, utilizando una distribución Elastix 20.3 de 64 bits sobre un servidor virtualizado con KVM. Esta central se vincula a la central principal de RIU, que a su vez conecta a todas las centrales de VoIP Universitarias. La interconexión de estas centrales se realiza a través de una VPN [12], la cual brinda un esquema de seguridad en la interconexión de las centrales y privacidad en las comunicaciones de voz realizadas entre ellas. En la figura 2 se muestra un esquema del estado de la red de VoIP de las Universidades Nacionales en el momento de las pruebas descritas.

4.2 Integración de la Red Telefónica tradicional con la Telefonía IP

Una vez resuelta la meta inicial de vincular a la UNCuyo con el resto de las Universidades Nacionales mediante enlaces y equipos de telefonía IP y contar con el correspondiente plan de numeración de prefijos, surgió naturalmente la posibilidad de integrar la red de VoIP con la red de telefonía *tradicional*. La misma se escribe en cursiva porque proviene de la red de telefonía analógica como en la mayoría de las instituciones, pero se basa en tecnología híbrida. La red telefónica de la UNCuyo se

basa en un sistema Alcatel Omni PCX [13] el cual ofrece telefonía IP híbrida y propietaria de la marca. Para vincular la red de telefonía IP con la central Alcatel, se implementa un segundo equipo Elastix que hace las veces de pasarela entre ambas redes. Este equipo se conecta mediante un enlace SIP [14] con la red de VoIP y mediante una tarjeta tipo E1 con la central Alcatel, como se muestra en la figura 3. Es importante resaltar que este equipo *intermediario*, funciona sobre un equipo real (no virtualizado), ya que de esa manera se le pudo instalar una tarjeta E1 "Digium" con la cual se materializa el enlace con la central Alcatel. A su vez todos los equipos se vinculan a la central Asterix de ARIU mediante un enlace troncal SIP montado sobre el VPN de RIU, como se muestra en la figura 3.

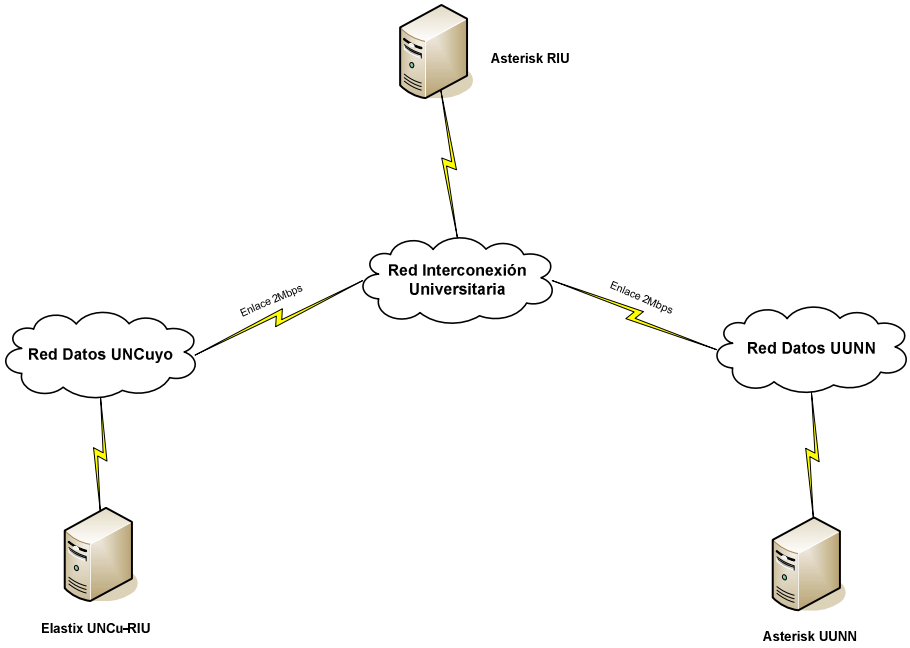

Fig. 2. Esquema de la red de VoIP de las Universidades Nacional y la conexión inicial de la Universidad Nacional de Cuyo.

En resumen, la arquitectura descrita, y que se muestra en la figura 3, comprende:
1. Una central Asterisk que se interconecta con el Asterisk de RIU (UNCu-RIU)
2. Otra central Asterisk que se hace las veces de gateway entre ambas redes (Telefonía IP y tradicional) y que se interconecta con la central Alcatel (UNCu-Alcatel)
3. Un enlace troncal SIP que interconecta ambos Asterisk.

La arquitectura planteada brinda las siguientes facilidades:
A. Realizar llamadas desde el exterior de la UNCuyo a cualquier interno en la central Alcatel. Esta comunicación se materializa por medio de la red IP de la RIU. Las mismas puede provenir de otra Universidad Nacional conectada al sistema de

telefonía IP de las UUNN o bien de cualquier Universidad de Latino América que esté vinculada a la central de VoIP de RedClara [15].
B. Efectuar llamadas desde cualquier interno telefónico de la central Alcatel hacia alguna otra Universidad conectada al sistema de VoIP-RIU o a cualquier terminal IP conectada a una de las centrales asterisk de la UNCuyo.

Con esta configuración se vincula cualquier dispositivo de telefonía tradicional con otro dispositivo IP, ya sea un teléfono IP estándar, un SoftPhone corriendo en una PC u otro dispositivo como un Smartphone, un dispositivo ATA, un equipo de VideoConferencia que soporte SIP, etc.

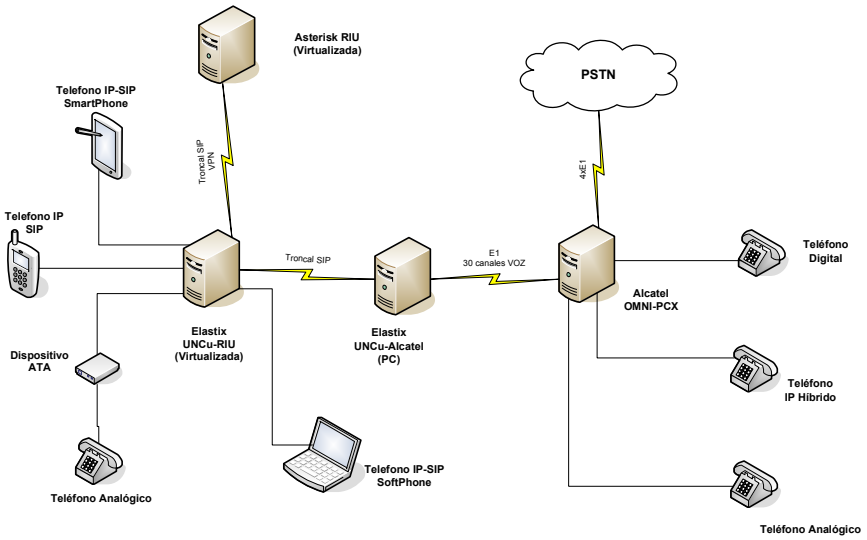

Fig. 3. Esquema de la red de telefonía IP de la Universidad Nacional de Cuyo y sus conexiones con la red telefónica *tradicional* y la red de la RIU.

4.3 Extensión para integrar equipos remotos de VoIP

El siguiente paso fue brindar acceso a teléfonos inteligentes o equipos PC móviles con software de cliente VoIP para que los mismos, convenientemente configurados, pudieran acceder en forma remota desde cualquier ubicación de Internet al sistema telefónico de la UNCuyo descrito en la sesión anterior. Con este propósito se instala una tercera central Asterisk (UNCu-Internet) sobre un servidor virtual y se interconecta a las otras dos centrales Asterisk mediante sendos troncales SIP, como se muestra en la figura 4 que representa la arquitectura actual del sistema telefónico de la universidad. De esta manera se tienen sendos vínculos de interconexión hacia: a) el interior de la UNCuyo por intermedio del Elastix conectado a la central Alcatel; b) a las otras Universidades Nacionales a través del Elastix conectado a RIU, y c) a los

usuarios que acceden desde sitios remotos por medio de este último Elastix con visibilidad desde Internet.

La arquitectura descrita, basada en tres servidores Asterisk independiza la función de cada uno de ellos evitando que todo el trabajo del sistema de VoIP se ejecute en un servidor único, con lo cual se obtiene mayor robustez e independencia.

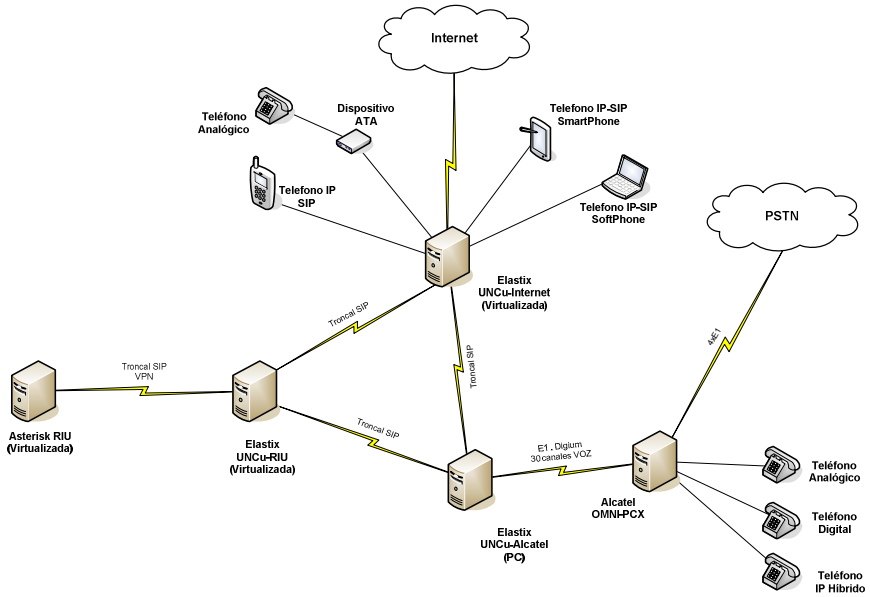

Fig. 4. Esquema actual de la red de telefonía de la Universidad Nacional de Cuyo materializado mediante la central Alcatel, los equipos Asterisk y los enlaces de VoIP y hacia la Red de Telefonía Publica (PSTN).

Como se observa en el esquema de la figura 4, cada equipo Asterisk de la red telefónica de la UNCuyo tiene una función determinada de acuerdo al siguiente detalle:

1. Elastix UNCu-RIU (Virtual): provee la interconectividad entre el sistema de VoIP de las Universidades Nacionales y el de la UNCuyo por medio de la VPN montada sobre la red RIU de las UUNN y el servidor Asterisk instalado en el datacenter de RIU.
2. Elastix UNCu-Alcatel(PC): provee la conectividad entre el sistema de telefonía tradicional (Alcatel Omni PCX) y el sistema VoIP (Asterisk/Elastix) interior y exterior a la UNCuyo.
3. Elastix UNCu-Internet(Virtual): Contiene la configuración y administra el acceso de los teléfonos de VoIP pertenecientes a la UNCuyo, este servidor provee la conexión de los terminales estén dentro de la red de la UNCuyo.

5 Un caso de análisis relacionado con la seguridad

5.1 Contexto del incidente

La PBX asterix (UNCu-Internet) es un equipo expuesto a internet y por ende factible de sufrir ataques y amenzas, las cuales son relativamente comunes.

En la PBX asterisk (UNCu-Alcatel) se incluyó un modulo de freepbx [16] llamado Outbound Route Permissions, el cual permite seleccionar rutas salientes de marcado. En este caso cuando se marca un número celular, o un número fijo ya sea local, o de larga distancia nacional o internacional, se toma la trama que interconecta la central Alcatel y el Asterisk (UNCu-Alcatel). La central Alcatel procede de inmediato a marcar el número solicitado. Muy pocas extensiones tienen habilitada esta facilidad de acuerdo a la configuración de las centrales. Es importante señalar que el módulo Outbound Route Permissions es, a la vez, tan útil como riesgoso ya que brinda una funcionalidad excepcional de marcado pero conlleva de poder realizar llamadas sin límites de destino ni tiempo si se hace un mal uso de la misma.

Es importante destacar, para completar el contexto de la situación, que en el mes de marzo de 2012 se comunicó una vulnerabilidad de seguridad en el paquete de FreePBX, informada en http://www.exploit-db.com/exploits/18649/, la cual hace posible realizar una ejecución remota de comandos con los privilegios de root .

5.2 Descripción del problema

El sector de administración y mantenimiento de la central telefónica Alcatel y responsable de los servicios de conexión de la UNCuyo a la red de telefonía pública (PSTN) recibe una comunicación del proveedor del servicio de acceso a la PSTN, en la cual le informa que se había procedido a bloquear el marcado por DDI (Discado Directo Internacional) desde la UNCuyo ya que había advertido un número inusual de llamadas internacionales desde adentro de la universidad hacia países no registrados en el patrón de tráfico habitual. Más aun, los mismos se habían realizado en horarios nocturnos o de madrugada y días feriados.

5.3 Estudio del incidente

Con el fin de conocer el origen del problema planteado, se analizaron los registros de la central Alcatel. De los mismos surgió que las llamadas habían entrado desde la trama que conecta a la central Asterisk (UNCu-Alcatel) con la central Alcatel. Como se señaló en la subsección 5.1, de esta manera un terminal registrado en la central Asterisk, puede tomar canales de la central Alcatel y marcar cualquier número de la red PSTN, y acceder así a destinos locales, nacionales e internacionales.

Del estudio de los registros, también surgió que se realizaron ataques por fuerza bruta para obtener tanto el número de extensión, así como la correspondiente contraseña para autenticar la misma y así acceder libremente a todo tipo de destinos.

Mediante el ataque detectado se logró que cualquier extensión pudiera utilizar el módulo “OutBound Route Permissions” que permite efectuar llamadas la PSTN sin ningún tipo de restricciones.

5.2 Recomendaciones de Seguridad

En la literatura se pueden consultar algunos trabajos relacionados con la seguridad y la telefonía IP [17],[18],[19]. A continuación se proponen algunas medidas que pueden ayudar a paliar los problemas de seguridad a los cuales se está expuesto:

1. Cerrar los puertos que sean innecesarios.
2. Cambiar el puerto 5060 donde escucha el Asterisk por omisión. Los botnet siempre escanean ese puerto en búsqueda de extensiones con claves débiles.
3. Eliminar las combinaciones de números de extensión/contraseña que sean obvias, por ejemplo 100/100 tampoco servirá utilizar 100100 como contraseña.
4. Comprobar en los registros del log del Asterisk los intentos fallidos de autenticación y en el caso de varios intentos, añadir de forma automática con IPTables [20] la dirección IP del ‘supuesto’ atacante, esto puede efectuarlo automáticamente el paquete fail2ban [21].
5. Es imprescindible automatizar la actualización de las reglas de IPTables, ya que los ataques suelen producirse cuando el sistema es más vulnerable: durante la noche o los fines de semana. Consecuentemente no se revisan los logs del sistema hasta que el administrador de sistemas retome su trabajo. El sistema de la UNCuyo fue atacado durante la noche y un fin de semana.
6. Revisar periódicamente los registros log. Asterisk loguea los intentos fallidos de registro SIP en mensajes de tipo NOTICE (algo que viene por omisión en el logger.conf y permite monitorizar quien se ha intentado registrar casi siempre).
7. Configurar una VPN para que las extensiones remotas que deben acceder y autenticarse a través de Internet lo hagan de forma segura por medio de la VPN.
8. Del lado de la configuración de Asterisk para la forma de efectuar un marcado hacia la PSTN, introducir un código PIN para marcar la salida hacia la PSTN, limitar la longitud total del número a marcar, configurar los prefijos permitidos rechazando los que no estén permitidos, limitar el tiempo de la llamada.

6 Conclusiones

La situación descrita corresponde típicamente a un compromiso entre riesgos y beneficios. En este caso concreto entre la necesidad de brindar acceso remoto (debidamente controlado) al sistema telefónico de la universidad y la facilidad de uso de dicho acceso.
De las consideraciones de la sección 5 surge que fallaron distintos componentes del sistema, que posiblemente no hubieran conducido al problema descrito si no se hubiera verificado la simultaneidad de los inconvenientes.
Muy posiblemente suceda que los encargados del sistema telefónico no valoren en su totalidad la herramienta que conforma una central de telefonía IP como las implementadas con Elastix / Asterix, como es el cuál es el caso de la central Asterisk

UNCU-Internet. Una vez violado el sistema, el acceso al mismo se puede efectuar mediante un dispositivo ATA, un SoftPhone, un SmartPhone, una terminal telefónica IP(SIP), etc.

Referencias

1. Reseña Histórica de la UNCuyo: http://www.uncu.edu.ar/paginas/index/resena-historica.
2. R. Cutuli, C. Catania y C. García Garino: Problemas y herramientas en la seguridad de redes de transmisión de datos universitarias. El caso de la Universidad Nacional de Cuyo. TICAL 2011.
3. Red de Interconexión Universitaria Argentina: www.riu.edu.ar.
4. InnovaRed, Red Nacional de Educación e Investigación en Argentina: www.innova-red.net.
5. M. Martín, F. Aversa: Tecnología de voz sobre IP aplicada a la integración de plataformas de telefonía en instituciones académicas públicas de Argentina. TICAL 2011
6. Asterisk: www.asterisk.org
7. Elastix: www.elastix.org
8. Virtual Box: www.virtualbox.org
9. PROXMOX: www.proxmox.com
10. KVM: http:// http://www.linux-kvm.org
11. OpenVZ: http://wiki.openvz.org
12. Redes Privadas Virtuales (VPN): http://openvpn.net
13. Alcatel: www.alcatel-lucent.com
14. Protocolo de Inicio de sesión (SIP): http://www.voip-info.org/wiki/view/SIP
15. Red Cooperación Latinoamericana de Redes Avanzadas (Clara): www.redclara.net
16. Freepbx: www.freepbx.org
17. Voice over IP. Decipher and decide. KPMG, 2004
18. R. Gutiérrez Gil: Seguridad en VoIP. Ataques, Amenazas y Riesgos. Universidad Politécnica de Valencia
19. H. Magnago, J.Aguirre y R. Prat: Planificación de Seguridad en VoIP. Departamento de Telecomunicaciones, Facultad de Ingeniería, Universidad Nacional de Río Cuarto.
20. IPTables: http://www.netfilter.org/projects/iptables/index.html
21. fail2ban: http://www.fail2ban.org