Ingeniería y Competitividad
ISSN: 0123-3033
inycompe@gmail.com
Universidad del Valle
Colombia

Baluja-García, Walter; Anías-Calderón, Caridad
Amenazas y defensas de seguridad en las redes de próxima generación
Ingeniería y Competitividad, vol. 8, núm. 2, 2006, pp. 7-16
Universidad del Valle
Cali, Colombia

Amenazas y defensas de seguridad en las redes de próxima generación

Walter Baluja-García* §, Caridad Anías-Calderón*

** Departamento de Telemática, Facultad de Ingeniería Eléctrica,*
Instituto Superior Politécnico "José Antonio Echeverría" (ISPJAE), Cuba
§ e-mail: walter@tesla.cujae.edu.cu

(Recibido: Febrero 23 de 2006 - Aceptado: Septiembre 27 de 2006)

Resumen

El advenimiento de las redes de próxima generación (NGN) es una realidad en el desarrollo de las telecomunicaciones. Si bien su introducción constituye un salto tecnológico, también representa un enorme reto desde el punto de vista de la seguridad. El presente artículo realiza un análisis integral sobre aspectos relacionados con la seguridad de estas redes. Inicialmente, se abordan las amenazas que se heredan de las redes telefónicas públicas conmutadas (PSTN), las redes de datos de protocolos de *Internet* (IP) y las redes de televisión, así como la forma en que éstas se combinan, para obtener las amenazas propias de las NGN. Luego, se analizan los mecanismos de defensa de las redes que convergen en las NGN para proponer los mecanismos de defensa aplicables a estas últimas, los principios de su combinación, así como los requerimientos de las herramientas de seguridad. El análisis presentado constituye un importante primer paso para organizar y hacer homogéneo el trabajo de seguridad en NGN.

Palabras clave: NGN, Telecomunicaciones, Seguridad, Amenazas de seguridad, Mecanismos de defensa.

Threats and security defense of next generation networks

Abstract

The coming of Next-Generation Networks (NGN) is a reality in the development of telecommunications. Although their introduction represents a technological jump, it also poses an enormous challenge from the security standpoint. In this article, an integral analysis is carried out on some aspects related to the security of those networks. First, the threats that are inherited from traditional public switched telephone networks (PSTN), Internet protocol (IP) data, and television networks are discussed together with the way in which they combine to obtain the characteristic NGN threats. Second, defense mechanisms of traditional networks are analyzed to propose defense mechanisms that can be applied to NGN. Also, the principles of NGN defense mechanism combination and the requirements of the corresponding security tools are considered. The analysis given here represents an important first step to organize and homogenize NGN security work.

Keywords: NGN, Telecommunications, Security, Security threats, Defense mechanisms.

1. Introducción

El mundo de las telecomunicaciones ha sufrido una transformación radical en la última década propiciada por circunstancias entre las que se destacan la competencia abierta entre operadores debido a la desregulación del mercado, la explosión del tráfico digital, el dominio del tráfico de datos (Pillado-Ortiz, 2000) y el incremento de la demanda de los usuarios por nuevos servicios *multimedia* y por una movilidad generalizada. Ante este cambio aparece un nuevo concepto, las redes de próxima generación (NGN), que pueden abarcar una variedad de protocolos, servicios y medios de comunicación (Solem & Zouganeli, 2004).

Las NGN unifican las redes telefónicas públicas conmutadas (PSTN), las redes de televisión y las de datos, creando una única red multiservicio de plataforma *Internet Protocol* (IP).

El advenimiento de las NGN significa un enorme y necesario avance y, a la vez, un reto de igual magnitud para el trabajo de seguridad en las redes de telecomunicaciones. Estudiar las amenazas y mecanismos de defensa para la seguridad de las NGN, permitirá alcanzar una idea bastante exacta de hacia dónde dirigir los esfuerzos en el desarrollo de implementaciones de seguridad. El presente artículo realiza un análisis sobre estos aspectos y sirve de base a futuros trabajos asociados con la seguridad en las NGN.

2. Características principales de las NGN

Entre las características fundamentales de las NGN se encuentran (SG13, 2004a) las siguientes:

• Transferencia basada en paquetes.

• Separación de las funciones de transporte y las de servicio. Desarrollo de servicios a través de interfaces abiertas.

• Soporte de un amplio rango de servicios y aplicaciones (tiempo real, *streaming* y *multimedia*).

• Capacidad de banda ancha con calidad de servicio (QoS) extremo a extremo.

• Trabajo integrado con redes precedentes (PSTN y otras) a través de interfaces abiertas.

• Movilidad generalizada. Se refiere a la movilidad de usuarios y dispositivos a través de diferentes tecnologías de acceso sin interrupción del servicio.

• Acceso de los usuarios a servicios ofrecidos por diferentes proveedores.

• Variedad en los esquemas de identificación de usuarios y dispositivos.

• Trabajo con un mismo perfil de servicio para un usuario a través de toda la red.

• Convergencia de los servicios fijos y móviles.

• Soporte de múltiples tecnologías de última milla.

• Cumplimiento de todos los requerimientos regulatorios (comunicaciones de emergencia, seguridad, intercepción legal y otros).

En las NGN, las entidades funcionales que controlan las políticas, sesiones, medios, recursos, servicios, seguridad y otros, están distribuidas en toda su infraestructura. Dichas entidades se comunican a través de interfaces abiertas. La comunicación entre las redes de diferentes operadores NGN, y entre redes NGN y redes precedentes, se realiza a través de pasarelas (o *gateways*) .

3. Tendencias en los servicios y aplicaciones

La separación de las funciones de transporte y servicios (SG13, 2004b), tal y como ocurre en las NGN, permite desarrollar estos últimos de forma independiente de las consideraciones de transporte y conectividad (Crimi, 2001). Este entorno abierto, basado en API (*Application Programming Interface*) y en otros sistemas intermediarios, ofrece a los proveedores de servicios, a terceras partes desarrolladoras y clientes avanzados, la posibilidad de crear e introducir aplicaciones de forma rápida y transparente.

En este escenario, las plataformas de servicios utilizan IP como protocolo base, ofreciendo diversas alternativas a los usuarios como:

• Servicios de voz que incluyen mensajería y telefonía.

• Servicios de datos (correo electrónico, *web*, intercambio de archivos y otros).

•Servicios de video (televisión, video en demanda [VOD] y otros).

• Combinación de los servicios anteriores (juegos interactivos, video-telefonía y otros).

4. Amenazas para las NGN, provenientes de los sistemas tradicionales de telefonía

Tradicionalmente, los servicios telefónicos son de tres tipos: telefonía fija, pública y móvil. Las modalidades de fraudes sobre estos servicios son cada vez más sofisticadas (Fumero-Paniagua, 2000), constituyendo amenazas al correcto funcionamiento de los mismos y provocando pérdidas millonarias.

Algunas de las manifestaciones de fraude que pueden encontrarse en varios de los servicios telefónicos son:

• **Suscripción:** cliente que solicita un servicio sin intenciones de pagar. Desde el instante en que se activa la cuenta se realizan numerosas llamadas nacionales e internacionales (Jacobs, 2004).

• **Servicios prepagados:** usurpación de códigos de prepago por parte de los defraudadores (perpetradores de fraude). Para esto se utilizan técnicas como la observación visual, la colocación de cámaras ocultas, robos de tarjetas y otros (Cerebrus Solutions, 2002). Típicamente se comercializan los códigos obtenidos.

•**Servicios de tasas de premios (PRS):** los proveedores de estos servicios realizan contratos con las operadoras y reciben ganancias por el número de llamadas telefónicas que inyectan a la red. En ocasiones llegan a provocar llamadas desde el servicio de un usuario, sin que este lo sepa (Jacobs, 2004).

También existen fraudes distintivos de cada tipo de servicio telefónico como son:

• ***Clip-On*** **(telefonía fija):** también se le conoce como robo o desvío de línea. Para realizar este fraude se coloca una conexión paralela con la línea del suscriptor, o se deshabilita el servicio del usuario legítimo.

•***Bypass*** **(telefonía fija)**: se basa en introducir tráfico internacional a la red telefónica nacional por una vía alternativa como líneas arrendadas, conexión a *Internet* (voz sobre IP) o por satélite.

• **Cajas rojas (telefonía pública):** mecanismo que simula los tonos de frecuencia que emite el teclado al comunicarse con el centro de conmutación, logrando evadir la facturación.

•**Abuso de los monederos (telefonía pública):** uso de monedas falsas, violación del mecanismo de recepción de la moneda y otros.

•***Roaming*** **(telefonía móvil):** los defraudadores explotan las demoras que existen en los procesos de activación de cuentas e intercambio de información de facturación cuando se efectúa el roaming entre redes (Cerebrus Solutions, 2002). De esta forma evaden, por pequeños períodos de tiempo, los limites establecidos en el uso de los servicios.

• **Clonado (telefonía móvil):** proceso de replicar el *hardware* o *firmware* de un cliente para emplear sus servicios. El cliente legítimo no conoce del hecho hasta que no recibe la factura sobrecargada (Jacobs, 2004).

5. Amenazas para NGN heredadas de las redes de datos IP

La siguiente lista aunque no exhaustiva si es representativa de las amenazas existentes en las redes de datos IP (Gamm et al., 2001):

• **Denegación de servicio (*Denial of Service*, [DoS]):** consiste en agotar los recursos de la red, de forma tal que no exista disponibilidad de estos y de los servicios que ofrecen. Un caso particular lo constituyen los ataques DDoS (*Distributed DoS*).

• **Escucha clandestina (*sniffing*):** es un ataque contra la confidencialidad del sistema. En este se intercepta la comunicación entre dos o varios elementos de la red.

• **Usurpación o robo de identidad (*spoofing*)**: consiste en ocupar una identidad falsa, ya sea una cuenta de usuario, el campo de remitente de un mensaje, una dirección IP, un sitio *web* (empleado para cometer *phishing*) u otra forma de identificación.

• **Acceso no autorizado:** viola la política de seguridad relacionada con el acceso. Casi siempre está relacionada con otro de los ataques.

• **Modificación de la información:** los datos son alterados, corrompidos e incluso inutilizados. Es un ataque contra la integridad de la información.

• **Ataques físicos a la infraestructura de las redes:** provocan daños físicos a los medios tecnológicos ya sean servidores, equipos de conectividad, terminales o cableado.

Las anteriores son amenazas directamente ligadas a la ejecución de fraude. No obstante, existen otras que afectan el funcionamiento de la red y la disponibilidad de sus servicios, como son las siguientes:

• **Programas malignos:** provocan el mal funcionamiento de las redes, los servicios y los sistemas operativos de las computadoras. Se han registrado pérdidas millonarias por esta causa.

• **Ataques de *spam*:** consiste en la emisión de una enorme cantidad de mensajes de correo con contenido de promoción comercial y otros, que repletan los buzones, cogestionan canales y molestan a los usuarios.

Puede añadirse que muchas soluciones de control y gestión se desarrollan sobre sistemas operativos de propósito general, cuyas deficiencias de seguridad son conocidas por los intrusos. Además, hay que tomar en consideración las debilidades de la familia de protocolos base (TCP/IP), las cuales son la causa de muchas de las amenazas antes comentadas (Bellovin, 2004; Siles-Peláez, 2002).

6. Combinación de amenazas

Puede afirmarse que la combinación de las amenazas provenientes de las redes de datos y de las PSTN, constituyen la principal fuente de amenazas de las NGN, teniendo en cuenta las características de este tipo de redes (Figura 1).

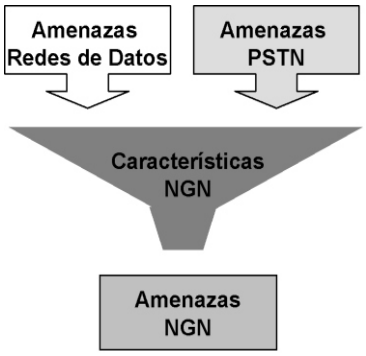

Figura 1. Factores que dan lugar a las amenazas de seguridad en las NGN.

Esto no excluye, aunque se consideran de menor aporte, los problemas de seguridad que se arrastran de los servicios de televisión. La expresión más notable de estos problemas de seguridad es la ruptura y clonación de códigos de las tarjetas inteligentes que proporcionan acceso a los servicios de TV por satélite o cable.

7. Amenazas de seguridad en las NGN

Algunas de las amenazas que aquí se mencionan se están materializando en las primeras implementaciones de NGN; el resto debe ir apareciendo con la generalización de esta tecnología.

Si bien el aporte de amenazas que hacen los servicios de televisión tradicionales a las NGN es menor que el de las redes de datos y las PSTN, la repercusión de las amenazas a los servicios de video en NGN es enorme. Precisamente alrededor de estos servicios se encuentran muchas de las facilidades que ya están exigiendo los usuarios y, por tanto, está centrada buena parte de las ganancias que ofrecerá NGN a operadores de telecomunicaciones, proveedores de servicios y fabricantes de equipamiento. En este entorno, las amenazas se dirigen a los servicios de IPTV

(televisión sobre IP), VOD y otros (Ramírez, 2005).

Teniendo en cuenta lo analizado hasta aquí, se encuentra un grupo importante de amenazas de seguridad para las NGN:

• Los programas malignos más frecuentes serán los troyanos, gusanos y combinaciones de estos. Van a ser utilizados en cuatro direcciones fundamentalmente:

• Apoderarse de información de identificación y configuración de terminales, dispositivos y usuarios.

• Provocar llamadas o solicitudes de servicios sin el conocimiento del usuario autorizado (especie de fraude PRS).

• Lanzar algunas de las variantes de ataques DoS, mediante la inyección de tráfico inservible y la modificación/destrucción de la información del elemento afectado (terminal de usuario, servidores, dispositivos de conectividad).

• **DoS**: dirigidos fundamentalmente a elementos de soporte de la infraestructura de gestión y de control de la red como *softswitch*, servidores NAT (*Network Address Translation*), servidores *multimedia*, infraestructura de contabilidad y facturación, dispositivos de entrada en la conectividad doméstica, entre otros.

• ***Spam*:** este ataque tendrá manifestaciones adicionales a las tradicionales avalanchas de mensajes de correo, y similares a esta. Este es el caso de los mensajes de correo de voz o llamadas telefónicas indeseables (*spit*), las avalanchas de mensajes instantáneos (*spim*) y las "interferencias" de video (*spiv*).

• **Escucha ilegal:** en este caso los ataques estarán dirigidos hacia donde las soluciones de confidencialidad son más débiles, y a los puntos de escucha establecidos legalmente. Debe tomarse muy en cuenta la debilidad de las transmisiones inalámbricas indebidamente protegidas.

• **Robo de identidad**: las características de ubicuidad de NGN hacen este ataque muy atractivo para los intrusos. Incluye variantes de los fraudes clásicos de suscripción, PRS, servicios prepagados, *clip-on* y clonado (este último en servicios de telefonía y video). Los programas malignos, los husmeadores (*sniffers*), la observación visual de la víctima, la ingeniería social y otros, van a ser herramientas muy utilizadas para el robo y suplantación de identidad.

• **Robo de la propiedad intelectual:** esta constituye una de las amenazas más preocupantes en el caso de los servicios de video y de multimedia en general (Ramirez, 2005).

• Variantes de *bypass*, *clip-on* y otros, que pueden surgir del empleo mal intencionado del encapsulado de paquetes en la telefonía IP.

Puede añadirse que la base IP de las NGN, el trabajo a través de interfaces abiertas, la distribución de las tareas de control y gestión, el amplio desarrollo de QoS, la ubicuidad de la red, entre otros, solo pueden hacerse realidad a partir de una alta componente de software. Esto introduce una gran cantidad de problemas de seguridad de mayor magnitud que en redes precedentes, debido a los índices de disponibilidad, fiabilidad, entre otros, que requieren las NGN.

En sentido general se consideran puntos estratégicos para los intrusos los terminales de usuario (teléfonos, computadoras, equipos domésticos, y otros), los dispositivos de gestión y control, los medios de comunicación, los servidores y la infraestructura de dispositivos de identificación-resolución de usuarios.

8. Mecanismos de defensa en los sistemas tradicionales de telefonía

Además del avance que han representado la digitalización y diferentes medidas de seguridad física aplicadas en equipos y terminales, el mecanismo de defensa por excelencia para los servicios tradicionales de telefonía es el sistema de gestión de fraudes (*Fraud Management System* [FMS]).

La gestión de fraudes abarca la recolección, correlación, análisis, interpretación y diseminación de información con el propósito de prevenir, detectar e investigar posibles actos fraudulentos (Larrazábal, 2004).

En los casos de operadores medianos y grandes, los FMS trabajan con millones de CDRs (*Call Details Records*) diarios y realizan diferentes tareas de procesamiento sobre estos.

Es común que existan enlaces entre los FMS y otros sistemas de información de los clientes, como es el estado de sus cuentas con el operador. Incluso, los FMS más potentes, poseen módulos para valorar nuevas cuentas o solicitudes y la explotación que los nuevos clientes hacen del servicio.

9. Mecanismos de defensa de las redes de datos IP

En las redes de datos IP existe un amplio grupo de mecanismos de defensa. Una lista de las soluciones tecnológicas más importantes sería (Baluja-García, 2002):

• **Cortafuegos:** sistema compuesto por elementos diversos como servidores *proxy*, filtrado de paquetes y otros. Define una zona confiable por donde circulan los datos entre dos o más redes diferentes.

• **Criptografía:** a menudo se considera la mejor solución para los problemas de seguridad. Agrupa soluciones que permiten proteger la confidencialidad, la integridad y la autenticidad de la información. Se utiliza en diversas aplicaciones: el envío y firma del correo electrónico, el comercio electrónico, la navegación *web*, el almacenamiento de información y otros.

• **Sistemas antivirus:** herramientas vitales para la detección y eliminación de programas malignos. Deben revisar toda información almacenada, transmitida o procesada por un dispositivo o red.

• **Sistemas de detección y de prevención de intrusiones (IDS/IPS):** herramientas con cierta inteligencia que automatizan la detección y/o prevención de intentos de intrusión en una red de computadoras. Pueden proteger una red completa, una zona de la red o un host en particular.

• **Monitores de seguridad:** también conocidos como detectores de vulnerabilidades. Se utilizan para detectar los servicios que ofrecen los diferentes dispositivos de red y verificar si estos son vulnerables. Constituyen una herramienta fundamental en los diagnósticos de seguridad (*Penetration Test*) que se realizan para comprobar los niveles de seguridad de las redes o sistemas.

•**Herramientas de trabajo forense:** permiten la localización, recolección, conservación y análisis de la evidencia digital ya se trate de crímenes informáticos o no. Su empleo está restringido a personal especialmente capacitado y autorizado.

10. Mecanismos de defensa para las NGN

A partir de la fusión en las NGN de los servicios de datos, video y voz con una base IP, es necesaria una combinación de mecanismos de defensa donde predominen aquellos que provienen de las redes de datos: antivirus, cortafuegos, cifrado de contenidos, certificados digitales, IDS, IPS y muchos otros.

Muchos especialistas señalan a IPv6 como una solución (TISPAN, 2005), no solo a los problemas de direccionamiento y apoyo a la QoS de las redes, sino a los problemas de identificación del origen y del cifrado de la información que transporta, y las debilidades que en general posee Ipv4.

Ante la escucha ilegal se acude principalmente a las soluciones de criptografía. En esta área se destaca el avance en la aplicación y desarrollo de las llamadas VPN (*Virtual Private Networks*), en particular su aplicación sobre MPLS (*Multi-Protocol Label Switching*) lo que permite obtener un red privada multipunto en el nivel de transporte de las NGN (Mampaey & Paridaens, 2005). También se trabaja con soluciones basadas en SSL (*Secure Socket Layer*) y TLS (*Transport Layer Security Protocol*).

La criptografía también juega un papel muy importante en la seguridad de los servicios de video a través de diferentes mecanismos como los

sistemas de acceso condicional (*Conditional Access Systems* [CAS]), los sistemas de protección de contenidos (*Content Protection Systems* [CPS]) y la gestión de derechos digitales (*Digital Rights Management* [DRM]) (Ramirez, 2005).

Las NGN requieren del fortalecimiento de los algoritmos, protocolos y sistemas criptográficos. En este sentido deben considerarse los resultados de las investigaciones y aplicaciones de la llamada criptografía cuántica, y de los sistemas cifradores de información basados en caos, o cifradores caóticos.

En los casos de soluciones de cifrado, como las comentadas anteriormente, debe disponerse de una infraestructura de distribución de claves (PKI) eficiente y segura. Además, tienen que tomarse en cuenta las orientaciones y leyes de los estados en cuanto al uso de estas soluciones. De otra forma, los controles que se establecen para mantener la seguridad nacional, en cada país, se dificultarían y encarecerían demasiado (Lintao, 2005).

Por otra parte, los ataques DoS a los canales de voz, video y datos, podrían mitigarse con técnicas de QoS siempre que los elementos que las proveen (por ejemplo, enrutadores [*routers*]) no caigan ellos mismos bajo los efectos de estos ataques (Huitema, 1999; Garg & Reddy, 2002). Esta idea de combinar QoS y seguridad, más específicamente de utilizar las herramientas de QoS para mejorar la seguridad, es abordada por diferentes especialistas y fabricantes (Wexler, 2004; Davis, 2005), y debe adquirir gran importancia en las redes del futuro.

La dependencia que las NGN tienen del *software*, la herencia de implementaciones inseguras, y la actividad de los intrusos, hace pensar que las actualizaciones o parches formarán parte de las soluciones de seguridad por mucho tiempo. No obstante, debe velarse porque todas las aplicaciones que se desarrollen y los servicios y sistemas que se implanten, cumplan con requisitos de programación y funcionamiento seguro y fiable. Entre otros, el empleo del paradigma AAA (*Authentication*, *Authorization*, *Accounting*) debe estar garantizado.

Especial interés debe prestarse a las soluciones de seguridad para *web* porque resulta evidente la tendencia de las aplicaciones a utilizar este tipo de tecnología. Así mismo, es necesario evitar el empleo de sistemas operativos de propósito general en la provisión, control y gestión de los servicios y de la red en general.

Los antivirus requieren evolucionar en la detección de manifestaciones no clásicas de programas malignos y alcanzar un mayor desarrollo en sus capacidades heurísticas. Los mismos deberán también trabajar en la inspección de contenidos y colaborar en la batalla *antispam* (WatchGuard, 2005).

Desde el punto de vista de la lucha antifraude, la combinación de FMS e IDS parece ser la solución técnica más adecuada (Rivera, 2003). Además, debe emplearse un modelo para la descripción de fraudes, que permita el diseño de técnicas para su detección automática y de reglas para ser implementadas en los sistemas de detección (Baluja-García & Llanes, 2005; Kvarnstrom et al., 2000). Las nuevas herramientas de gestión de fraude tienen que ser adaptables, trabajar con perfiles de usuarios y servicios, aplicar análisis estadísticos, y correlacionar información de diversas fuentes.

Deben establecerse servicios de identificación, autenticación y control de acceso para restringir la actividad de terminales, servidores, sistemas y usuarios. Estos últimos deben identificarse ante los sistemas, los dispositivos y ante sus propios terminales (la seguridad de los terminales resulta vital). Para todo esto se requiere el empleo de técnicas como la biométrica y el análisis de experiencias como LDAP (*Lightweight Directory Access Protocol*), DNS (*Domain Name Service*), OTP (*One Time Password*), IPv6, certificación digital, autenticación SIP (*Session Initialization Protocol*), entre otros.

Las soluciones de seguridad, ya sean sistemas antivirus, cortafuegos, IDS/IPS u otros deben estar distribuidos a través de toda la red, aplicando los esquemas de defensa perimetral, distribuida y en profundidad. Debe contarse con mecanismos de seguridad desde los terminales del usuario, hasta los servidores, incluyendo los dispositivos y

redes de acceso y de núcleo. Es necesario diseñar soluciones integrales que permitan trabajar la llamada seguridad bajo demanda (SoD) (WatchGuard, 2005).

El diseño y planificación de soluciones de seguridad debe trabajar tres líneas fundamentales: la prevención, la detección y la recuperación. En el marco de la prevención deben incluirse medidas destinadas a evitar que la red, dispositivo o sistema protegido se convierta en el origen de los ataques, lo que disminuye considerablemente las afectaciones por incidentes de variantes de *spam*, DDoS y otros.

Otra necesidad primaria es la agilidad en la estandarización. Se observa exceso de rapidez en la fabricación de productos, sin embargo la estandarización, que facilita y hace homogéneo todo el trabajo de seguridad, incluyendo la fabricación de *software* y *hardware*, demora años enfrascada en planes de acción, informes de resultados y otros. Esto trae como consecuencia que el *hardware* y el *software* tengan numerosos problemas de seguridad.

11. Requerimientos de las herramientas de seguridad para las NGN

El reto de la seguridad en las NGN implica contar con herramientas (fundamentalmente cortafuegos, IDS, IPS, FMS, antivirus y sus combinaciones) que incluyan en sus diseños determinados requerimientos, explicados brevemente a continuación (Figura 2):

Figura 2. Requerimientos de las herramientas de seguridad para NGN.

• **Trabajo distribuido:** debido a la cantidad y dispersión de los puntos a proteger, y el volumen de eventos a analizar, las herramientas de seguridad deben tener presencia en varios dispositivos o sistemas al mismo tiempo. Uno de estos casos es el de los IDS de red (*Network* IDS [NIDS]) que necesitan ubicar sus sensores de tráfico en diferentes tramos de la red para detectar incidencias.

• **Administración centralizada:** aún cuando el trabajo de estas herramientas sea distribuido, debe concentrarse toda la labor de su administración. Esto puede hacerse por zonas de la red, grupos de clientes, servidores u otros y desde estos puntos configurar, actualizar, analizar y estudiar los reportes, y tomar decisiones. La comunicación entre las consolas de administración y los nodos o sensores que ellas gestionan debe ser segura. Esta administración centralizada tiene ventajas como la de detectar ataques simultáneos, ejecutar reacciones defensivas globales y otras.

• **Escalabilidad:** posibilidad de las herramientas de seguridad de proteger cada nuevo servicio a partir de un grupo pequeño de mejoras o modificaciones en sus códigos y/o componentes.

• **Portabilidad:** capacidad de las soluciones de seguridad de ubicarse y adaptarse a todo tipo de entorno. Esto incluye la red de acceso, las redes y dispositivos domésticos (televisores, computadoras, equipos de juegos en línea y demás), los dispositivos móviles, entre otros. Este requerimiento, como el anterior, permitirá a las herramientas de seguridad adaptarse a los vertiginosos cambios que se observan en los servicios y dispositivos de telecomunicaciones.

• **Operación segura:** se trata de construir herramientas de *software*, o combinaciones de *hardware* y *software*, que cumplan con requisitos como la seguridad en el código, adecuado tratamiento de errores, empleo del paradigma AAA, protección ante ataques DoS y demás intentos de intrusión comunes, entre otros. Las soluciones de seguridad no pueden introducir nuevas vulnerabilidades en el sistema o red NGN.

• **Empleo de tecnologías avanzadas:** garantiza la adaptabilidad, el aprendizaje, la eficiencia, el

análisis y otras necesidades de funcionamiento de las herramientas de seguridad. Entre otros, debe revisarse el empleo de la fusión y minería de datos, las redes neuronales y los agentes móviles. En la detección de intrusiones se trabaja por introducir con éxito el uso de estas tecnologías (Bass, 2000; Axelsson, 2000; Krugel & Toth, 2001).

12. Conclusiones

Las amenazas que afectan a las redes de datos, voz y televisión se combinan y evolucionan, dando lugar a nuevas amenazas que hacen muy complejo el trabajo de seguridad en las NGN. Se precisa entonces una evolución de los mecanismos de defensa, los cuales por una parte deben obtenerse de una combinación de los existentes en las redes que convergen y por la otra ser desarrollados cumpliendo un conjunto de requerimientos discutidos en este artículo. Todo lo analizado debe tomarse como base para abarcar la seguridad desde el núcleo de la red hasta los terminales de los usuarios, incluyendo las redes de acceso.

El análisis realizado constituye un primer paso para cubrir la necesidad de organizar y hacer homogéneo el trabajo de seguridad de las NGN. Esto es, disponer de modelos y arquitecturas que permitan planificar la seguridad de acuerdo a los requerimientos de cada lugar, servicio, dispositivo o red y diseñar y desarrollar las herramientas de seguridad que se necesitan. En fin, asegurar las NGN, así como sus dispositivos, protocolos y redes.

13. Referencias bibliográficas

Axelsson, S. (2000). *Intrusion detection systems: a survey and taxonomy*. Chalmers University of Technology, Göteborg, Sweden. http://www.mnlab.cs.depaul.edu/seminar/spr2003/IDSSurvey.pdf

Baluja-García, W. (2002). Belicismo en Internet. Causas y defensas. *Telem@tica*, *Revista Digital de la Información y las Comunicaciones*, Año I (19), 7-9. http://www.cujae.edu.cu/revistas/telematica

Baluja-García, W., & Llanes, A. C. (2005). Estado actual y tendencias del enfrentamiento del fraude en las redes de telecomunicaciones. *Revista Ingeniería Eléctrica, Automática y Comunicaciones* 26 (2), 45-52.

Bass, T. (2000). Intrusion Detection Systems and multisensor Data Fusion. *Communications of the Association for Computing Machinery* (ACM) 43 (4), 99-105.

Bellovin, S. M. (2004). *A Look back at security problems in the TCP/IP protocol suite*. Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04), p.229 - 249. http://www.cs.columbia.edu/~smb/papers/acsac-ipext.pdf

Cerebrus Solutions (2002). *Fraud Primer. Issue 2.3*. Cerebrus Solutions Ltd.

Crimi, J. C. (2001). *Next Generation Network (NGN) Services*. Telcordia Technologies, Inc. http://www.mobilein.com/NGN_SVCS_WP.pdf

Davis, R. (2005). *QoS for Security*. Cisco Systems. http://www.cisco.com/E-Learning/bulk/public/celc/qos/player.html.

Fumero-Paniagua, G. (2000). El Fraude en las Telecomunicaciones. Tecnología ICE 10 (1), 70-74. http://www.ice.go.cr/esp/cencon/pdf/infocom/fraude_en_telecomunic.pdf

Gamm, B., Howard, B., & Paridaens, O. (2001). Security features required in an NGN. *Alcatel Telecommunications Review*, 2nd Quarter, 129-133.

Garg, A., & Reddy, A. L. N. (2002). *Mitigating denial of service attacks using QoS regulation*. Proceedings of 10th IEEE International Workshop on Quality of Service, p. 45-53.

Huitema, C. (1999). *Challenges of the next generation networks*. Internet'99 Conference, Moscow. http://www.huitema.net/papers/challenges/challenges99.html

Jacobs, R. (2004). *Telecommunications fraud*. Dimension Data Inc..
http://www.dimensiondata.com/DocumentLibrary/WhitePapers/ServiceProviderSolutions/TelecommunicationsFraudWhitePaper.htm

Krügel, C., & Toth, T. (2001). *Applying mobile agent technology to intrusion detection*. Distributed Systems Group, Technical University, Vienna, Austria.
http://www.auto.tuwien.ac.at/~chris/research/doc/2001_01.pdf

Kvarnström, H., Lundin, E., & Jonsson, E. (2000). *Combining fraud and intrusion detection- meeting new requirements*. Proceedings of the 5th Nordic Workshop on Secure IT Systems (NordSec 2000), Reykjavik.
http://www.ce.chalmers.se/~emilie/papers/Kvarnstrom_nordsec2000.pdf

Larrazábal, G. (2004). Gestión de Fraude en Operadores de servicios de Telecomunicaciones. CITEL'2004, III Congreso Internacional de Telemática, Cuba.
http://www.cujae.edu.cu/eventos/citel2004/Presentaciones_Trabajos/Conferencias/Antifraude%20en%20las%20telecomunicaciones.ppt

Lintao, J. (2005). Concerning the security of communication networks. *Huawei Technologies* (16), 18-24.

Mampaey, M., & Paridaens, O. (2005). *Alcatel Vision for Secured Next Generation Networks*. Technology white paper.
http://www.alcatel.com/publications/

Pillado-Ortiz, J. M. (2000). *Redes del futuro, asuntos de interés e impactos para Hispanoamérica*. Asociación Hispanoamericana de Centros de Investigación y Empresas de Telecomunicaciones (AHCIET)-Telcordia Technologies, Inc.

Ramirez, D. (2005). *Converged video network security*. Lucent Technologies Inc..
http://www.lucent.com/livelink/090094038009a061_White_paper.pdf

Rivera, F. S. (2003). *Sistemas inteligentes para la detección y control de fraude*. XXVI Taller de Ingeniería de Sistemas, Chile.

SG13 (2004a). *General overview of NGN. Recommendation Y.2001*. Study Group 13, UIT-T.

SG13 (2004b). G*eneral principles and general reference model for Next Generation Networks. Recommendation Y.2011*. Study Group 13, UIT-T.

Siles-Peláez, R. (2002). *Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados*.
http://www.criptored.upm.es/guiateoria/gt_m464a.htm

Solem, A. & Zouganeli, E. (2004). Next Generation Network an ITU-T vision. *Telektronikk* 3 (1), 114-121.
http://www.telenor.com/telektronikk/volumes/pdf/1.2004/page_114-121. pdf

TISPAN (2005). *Security analysis of IPv6 application in telecommunications standards*. Technical Report 102.419v1.1.1. Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN), European Telecommunications Standards Institute (ETSI).
http://www.etsi.org/services_products/freestandard/home.htm.

WatchGuard (2005). *WatchGuard for MSS: a complete management solution for service providers*. WatchGuard Technologies, Inc.

Wexler, J. (2004). *Security and QoS unite*. Computerworld.
http://www.computerworld.com/networkingtopics/networking/story/0,10801,89113,00.html