Identificación y análisis del anonimato en comunicaciones electrónicas

Por Javier y Gloria Areitio Bertolín

Prof. Dr. Javier Areitio Bertolín
Catedrático de la Facultad de Ingeniería. ESIDE.
Director del Grupo de Investigación Redes y Sistemas. Universidad de Deusto.
jareitio@eside.deusto.es

Prof. Dra. Gloria Areitio Bertolín
Laboratorio de Informática Aplicada. Universidad del País Vasco (UPV / EHU)
gloria.areitio@ehu.es

En el presente artículo se identifican y definen los conceptos de anonimato, pseudo-anonimato, privacidad y confidencialidad en el área de las comunicaciones electrónicas. Se identifican los grados de anonimato, se detallan los objetivos del anonimato, los ataques y atacantes al anonimato, se identifican algunas razones y aplicaciones del anonimato. Por último se muestran los principales tipos de anonimato y se analizan diversas tecnologías para conseguir el anonimato en una red de comunicaciones electrónicas como Anonymizer, Mixnet, OR, TOR, Crowd.

El anonimato en el área de las comunicaciones electrónicas posibilita mantener oculta la información de identificación de la transacción y/o de las partes que se comunican. Tres razones por las que se necesita el anonimato son para proteger las actividades sensibles, para la publicación resistente a la censura, para la protección contra generación de perfiles. Se pueden identificar cuatro tipos usuales de anonimato: anonimato del emisor-remitente, del receptor, no vinculación entre el emisor y receptor y no vinculación de las transacciones. Existen diversos niveles de anonimato, como por ejemplo de nivel de enlace de datos (o nivel L2 o nivel MAC), de nivel de red (o nivel de encaminamiento o nivel L3 o nivel IP), de nivel de aplicación, etc. El anonimato puede ser de conexión (se trata de ocultar la vinculación entre emisor y receptor, las rutas y enlaces de comunicación de datos) y/o de contenido (se intenta ocultar la información utilizando esteganografía-watermarks, cifrado y canales subliminares).

El total anonimato entra en conflicto con la contabilización y auditoria de las acciones, en cambio el pseudo-anonimato permite autenticación y permite establecer confianza. Las acciones pueden ser vinculadas hacia atrás de un pseudónimo (identidad virtual) pero a menudo no a la identidad del mundo real. Las herramientas de pseudo-anonimato generan automáticamente nombres de usuario, contraseñas, direcciones de correo electrónico, etc. únicas para cada sitio Web que el usuario visite; actúan como un *proxy* entre el usuario y los sitios Web visitados.

La privacidad puede verse como: (1) La protección en relación con los datos de las personas. (2) El derecho a que no lo vigilen. (3) El poder de controlar que otros puedan conocer algo acerca de una persona. (4) Ser capaz de navegar por la Web sin ser observado por cookies. (5) Poderse comunicar por correo electrónico sin spam o correo basura no deseado. Algunos dispositivos electrónicos que permiten monitorizar las actividades de las personas que los utilizan son: el JukeBox, cuyo software de transferencia de música informa de todas las descargas a Creative Labs (http://www.nomadworld.com), el eMarker de Sony permite saber el artista y título de las canciones que se escuchan por la radio, guarda un registro personal de toda la música que oigas en el sitio Web emarker (http://www.emarker.com), el: CueCat, guarda el registro personal de anuncios en los que una persona está interesada (http://www.crq.com/cuecat.html), el Sportbrain que se lleva en el cinturón del pantalón monitoriza el ejercicio físico diario, al colocarlo en un teléfono móvil a medida que se acompaña descarga los datos al sitio Web de la compañía para su análisis (http://www.sportbrain.com/).

Figura 1. Grados-niveles de anonimato

Grados de anonimato. Tipos de atacantes. Objetivos de anonimato.

Se pueden identificar seis grados de anonimato que van desde la privacidad absoluta a la situación de descubierto con toda probabilidad y son: (1) Privacidad absoluta. El atacante no tiene forma alguna de distinguir la situación en la que un emisor potencial de hecho envía o no un mensaje. (2) Fuera de sospecha. El atacante puede ver evidencia de un mensaje enviado pero el emisor tiene la misma probabilidad de ser el originador que cualquier otro posible emisor del sistema. (3) Inocencia probable. La probabilidad de que el emisor sea el originador puede ser mayor que la de cualquier otro potencial emisor, pero la probabilidad de ser el originador es igual a la de no serlo. (4) Inocencia posible o negación plausible. La probabilidad de que el emisor sea el originador es mayor que no serlo, pero aún existe una probabilidad no trivial de que el originador sea otro. (5) Descubierto. Desde el punto de vista de los atacantes existe una elevada probabilidad acerca de quién es el emisor. (6) Descubierto con toda probabilidad. El atacante puede identificar la identidad del

Figura 2. Formas de proteger la identidad de usuario

emisor y probarlo ante cualquiera.

Los principales tipos de atacantes al anonimato son: (1) Escuchas clandestinos locales, globales e ISP, son adversarios pasivos. Pueden observar la comunicación hacia y desde los computadores de los usuarios. (2) Adversarios activos que participan, inyectan o borran mensajes, por ejemplo miembros *crowd* que colaboran y confabulan. Miembros *crowd* que pueden reunir su información y desviarse del protocolo. (3) Servidor final. Es el servidor Web al que se dirige la transacción.

Se pueden identificar tres objetivos de anonimato en los protocolos de encaminamiento anónimo: (1) Anonimato de identidad. Un nodo o computador que recibe o envía paquetes no puede ser identificado por sus nodos vecinos. (2) Anonimato de ruta. Un nodo que reenvía paquetes no debe poder determinar las identidades de los otros nodos que también participan en un protocolo de encaminamiento anónimo. (3) Anonimato de localización. Incluso aunque un nodo pueda sospechar que esta presente otro nodo con identidad especificada, no es posible determinar incluso la localización aproximada del nodo.

Razones y aplicaciones del anonimato.

Actualmente crece el número de entidades de las que nos queremos ocultar, así por ejemplo: (1) Socios de comunicación en el anonimato del emisor. (2) Atacantes externos como escuchas clandestinas locales que aplican sniffers a los enlaces específicos de una red local. (3) Atacantes internos, que se confabulan, que comprometen la seguridad de los elementos como routers, servidores, etc. El anonimato presenta diferentes aplicaciones: (1) Privacidad. Ocultar las transacciones online, navegación Web, etc. de gobiernos intrusivos, empresas de marketing y entidades que acaparan información. (2) No trazabilidad del correo electrónico. Por ejemplo negociaciones confidenciales de negocios, comunicaciones sensibles socialmente (reuniones de Alcohólicos Anónimos online), disidentes políticos, confidentes y encuestados corporativos anónimos, utilizando encuestas anónimas por correo electrónico. (3) Cumplimiento de Leyes e inteligencia. Por ejemplo comunicaciones secretas en redes públicas, operaciones de pinchado de líneas y honeypots. (4) Dinero digital o electrónico para compras online, en este caso no se debería poder vincular la identidad del comprador con la del vendedor. (5) Votación electrónica anónima. (6) Publicación resistente a la censura. (7) Cripto-anarquía.

Binomio de seguridad privacidad-anonimato.

Consideremos un cierto usuario XX de un computador con sistema operativo cuyo nivel de seguridad sea máximo, por ejemplo A1 con la métrica de seguridad TCSEC, supongamos que XX bloquea todo el contenido activo y cookies y cifra todas las comunicaciones de red. En estas condiciones aún puede identificarse cierta fuga de información personal a las siguientes entidades: (1) A la persona con quién se comunica, que puede saber la dirección IP, dirección de correo electrónico y dirección física MAC de tarjeta de red del usuario XX. Esta información le permite saber donde trabaja, donde vive y quizás su nombre. (2) A su ISP (Proveedor de Servicio Internet) o a los responsables corporativos de su empresa. Pueden saber los sitios Web que visita, las personas a las que envía correo electrónico, etc. Esto posibilita la fuga de: (a) Información acerca de su estado mental o salud física. (b) Confidencias o encuestas anónimas. Los mecanismos de anonimato abordan este problema ocultando quién se comunica con quién y su contenido de información.

Concepto de anonimato. Ataques al anonimato.

A la hora de definir el anonimato se pueden identificar tres aspectos. (1) El anonimato es el estado de no ser identificable dentro de un conjunto de sujetos. Se trata de ocultar las actividades entre otras similares. Una entidad cualquiera no puede ser anónima por si misma. Existe una diferencia entre anonimato y confidencialidad, esta última permite ocultar el contenido de información de los documentos o mensajes en texto en claro almacenados o transmitidos convirtiéndolos en texto cifrado, éste se puede capturar pero no entender. (2) Imposibilidad de vinculación de la acción a la identidad, por ejemplo el remitente y su correo electrónico no están más relacionados después de observar la comunicación que tuvo lugar anteriormente. (3) No observabilidad (difícil de realizar). Cualquier elemento de interés (mensaje, evento, acción) no es distinguible de cualquier otro.

Los principales ataques al anonimato son: (1) Análisis pasivo del tráfico. Consiste en inferir del tráfico de red aspectos como quién habla con quién y qué volúmenes da

datos y a que hora se han transferido. Para ocultar el tráfico que genera una entidad se debe transportar el tráfico de otras entidades. (2) Análisis activo del tráfico. Consiste en inyectar paquetes o poner una firma de tiempo en el flujo de paquetes. (3) Comprometer los nodos de red. Consiste en que el atacante compromete algunos routers. No es obvio saber qué nodos han sido comprometidos. El atacante puede estar pasivamente registrando el tráfico. Lo mejor es no confiar en ningún router individual. Se debe asumir que alguna fracción de todos los routers es buena (no esta comprometida), pero no se sabe cual.

Un informe de la AAAS (American Association for the Advancement of Science) señala que las comunicaciones anónimas online son una tecnología moralmente neutral. Las comunicaciones anónimas deberían considerarse como un sólido derecho humano, en USA es un derecho constitucional (segunda enmienda). Internet proporciona muchísimas oportunidades para recoger información de las personas. La comunicación anónima proporciona la posibilidad a las personas maliciosas de realizar spam, engaños y fraude. Para personas buenas permite la privacidad, posibilitando anonimato en actividades de la policía, periodísticas, grupos de discusión, encuestas y confidencias anónimas, etc. El término anónimo se define como de autor u origen desconocido, que carece de individualidad, distinción o posibilidad de reconocerlo. Una entidad anónima no significa que no pueda ser identificada, significa que es indistinguible dentro de un grupo concreto, la probabilidad de que sea el originador de un mensaje es reducida. El anonimato es el estado de no ser identificable dentro de un conjunto de sujetos, por ejemplo un remitente o un destinatario serán anónimos entre un conjunto de remitentes o destinatarios. La no vinculación de dos o más elementos (por ejemplo, sujetos, mensajes, eventos, acciones, etc.) significa que dentro de este sistema, estos elementos no están más ni menos relacionados en lo que se refiere al conocimiento a priori, por ejemplo emisor-receptor (entrega anónima), comerciante-comprador (autenticación anónima con dinero electrónico), votación electrónica.

Tipos de anonimato. Tecnologias para el anonimato. Privacidad sobre redes públicas.

La comunicación electrónica anónima se ocupa de estudiar las técnicas que facilitan la comunicación ocultando quien es el emisor, quién es el receptor y cual es la vinculación entre ellos. Es aplicable a la privacidad en comercio electrónico y en general, al comercio de música, la comunicación encubierta, los BBS anónimos, por ejemplo de Alcohólicos Anónimos o AA, etc.

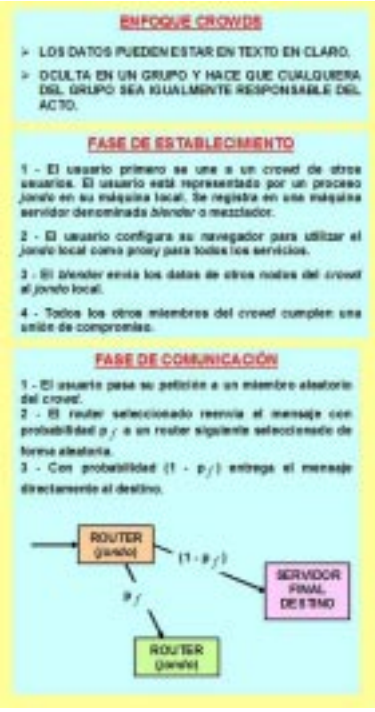

Figura 3. Funcionamiento del enfoque Crowds para el anonimato. Fases de establecimiento y comunicación

Atendiendo a cuales son las entidades que se intenta ocultar se pueden identificar tres tipos de anonimato: (1) Anonimato del emisor/remitente, aquí el atacante no puede determinar el emisor de un mensaje concreto. (2) Anonimato del receptor, aquí el atacante no puede determinar el receptor al que va a parar un mensaje. (3) No vinculación, el atacante puede determinar los emisores y receptores pero no las asociaciones entre ellos, el atacante no sabe quién se comunica con quién.

Para el anonimato se han ido diseñando diversas tecnologías basadas en el relleno de tráfico, cifrado, elección aleatoria, etc. La forma de demostrar que alguien no puede hacer algo no es sencillo, se puede acudir a la criptografía, demostrar que si pueden, también pueden hacer algo que pensamos o sabemos que realmente es difícil. El estado actual del arte mide el anonimato cuantificando el nivel de entropía del sistema.

Existen diversos enfoques generales para el anonimato: (1) Enfoque centralizado, el anonymizer. Anonymizer es una protección especial para tráfico http, actúa como un proxy para peticiones del navegador, re-escribe enlaces en páginas Web y añade un formulario que permite introducir los URLs. Los principales inconvenientes: debe ser de confianza y representa un único punto de fallo/ataque. Actúa como un proxy para los usuarios, oculta la información desde los servidores finales, ve todo el tráfico Web, añade anuncios a páginas, servicio gratuito, servicio de suscripción disponible en: http://www.anonymizer.com. (2) Crowds, camino aleatorio probabilístico, DCnet (Dining Cryptographers net), Mixes de Chaum (Mix básico), OR (Onion Routing) y Cashmere (anonimato comparable a Mix de Chaum, desarrollado en 2005, proporciona anonimato en el nivel L3 de encaminamiento, en vez

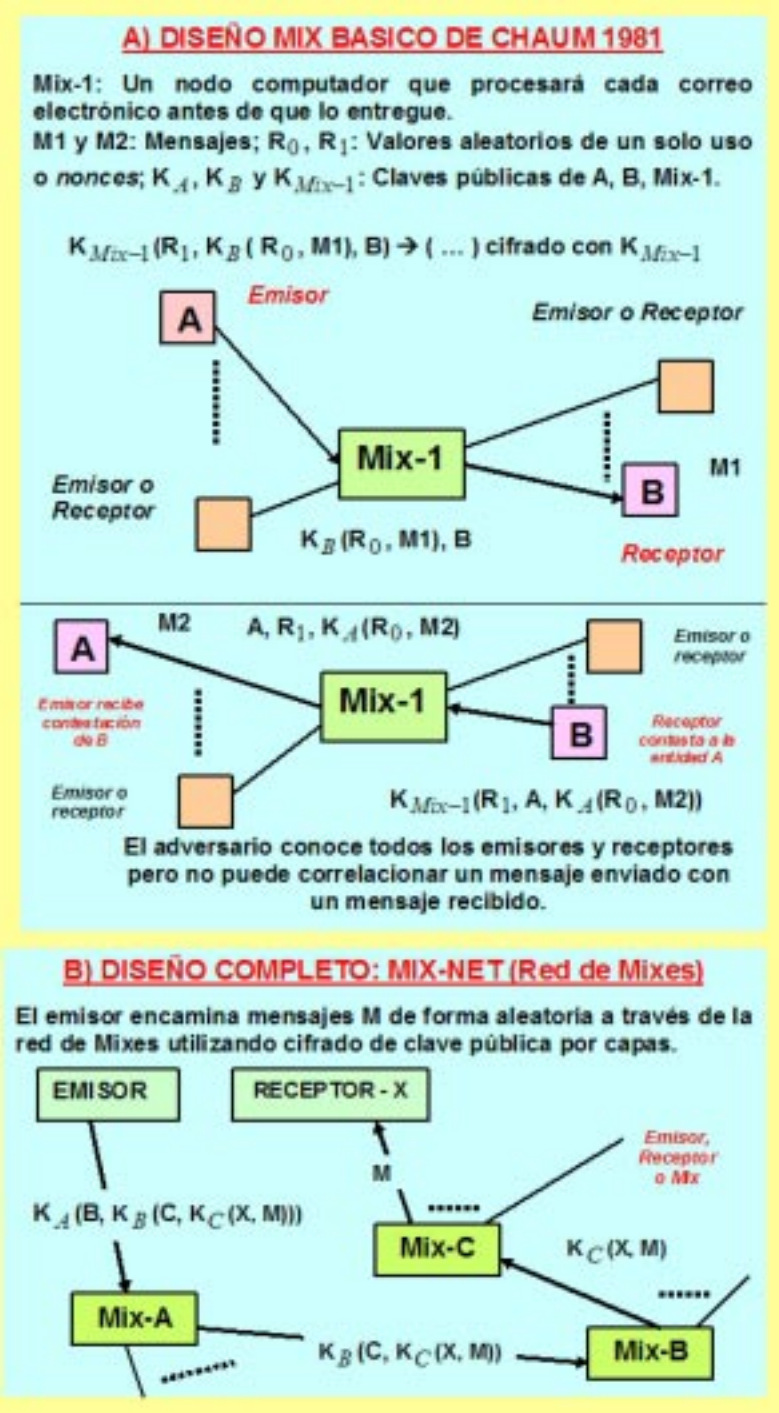

Figura 4. Enfoques de anonimato: Mix básico de Chaum y Mix-net.

de nodos aislados utiliza grupos para retransmitir el tráfico).

Los *sistemas basados en retransmisores* pueden clasificarse atendiendo a su nivel de latencia en: (1) Elevada latencia. Maximizan el anonimato pero a expensas de introducir un elevado costo en cuanto a latencia. La red resiste fuertes adversarios globales, introduce demasiado retraso para algunas aplicaciones TCP. Algunos ejemplos son: Babel, Mixmaster (remailer tipo II) y Mixminion (remailer tipo III) (es una red de Mixes, es adecuada para aplicaciones de elevada latencia como el correo electrónico anónimo; http://www.mixminion.net), Java Anon Proxy. (2) Baja latencia. Permiten el anonimato del tráfico interactivo que contiene más paquetes que son dependientes del tiempo. Maneja una variedad de protocolos bidireccionales. La dependencia del tiempo de las comunicaciones es una preocupación de diseño. Algunos ejemplos son: Anonymizer, Pipenet y Tor (TCP based Onion Routing, requiere una fuente para prenegociar una clave simétrica para cada salto de la ruta).

Un enfoque útil en tecnologías de anonimato es el *encaminamiento aleatorio*, se trata de ocultar el origen del mensaje encaminándolo de forma aleatoria, técnicas que utilizan esta filosofía son Crowds, Freenet y Onion Routing; los routers no saben si el origen aparente de un mensaje es el verdadero emisor u otro router.

Internet se diseñó como una red pública, al igual que las máquinas de una red local pueden ver tu tráfico, los routers de red ven todo el tráfico que pasa a través de ellos. La información de encaminamiento es pública, las cabeceras de los paquetes IP identifican el origen y destino, incluso un observador pasivo puede conocer quién se comunica con quién. El cifrado no oculta las identidades, oculta la carga útil pero no la información de encaminamiento. Incluso el cifrado a nivel IP (modo túnel IPsec/ESP) revela las direcciones IP de las pasarelas IPSec.

Las técnicas de *watermarks* así como la *esteganografía* persiguen el ocultar información escondiéndola dentro de algún cierto soporte como una fotografía (.tiff, .jpg, .bmp, etc), un fichero de texto, audio o video, etc.; suele ser usual

combinar las técnicas de ocultación de los datos utilizando *esteganografía-watermarks* con ocultación del contenido de los mismos mediante *técnicas de cifrado*. Los *servidores de localización oculta* se despliegan en Internet para que todos puedan conectarse a ellos sin saber donde están o quién los ejecuta, son accesibles desde cualquier sitio, son resistentes a la censura, pueden sobrevivir a ataques DoS y resisten a ataques físicos ya que no se puede encontrar el servidor físico. Para crear un servidor de localización oculta: (1) El cliente obtiene un descriptor de servicio y una dirección de punto de introducción de un directorio (servidor de búsqueda de servicio). (2) El servidor de localización oculta crea rutas onion a los puntos de introducción. Así mismo proporciona direcciones y descriptores de puntos de introducción al directorio de búsqueda de servicios. Para utilizar un servidor de localización oculta: (1) El cliente crea una ruta onion a un punto de encuentro, éste empareja los circuitos desde cliente a servidor. (2) El cliente envía la dirección del punto de encuentro y cualquier autorización, que se necesite, al servidor a través del punto de introducción. (3) Si el servidor elige hablar con el cliente, conecta con el punto de encuentro.

Figura 5. Comparativa entre los enfoques de anonimato. Redes Mix Mix-Net y Crowds.

Tecnologia para la construcción del anonimato: MIX.

Los sistemas de anonimato modernos utilizan el Mix como bloque de construcción básico. Una de las primeras tecnologías de anonimato fue el diseño de Red Mix o Mixnet de Chaum de 1981 que sugirió ocultar la correspondencia (mensajes de correo electrónico) entre emisor y receptor envolviendo los mensajes en capas de cifrado de clave pública. Estos mensajes deberían atravesar un conjunto de Mix en el camino hacia el receptor. Los Mix descifran, retardan y reordenan los mensajes antes de pasarlos hacia delante. En una red Mix los paquetes que se envían del origen al destino deben pasar a través de un conjunto de Mixes. Un Mix reordena y re-cifra los datos que le llegan para reenviarlos, de esta forma se previene la correlación entre los flujos de entrada y salida. En una red Mix cuando aumenta el número de Mixes, también se incrementa el número de reordenaciones y re-cifrados que hacen aumentar la dificultad para correlacionar los mensajes entrantes y salientes, sin embargo, también se incrementa la latencia y disminuye la tasa de entrega. Un nodo Mix también puede volverse malicioso y examinar los contenidos de los paquetes que re-cifra. En una cascada Mix los mensajes se envían a través de una secuencia en serie de Mixes, también se puede utilizar una red de topología arbitraria de Mixes denominada Mixnet, algunos de los Mix pueden estar controlados por el atacante pero incluso con uno bueno se garantiza el anonimato. Se utiliza relleno y tráfico en buffer para frustrar los ataques de correlación.

Los principales inconvenientes del esquema Mixnet básico son: (1) El cifrado y descifrado de clave pública en cada Mix es computacionalmente costoso en tiempo. (2) Las Mixnets básicas poseen elevada latencia, son buenas para correo electrónico pero no adecuadas para navegación Web anónima. El reto es una red de anonimato de baja latencia, utilizar criptografía de clave pública para establecer un circuito con claves simétricas entre saltos en el circuito; utilizar descifrado y re-cifrado simétrico para mover los mensajes de datos sobre los circuitos establecidos; cada nodo se comporta como un Mix, el anonimato se preserva aunque algunos nodos tengan su seguridad comprometida. El enfoque Mix ofusca los datos y mezcla los datos con tráfico encubierto.

Tecnologia para la construcción del anonimato: OR.

La red Mix se modificó dando lugar a OR (Onion Routing) en 1997 (Reed, Syverson y Goldschlag) que permite encaminar información para ser codificada en un conjunto de niveles cifrados, es decir *onions.* El original OR (Onion Routing) es una red distribuida superpuesta

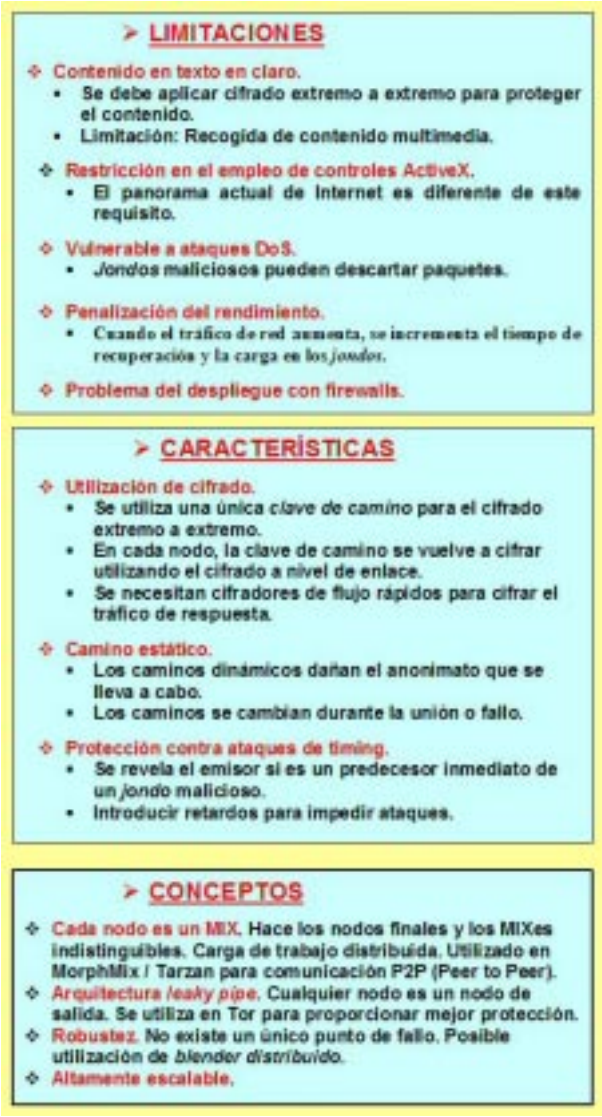

Figura 6. Limitaciones, características y conceptos del enfoque de anonimato Crowds.

ideada para hacer anónimas las aplicaciones basadas en TCP. El proxy onion del lado del cliente (OP) elige un circuito de routers onion, un router onion (OR) es un servidor que recibe mensajes desde los nodos extremos, los reordena y reenvía hacia el destino. Los mensajes se dividen en células de tamaño fijo y se empaquetan en un objeto de datos denominado "onion" por medio de sucesivos niveles de cifrado. Cuando el onion atraviesa el circuito, los niveles de cifrado se separan y el mensaje se pasa al siguiente router OR del circuito. Onion Routing necesita una autoridad central lo que lo hace impráctico para redes móviles *ad hoc*. En Onion Routing el emisor elige una secuencia aleatoria de routers, algunos son honestos y otros pueden estar controlados por el atacante, el emisor controla la longitud del camino. Para el establecimiento de la ruta la información de encaminamiento para cada enlace se cifra con la clave pública del router, cada router aprende sólo la identidad del siguiente router. El enfoque Onion Routing ofusca los datos y utiliza el relleno de células para hacer que los datos parezcan similares, utiliza criptografía para dificultar las escuchas clandestinas. Para enviar un mensaje M a un receptor B, se elige un subconjunto aleatorio de n routers onion R1, . . . , Rn; se obtienen sus n claves públicas PK1, . . . , PKn y se forma un onion: Cifrado con PK1(R2,Cifrado con PK2(R3, . . . Cifrado con PKn(B, M)…)

Tecnologia para la construcción del anonimato: TOR.

Tor (TCP based Onion Routing) representa la segunda generación de red OR (Onion Routing), desarrollado por R. Dingledine, N. Mathewson y P. Syverson, ejecutándose desde 2003, especialmente diseñada para comunicaciones Internet anónimas de baja latencia. Es una red de anonimato basada en circuito superpuesta, es adecuada para aplicaciones de baja latencia como navegación Web anónima. Existen más de cien nodos en los cuatro continentes, con miles de usuarios. Es fácil de utilizar en base a un proxy cliente; disponible de forma gratuita, se puede utilizar para la navegación anónima (http://tor.eff.org). Tor incorpora mejoras sobre el Onion Routing tradicional, por ejemplo añade el reenvío secreto y la construcción del camino incremental. Tor necesita una fuente para pre-negociar una clave simétrica para cada salto en la ruta, que es virtualmente imposible en redes móviles debido a la movilidad del nodo.

El establecimiento de un circuito Tor es el siguiente: (1) El proxy cliente establece una clave de sesión simétrica y un circuito con el router onion número 1. (2) El proxy cliente extiende el circuito estableciendo una clave de sesión simétrica con el router onion número 2; existe un túnel a través del router onion número 1 que no necesita onion. (3) El proxy cliente extiende el circuito estableciendo una clave de sesión simétrica con el router onion número 3; existe un túnel a través de los router onion números 1 y 2. Las aplicaciones cliente se conectan y se comunican sobre el circuito Tor establecido. Los datagramas se descifran y se vuelven a cifrar en cada enlace.

Las principales cuestiones de gestión en Tor son: (1) Muchas aplicaciones pueden compartir un circuito. Múltiples corrientes TCP pueden existir sobre una conexión anónima. (2) El router Tor no necesita privilegios de root o raíz. Esto anima a las personas a configurar sus propios router. Además cuantos más participantes haya mejor anonimato para todos. (3) Servidores de directorio. Mantienen las listas de router onion activos, sus localizaciones, las claves públicas corrientes, etc.. Controlan cómo se unen nuevos routers a la red; el *ataque Sybil* consiste en que el atacante crea un gran número de routers. Las claves de los servidores de directorio se envían con código Tor. Tor es un esquema eficiente a gran escala del tipo onion routing, utiliza intercambio de claves Diffie-Hellman autenticado para construir circuitos que son cifrados con claves simétricas; su objetivo es dar seguridad en entornos con routers que han visto comprometida su seguridad.

Tecnología de anonimato sin autoridad central: CROWDS.

Un *crowd* es un conjunto de usuarios formado dinámicamente. Cada usuario ejecuta un proceso denominado *jondo* en su computador, cuando dicho *jondo* se arranca contacta con un servidor denominado *blender* para pedirle su admisión al *crowd*. Si se le admite, el *blender* informa a los miembros actuales del *crowd* y envía la información necesaria (es decir las claves) para que se una al *crowd*. El usuario configura su navegador para utilizar su *jondo* como Web proxy, cuando el *jondo* recibe la primera petición del navegador, inicia el establecimiento de un camino aleatorio de *jondos* en el *crowd.* El *jondo* escoge un *jondo* (posiblemente él) del *crowd* aleatoriamente y le reenvía la petición (después de ocultarla). Cuando este *jondo* recibe la petición la reenvía de nuevo con probabilidad pf (a un *jondo* seleccionado de forma aleatoria) y presenta la petición al servidor destino con probabilidad (1 – pf). Las siguientes peticiones siguen el mismo camino. Las respuestas del servidor atraviesan el mismo camino en dirección opuesta. La comunicación entre *jondos* se encuentra cifrada. Los usuarios se unen a un *crowd* de otros usuarios. Las peticiones Web desde el *crowd* no pueden vincularse a ningún individuo. Permite una protección contra: servidores finales, otros miembros *crowd,* administradores del sistema y escuchas clandestinas. *Crowd* puede considerase el primer sistema para ocultar la vigilancia de datos de la Web sin confiar en una autoridad central. El *jondo* de cada usuario siempre reenvía la petición a un miembro aleatorio del *crowd*, por tanto oculta la identidad del usuario. El servidor final es igualmente probable que reciba la petición desde cualquier miembro del *crowd*. Un escucha clandestino local puede ver que el usuario originó una petición, por tanto el emisor queda descubierto pero no puede ver el destinatario de dicha petición.

Figura 7. Utilización del enfoque de anonimato basado en un único proxy Anonymizer.

Consideraciones finales.

En el fascinante mundo de la seguridad se pueden identificar básicamente cinco métodos de defensa: (1) Prevenir ataques, bloqueándolos o cerrando vulnerabilidades, por ejemplo cargando parches de seguridad en el S.O. (2) Disuadir el ataque, haciéndolo más difícil ya que no se puede hacer imposible. (3) Desviar el ataque hacia otro objetivo más atractivo como por ejemplo *honeypots, honeynets, nepenthes*, etc. (4) Detectar el ataque, durante y después. (5) Recuperarse del ataque. El anonimato puede utilizarse para hacer mal por ejemplo para enviar contenido ilícito, correos electrónicos para acosar, para inundar con foros de discusión, mailbombing, etc.

Este artículo se enmarca en las actividades desarrolladas dentro del proyecto *LEFIS-APTICE: Legal Framework for the Information Society II* (financiado por Socrates 2005. *European Commission*).

Bibliografia.

- Areitio, J. "Identificación, clasificación de objetivos de seguridad y creación de un modelo de servicios técnicos de seguridad para TIC". Revista Española de Electrónica. Nº 588. Noviembre 2003.
- Areitio, J. y Areitio, G. "Identificación y Análisis del Control de Acceso para la Seguridad de TIC". Revista Española de Electrónica. Nº 591. Febrero 2004.
- Areitio, J. y Areitio, G. "Identificación y Análisis de la tecnología de detección y prevención de intrusiones". Revista Española de Electrónica. Nº 615. Febrero 2006.
- Bejtlich, R. "Extrusion Detection. Security Monitoring for Internal Intrusions". Addison-Wesley. 2006.
- Conti, G. "Security Data Visualization". No Starch Press. 2007.
- Rincón, J.M. y otros. "El espacio documental en el entorno transaccional de un sistema de gestión". Boletín de estudios económicos, Vol. 60, Nº 184. págs. 135-162. 2005.
- Forouzan, B.A. "Network Security". McGraw-Hill. 1st Edition. 2007.
- Hurley, W. "Self-Defensing Networks: Rules of Engagement for Active Network Security". O'Reilly Media. 2006. ❑