[PAN] Comunicaciones anónimas (Resumen)

Cada red de comunicación usa direcciones para realizar el enrutado de forma que los datos puedan ser transmitidos de origen a destino. En general esas direcciones son visibles para cualquiera que observe la red y suelen ser identificadores únicos, de forma que todas las comunicaciones relacionadas con un usuario pueden ser trazadas. En ocasiones sabiendo esto se puede asociar una comunicación con una persona física, lo que puede comprometer su privacidad.

Teniendo en cuenta esto, anonimizar los canales de comunicación es necesario para mantener la privacidad de los usuarios y para proteger las propias comunicaciones contra análisis de tráfico. Este proceso puede también incluir el uso de técnicas de anonimización en capa de aplicación, como autenticación anónima o protocolos de votación anónimos.

Una comunicación anónima oculta quien se comunica con quien, pueden darse varios casos:

- El emisor debe ser ocultado para todos, incluido el receptor
- El receptor debe ser ocultado para todos, incluido el emisor
- Tanto el receptor como el emisor deben ser ocultados para terceros.

Hay varios niveles de anonimidad:

- La privacidad total puede ser garantizada para que todo el mundo pueda actuar de forma anónima.
- Privacidad Parcial, las agencias gubernamentales son capaces de deshacer la anonimidad para todo el mundo
- Nada de privacidad, todo el mundo puede observar todo

Definiciones de Pfitzmann y Hansen:

- Anonimidad: Es el estado en el que uno no puede ser identificado dentro de un grupo de sujetos. Requiere que exista un grupo anónimo, que es un grupo de sujetos con potencialmente los mismos atributos. En el caso de las comunicaciones, este grupo puede consistir en sujetos que puede ser usados para enviar o recibir transmisiones
- No-Enlazabilidad: Significa que un usuario puede hacer el uso de un servicio sin poder ser enlazado con múltiples usos. No se puede determinar si un usuario a realizado una operación.
- No-Observabilidad: Es el estado de los objetos de interés de no ser distinguibles de otros elementos de interes. Los mensajes no pueden ser diferenciados de ruido. No se puede detectar cuando un mensaje ha sido enviado o recibido.
- Pseudoanonimidad: Se usa un pseudónimo como identificador.

Modelos de ataque sobre redes de comunicación:

- Tipo I (Atacante pasivo): Puede observar todas las comunicaciones
- Tipo II (Atacante pasivo con capacidades de envío): Además de observar las comunicaciones, también puede tomar parte en el proceso enviando nuevos mensajes
- Tipo III (Atacante Activo): Puede controlar todas las comunicaciones, puede realizar eliminaciones, envíos o retrasar mensajes.

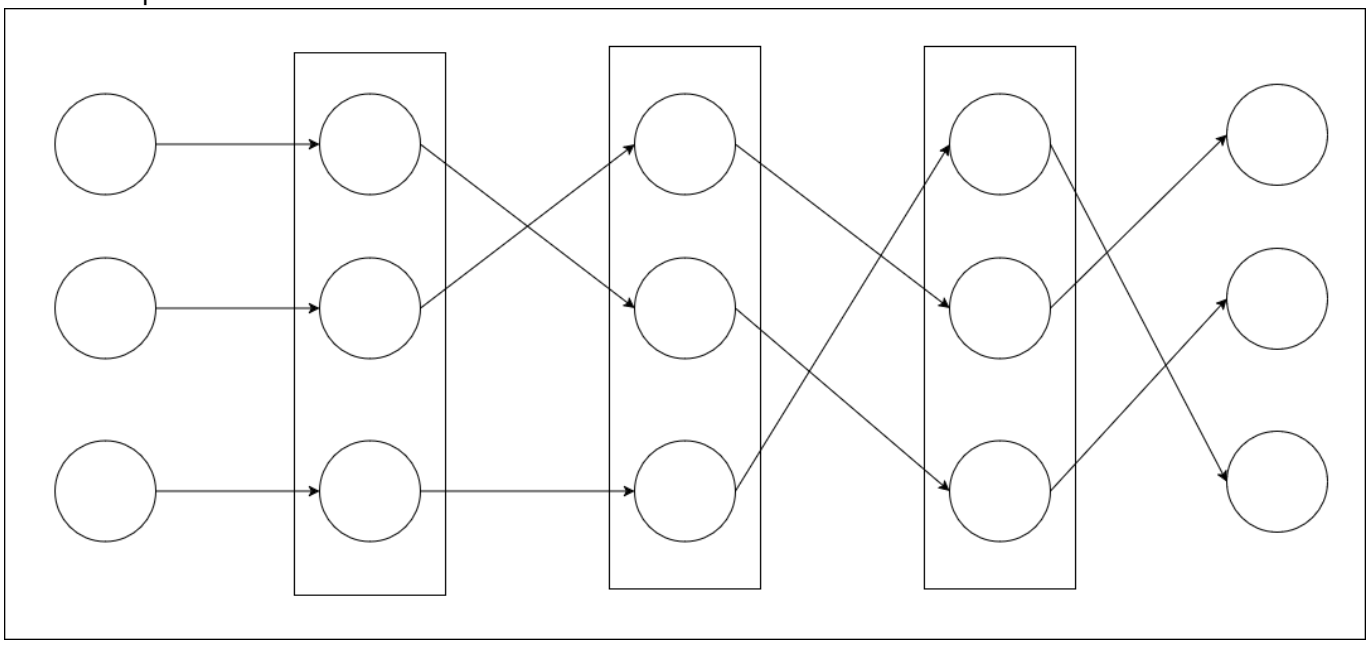
Requerimientos para la anonimidad en redes de comunicación:

- Tráfico de cobertura: Una sola transmisión, realizada por una sola persona puede ser observada

con facilidad. Para poder enmascarar dicha transmisión se debe proveer tráfico adicional. Si el atacante controla el tráfico de cobertura no se puede asegurar la anonimidad.
- Tráfico embebido: El tráfico generado por un usuario debe ser embebido de forma adecuada y silenciosa en el tráfico de cobertura de forma que el atacante lo lo pueda distinguir.
- Efectividad: Si hay N mensajes de diferentes usuarios, K mensajes deben ser reales mientras que M=n-K deben ser tráfico de cobertura. La efectividad del sistema puede ser definida como K/N, donde 1 es el caso óptimo, siendo todos los mensajes reales.

Redes MIX

Buscan implementar un sistema de correo electrónico anónimo



- Si todos los nodos son honestos y siguen el protocolo, las salidas son permutaciones de las entradas y el contenido del mensaje no se ve alterado
- Si al menos un nodo oculta el intercambio, la permutación es secreta, por lo que la correspondencia entre las entradas y salidas es desconocida.
- La honestidad de los nodos puede ser verificada públicamente, por o que se puede garantizar que las salidas son permutaciones de las entradas.
- Las redes Mix deben operar incluso en casos donde los nodos fallen o sean comprometidos.

Nodos de procesado

Cada entrada, un mensaje m, es secuencialmente cifrado usando la clave pública K_i de cada nodo i. En cada etapa de la red Mix se realizan dos operaciones:

- Cada nodo i usa su clave privada K_i^{-1} para eliminar una capa de cifrado para cada una de sus entradas
- Estos mensajes parcialmente descifrados son permutados en la etapa i antes de ser enviados a siguiente paso en un orden aleatorio
- Todas las partes son enviadas a la etapa i+1 a la vez

Ventajas y desventajas

Tipo	Ventajas	Desventajas
Cadena de descifrado	Las direcciones intermecias pueden ser incluidas para el enrutado	El emisor debe realizar múltiples cifrados Cada etapa debe participar en un orden específico Las entradas pueden ser trazada por apariencia o tamaño
Cadena de recifrado	El emisor realiza un solo cifrado. Las entradas no pueden ser trazadas por apariencia o tamaño No se requiere que todas las etapas participen y el orden no importa	

Cascada

- Consiste en una secuencia fija de etapas que es compartida por cada emisor o receptor involucrados en la comunicación
- La primera etapa comienza mezclando todos los mensajes, agrupándolos en grupos de tamaño L que son procesados de forma síncrona.
- Una etapa defectuosa puede comprometer toda la red.
- Los ataques pasivos son posibles trazando los mensajes a través de los grupos mezclados, cuanto más grande el grupo, más difícil es seguir el mensaje
- Los ataques activos también son posibles, pero el ataque debe tener cierto control sobre la red mix.

Enrutado libre

- Consiste en una serie de etapas interconectadas que no tienen por que ser dependientes
- Cualquier etapa puede recibir entradas de emisores, además pueden pasar una salida directamente al receptor.
- Cada etapa puede esperar hasta que L mensajes son agrupadas en un grupo, pero solo por cierto período de tiempo fijado, tras eso, se pasan los mensajes a la siguiente etapa.
- Este modo de operación es asíncrono.
- Los ataques pasivos pueden trazar mensajes debido al tráfico no uniforme que pas por las etapas.
- Los ataques activos pueden realizarse inundando la red con tráfico para aislar mensajes.

Verificación

Para verificar una red mix se debe analizar como de correcto es el procedimiento de acuerdo a los siguientes criterios:

- El grupo de entrada ha sido procesado y permutado
- Los mensajes no se han corrompido
- No hay entradas de más o de menos

Estas verificaciones pueden ser realizadas a nivel de la red entera o a nivel de cada una de las

etapas. En general estos mecanismos NO pueden ser aplicados a redes de enrutado libre.

Red mix con emisor verificable

Detecta mensajes corruptos a la salida de la red, pero no en las entapas intermedias. Para implementar este sistema de verificación, el emisor incluye un checksum con el mensaje. Tanto el checksum como el mensaje son cifrados con la clave privada del emisor. Cualquiera puede detectar si el mensaje ha sido alterado descifrándolo con la clave pública del emisor.

Este sistema no puede detectar si se han añadido mensajes de más. La eliminación de mensajes solo puede ser detectada si el emisor revisa si su propio mensaje está presente en la salida de la red. No se pueden identificar etapas comprometidas.

Red mix con etapa verificable

Cada etapa verifica las salidas de la red usando protocoles adicionales para asegurar que todo funciona correctamente. Creando varias copias del grupo de entrada o repitiendo todo el proceso de la red mix se pueden detectar etapas comprometidas en cadenas de recifrado. El revelado de secretos o uso pruebas de cero conocimiento en una etapa pueden ser verificados por otros. Se usan mecanismos de recuperación para reiniciar las operaciones en caso de que se detecten comportamientos extraños.

Onion Routing

Se basa en la idea de enrutado por múltiples nodos y cifrado multicapa:

- Un mensaje dado es cifrado capa por capa usando las claves de todos los nodos de camino al receptor.
- Cada nodo deshace una capa de la cebolla descifrándola, de forma que la dirección del siguiente salto es revelada y pasa el resto del mensaje todavía cifrado al siguiente nodo.
- Al contrario de lo que pasa con las redes mix, no se oculta el tráfico de la red mezclando los mensajes, el orden de las entradas y salidas de cada nodo es irrelevante.

Este mecanismo consiste en varias entidades:

- La aplicación cliente donde la comunicación se inicia
- Un Proxy Onion: Determina el camino del origen al destino a través de N nodos diferentes, donde al primero se le llama embudo de entrada y al último embudo de salida. También se encarga de construir las capas que serán enviadas por la red onion.
- Routers: Se encargan de pelar una capa de la cebolla y pasar las capas restantes al siguiente salto hasta que se alcanza el embudo de salida. En caso de una respuesta realizan la operación a la inversa.
- Embidos de entrada y salida: El de entrada puede ver e interactuar con el emisor de la comunicación mientras en el de salida puede ver e interactuar con el receptor de la comunicación.

TOR

Es la implementación más conocida del Onion Routing. Se la considera la versión evolucionada de la idea original, mejorando algunos aspectos así como el mecanismo para su uso en aplicaciones reales.

- No es una red P2P, los usuarios no actúan como nodos, son solo usuarios que se unen a la red utilizando un navegador de internet. La red opera a través de nodos que son proveídos por organizaciones e individuos que donan sus capacidades de procesamiento y ancho de banda al proyecto.
- Algunos nodos también actúan como servidores directorio.
- No es seguro contra ataques end-to-end: Si la misma entidad controla el primer y el último nodo, puede inferir el emisor y el receptor, así como el contenido del mensaje. No oculta la identidad del emisor a nivel de aplicación.

Construye circuitos de una forma diferente a la forma original:

- usa siempre 3 nodos, primero el embudo de salida es seleccionado, un nodo es seleccionado solo una vez. El primer nodo es un nodo guardia considerado fiable. Los circuitos son rotados periódicamente.
- Cada nodo tiene una clave de identidad de larga duración y una clave onion de baja duración. La de identidad se usan para firmar certificados TLS que se usan para comunicarse con otros nodos y clientes. La clave onion es rotada periódicamente y es usada para contruir circuitos y negociar claves efímeras para cifrado y descifrado de mensajes.

Una vez se ha construido el circuito y se establecen las claves compartidas entre nodos y emisores, los datos pueden ser enviados.

Servicios ocultos

La idea es que tanto el usuario como el servidor no sepan sus direcciones IP. Para lograr esto el servidor solicitar 3 nodos onion diferentes para actuar como punto de entrada. Una vez se han establecido estos puntos, el servidor construyen un descriptor de servicio oculto que es publicado a través de una tabla hash distribuida a través de la red onion. Tras eso los usuarios pueden solicitar un servidor específico a través de una dirección onion. Una vez que se tiene la dirección del punto de introducción, se selecciona uno de forma aleatoria