Redes de Comunicación

Es importante proteger las comunicaciones para que no quede rastro de las comunicaciones. A nivel de aplicación puede ser necesario reforzar el sistema. Se le debe permitir a un usuario acceder a una red sin revelar su identidad. El problema de estos sistemas es que si accede algún mal actor no es posible identificarlo.

Anonimidad

Supone no ser capaz de distinguir a una persona dentro de un conjunto de personas.

Unobservabilidad

Un objeto de interes no es distinguible de otros elementos de interés

Pseudonimidad

El estado de usar un pseudónimo como identificador

Tipos de ataques en redes de comunicación

- Tipo 1 Pasivo: Se pueden observar los enlaces de comunicación
- Tipo 2 Atacante pasivo con capacidades de envío: Un observador que puede inyectar paquetería
- Tipo 3 atacante activo: Puede controlar enlaces de comunicación, eliminar paquetes, enviar o retrasar otros paquetes.

Requerimientos para la anonimidad en redes de comunicación

- Tráfico cubierto: Se añade tráfico adicional a la red para enmascarar una transmisión, funciona siempre y cuando el atacante no controle la red
- Efectividad. No se deben meter más de cierta cantidad de mensajes ya que se puede volver completamente ineficiente la comunicación. K/N nos dice cuanta paquetería es buena de verdad. Si K/N=1 Entonces es completamente eficiente, todos los paquetes son reales y no hay ningún dummy.
- Si hay nodos comprometidos, tiene que haber al menos uno honesto, siendo lo más recomendable un mínimo de 2.

Redes Mix

- Se necesita mínimo un nodo honesto.
- Se van permutando los mensajes entre nodos y se van transformando (Lo que podríamos llamar barajar) para cambiar su forma, haciendo más difícil su trazabilidad. Este proceso se hace a lo largo de N etapas.

Redes de descifrado

En cada etapa cada nodo realiza una transformación en la que retira una capa del mensaje envíado. Para descifrar se parte del núcleo, se cifra el mensaje con la clave del receptor, poniendo la dirección del receptor y se cifra con el siguiente nodo y se repite el proceso hasta el nodo final (Similar a la Práctica 1 de SI de cifrado anidado).

ReCifrado

En este este subtipo de red Mix el emisor cifra un mensaje m usando la clave pública K de la red mixta donde g es un generador y r un string aleatorio:

$Ek(m,r) = g^r || (Ax || m)k'$

Se cifra una vez el mensaje y la dirección del destinatario. Los caminos que se toman están prefijados. La ventaja de este tipo de redes es que da igual el orden por el que pase el mensaje por los nodos. No es necesario que se pase por todos los nodos para que el mensaje pueda ser descifrado. En cada nodo se aplica un recifrado al mensaje, multiplicando el mensaje por la clave K elevada al valor aleatorio que se esté utilizando, cambiando la apariencia del mensaje, esto se realiza durante n etapas. Una vez pasan esas etapas se comienza a descifrar. Este descifrado es un poco particular ya que no es necesario que participen todos los nodos. Solo usando T nodos se puede descifrar el mensaje, colaborativamente esos T nodos irían ayudando a descifrar el mensaje. Para descifrar el mensaje se cogen las claves privadas de cada uno de los nodos y se usan para construir la clave pública, que es el generador elevado a la clave privada. Se hacen descifrados parciales hasta que se llega al nodo T que, una vez este tiene el mensaje descifrado, se lo manda al destinatario.

Redes de cifrado vs Recifrado

Las redes de descifrado tienen un problema, y es que se tiene que pasar por todos los nodos. Según se van descifrando las capas se puede crear una traza. La ventaja es que se pueden meter las direcciones de la siguiente etapa, por lo que se puede determinar una cascada.

Las redes de ReCifrado solo necesitan un cifrado inicial, el mensaje no varía durante el tiempo, por lo que no se puede crear una traza, no tiene por que pasar por todos los nodos, solo es necesario que se pase por una cantidad de T nodos. Lo malo es que la red debe ser predefinida.

Topología de cascada

Consiste en una secuencia de fases fija a la que pertenecen cada emisor o receptor.

Free Routing

Se tiene una serie de nodos interconectados disponible y se selecciona una cantidad fija de ellos. Tiene un problema y es que no hay un punto de entrada o salida, por lo que es recomendable meter tráfico de cobertura. Si hay un atacante en estos nodos, puede insertar tráfico para trazar paquetería.

Esquemas de verificación

Este tipo de redes tienen una demostración matemática bastante fuerte detrás, por lo que es posible realizar verificaciones para saber si la red mix funciona bien o mal. Se toman como base para las operaciones

- La entrada de mensajes procesados y permutados
- Mensajes que no han sido corrompidos
- Entradas que han sido dropeadas

Se debe ir comprobando etapa a etapa, lo que genera un problema ya que implica replicar la paquetería, realizar el permutado y comprobar si hay una situación en la que el orden no varíe, que un nodo siempre envíe los paquetes a los mismos nodos, lo que sería signo de un nodo comprometido. Si queremos verificar los enlaces de las etapas se debe enviar información hacia atrás, lo que es muy costoso.

Onion Routing

Pensados para ser viables de implementar en tiempo real y ser eficientes. Todas estas redes crean una cebolla (Por las capas) hasta el destinatario. A medida que el mensaje fluye por la red, en cada nodo se quita una capa, se desvela la dirección y se envía el mensaje a esta hasta que llega al destinatario. Aquí no hay el shuffling de mix. En la comunicación intervienen:

- Un cliente que nos introduce en la red, un proxy, que es quien nos mete en la red.
- Los routers, que son los puntos intermedios, que hay 2, el entry funnel y el exit funnel.

El mensaje de un emisor entra por el nodo de entrada, circula por una serie de routers, sale por el nodo de salida y llega al destinatario. El problema es que los cifrados con clave asimétrica son muy costosos, por lo que se usa cifrado con clave compartida simétrica. En caso de que el receptor tenga que responder al mensaje se crea una cebolla de vuelta.

En el caso de tor, tenemos una versión con ciertas modificaciones sobre el modelo original, se usan claves simétricas. Hay un par de nodos disponibles, no es p2p, hay una serie de nodos intermedios que ceden organizaciones. Esto es un problema de seguridad ya que hay organizaciones que pueden tener cierto control sobre la red. Existe un directorio con la lista de nodos disponibles, tor selecciona 3 y envía el mensaje a través de ellos. Si la entrada y salida de tor son controlados por un mismo atacante, el mensaje queda comprometido. Por ello Tor tiene mecanismos para evitar que un mensaje pase por más de uno nodo de cada organización.

Se usan 3 nodos:

1. Se empieza por el nodo de entrada que permita el tipo de tráfico que se quiere enviar al destinatario
2. Se usa un nodo intermedio una sola vez. El sistema evita que el mensaje pase por dos nodos de la misma familia y trata de que vaya por nodos con cierta reputación. El Path de tor va cambiando con el tiempo, va rotando. Las claves también rotan. Los circuitos se crean de manera telescópica.
3. Se termina por el nodo de salida

Los circuitos tienen 2 segmentos, uno de el nodo de entrada al intermedio y otro del nodo intermedio a la salida. Los mensajes son de tamaños fijos de 512B para que no puedan ser distinguidos.

Una de las mejores características de tor son los **Servicios Ocultos**, que serían los dominios .onion.Estos servicios comienzan buscando un punto de introducción y selecciona un punto de encuentro, para ello se establece un cirtuito para llegar a un punto de introducción. El servicio oculto decide si responder a las respuestas que recibe o no, si responde, procede a enviar la respuesta por un path distinto. El objetivo de esto es mantener la anonimidad del servidor.