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.

From:
https://www.knoppia.net/ - **Knoppia**

Permanent link:
https://www.knoppia.net/doku.php?id=pan:niideaxd&rev=1731517029

Last update: **2024/11/13 16:57**