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).