Comunicaciones Anónimas

Todas las redes de comunicaciones usan direcciones para realizar el enrutamiento de forma que los datos pueden ser transmitidos del origen al destino. Dichas direcciones suelen ser visibles para cualquiera que observer la red. Normalmente estas direcciones son identificadores únicos de forma que todas las transacciones relacionadas con un usuario puedan ser trazadas. Estas direcciones pueden ser asociadas con personas, lo que puede comprometer la privacidad.

Teniendo este en cuenta, anonimizar los canales de comunicación se vuelve algo necesario para poder salvaguardar la privacidad de los usuarios y proteger las comunicaciones contra el análisis de tráfico. Para ello puede ser necesaria la aplicación de técnicas de anonimización sobre la capa de aplicación como autenticación anónima, protocolos de voto anónimos o divisas anónimas.

Un sistema de comunicación anónimo oculta quien se está comunicando con quien y se pueden aplicar diferentes escenarios:

- El remitente debe ser ocultado para todo el mundo, incluyendo el receptor.
- El receptor debe ser ocultado para todo el mundo, incluyendo el remitente.
- Tanto el receptor como el remitente deben ser ocultados de terceras partes, puede que hasta tengan que autenticarse el uno al otro.

Esot significa que es necesario proveer la capacidad para que los usuarios puedan usar internet sin revelar sus identidades mientras operan con normalidad. El problema es que hay una contradicción entre privacidad personal y la aplicación de las leyes, incluyendo seguridad nacional. Se pueden establecer varios niveles de anonimidad:

- La **privacidad total** puede ser garantizada, de forma que todo el mundo es anónimo:
  - Todo el mundo usa los servicios para su propio beneficio
  - Esto incluye criminales y actores maliciosos, lo que facilita las actividades ilegales sin control alguno.
- **Privacidad parcial**, las agencias que aplican la lay pueden deshacer la anonimidad para todo el mundo.
  - Esto significa que las actividades de todo el mundo pueden ser monitorizadas
  - Hay una versión ligera en la cual las agencias solo pueden deshacer la anonimidad con una orden judicial debido a la sospecha de acciones ilegales.
- **Ausencia de Privacidad**: Todo el mundo puede observar todo
  - No hay privacidad, todas las actividades son públicas.

Existen varias definiciones que pueden ser aplicadas a los sistemas de comunicación:

- **Anonimidad**: El estado de no ser identificable en un conjunto de sujetos. Requiere un conjunto de anonimidad, donde varios sujetos tienen potencialmente los mismos atributos. En cuanto a comunicaciones, los conjuntos de anonimidad consisten en sujetos que pueden ser localizados para enviar o recibir transmisiones.
- **No-Enlazabilidad**: Significa que un usuario puede usar cualquier recurso o servicio sin que sea posible enlazar los usos juntos. No se puede determinar si un usuario realizó una operación o no. Si dos elementos o acciones de interés son observadas e inspeccionadas por un atacante, no están más o menos relacionadas que las acciones anteriores.
- **No-Observabilidad**: El estado de un objeto de interés es indistinguible de cualquier otro elemento de interés. Un mensaje no puede ser diferenciado de ruido aleatorio. No se puede

identificar cuando se ha intercambiado un mensaje.
- **Pseudoanonimidad**: Se usa un pseudónimo como identificador. Puede ser asociado a un individuo. Permite reclamar responsabildiades en caso de mal comportamiento.

Existen varios modelos de ataque sobre redes de comunicaciones:

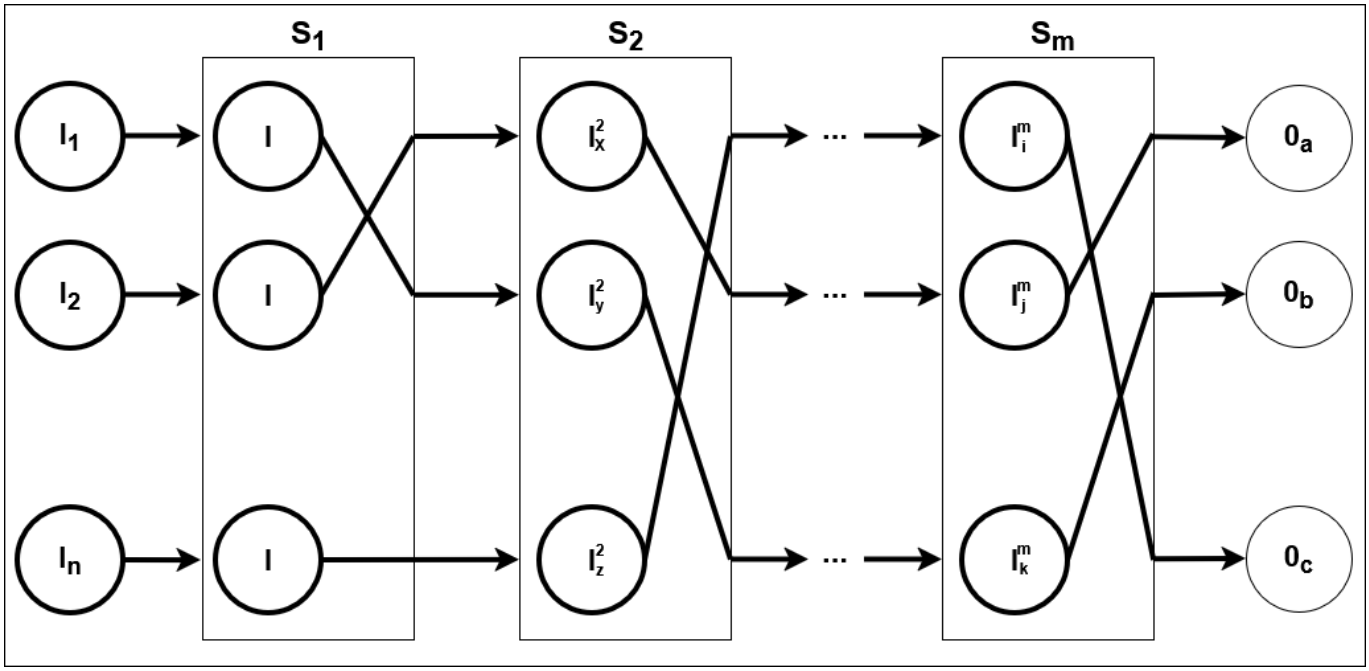
- **Tipo 1 (Atacante pasivo)**: Observalas comunicaciones y enlaces
- **Tipo 2 (Atacante pasivo con capacidades de envío)**: Además de observar las comunicaciones, el atacante puede tomar parte en el proceso emitiendo mensajes.
- **Tipo 3 (Atacante activo)**: Puede controlar todos los enlaces de comunicación, eliminar, responder, enviar o retrasar mensajes.

Requerimientos para la anonimidad en redes de comunicaciones:

- **Tráfico de cobertura**: Se envía tráfico adicional con el mensaje de una persona para enmascarar la transmisión. Si un atacante controla el tráfico de cobertura no se puede asegurar la anonimidad.
- **Tráfico embebido**: El tráfico generado por un usuario debe ser introducido de forma silenciosa y adecuada dentro del tráfico de cobertura de forma que un atacante no lo pueda distinguir. Esta función suele ser realizada por una tercera parte que agrupa varios mensajes y los embebe en una transmisión con otros. Solo se alcanza la anonimidad si hay al menos 2 partes honestas que trabajen juntas. Si hay N participantes y N-1 son deshonestos, no se puede asegurar la anonimidad.
- **Efectividad**: Si tenemos N mensajes de diferentes usuarios. K mensajes son reales, mientras que $M=N-K$ son tráfico de cobertura. La efectividad del sistema es definida por K/N donde 1 es el caso óptimo, donde todos los mensajes son reales y no es necesario tráfico de cobertura. Para alcanzar el sistema más óptimo tienen que existir N usuarios diferentes que transmitan N mensajes diferentes, para ello es necesario esperar hasta que hayan suficientes mensajes, lo que puede demorar las comunicaciones de la red.

Redes MIX

El diseño de redes mix fue creado para implemetar sistemas de correo electrónico anónimos.



- Si todos los nodos son honestos y siguen el protocolo, las salidas son permutaciones de las entradas y el contenido del mensaje se mantiene intacto.
- Si al menos uno de los nodos oculta el intercambio que hace, este es secreto, demodo que la correspondencia entre las entradas y salidas es desconocida.
- La honestidad de los nodos puede ser verificada públicamente de forma que se puede garantizar que las salidas son permutaciones de las entradas.
- Las redes mix deben funcionar correctamente incluso si falla uno de los nodos o si alguno de los nodos está comprometido.

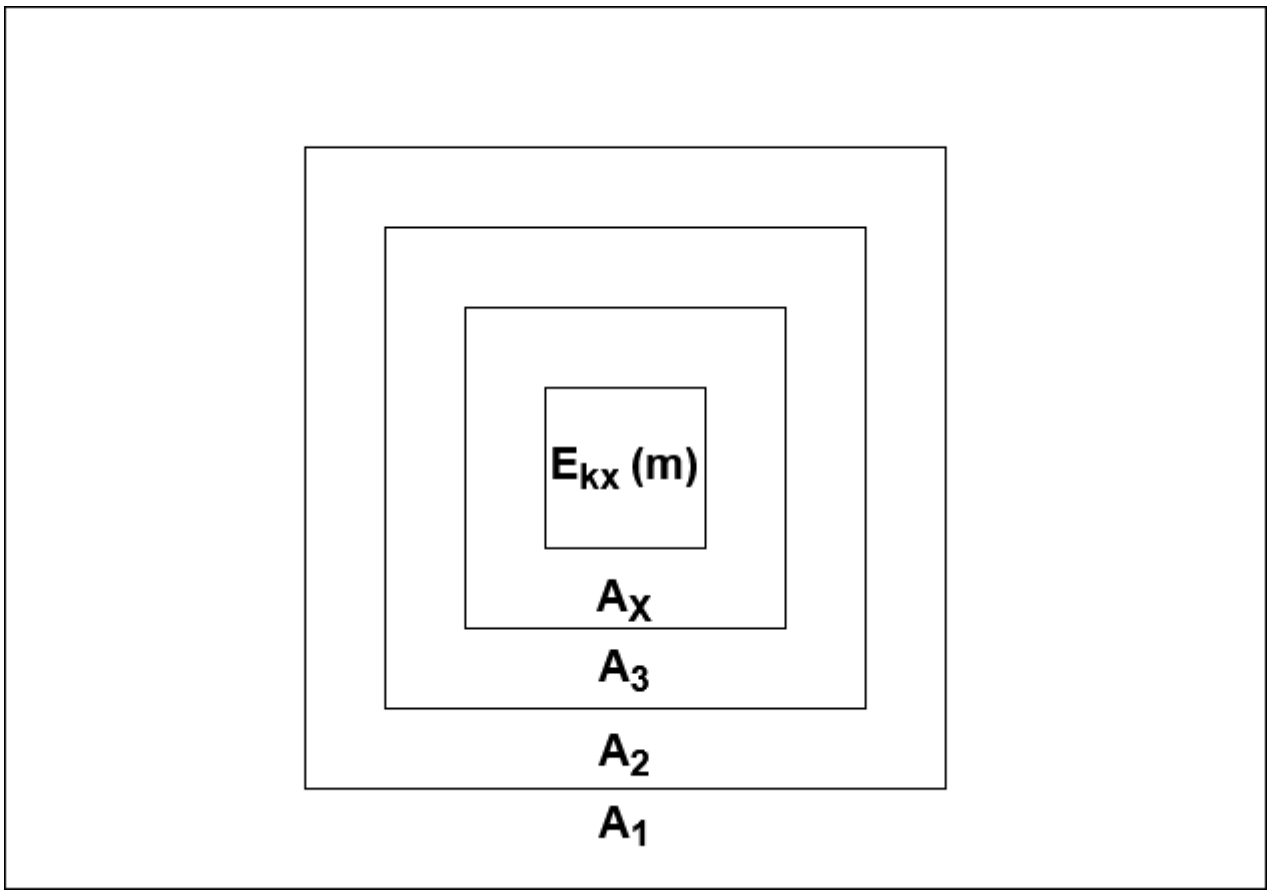
Modos de procesado

Cadena de descifrado

Esquema basado en criptografía RSA. Cada entrada (m) es secuencialmente cifrada usando la clave pública (K_i) de cada nodo.

$E_k(m,r) = A_1 || E_{k1}(A_1 || E_{k2}(A3 || ... E_{kn}(A_x || E_{kx}(m) || r_n) ... || r_2) || r_1)$

Donde A_i es la dirección de la etapa i y r_i es una cadena de caracteres aleatoria usada para aleatorizar el cifrado de la capa i



- A través de la red mix se realizan 2 operaciones en cada etapa:
  - Cada nodo i usa su clave privada K_i^{-1} para eliminar una clave de cifrado de cada una de sus entradas
  - Estos mensajes parcialmente descifrados se permutan en la etapa i antes de enviarse a la siguiente etapa con un orden aleatorio
- La comunicación en dos direcciones es posible incluyendo un RPI (Return Path Information) y claves asimétricas compartidas K^s_s junto con el mensaje m donde A_i es la dirección de la etapa i, r_i es una cadena aleatoria usada para aleatorizar el cifrado de la capa i y K_i^s son claves simétricas compartidas entre el remitente y la etapa i.
  - Por lo tanto, el receptor recibirá la siguiente salida de la red mix:

$E_kx (m || RPI || K_s^s)$

- Tras el descifrado, el receptor envía la respuesta m' a A_n como:

$E_{k_s^s} [m'] || RPI$

- El receptor no conoce el camino hasta el receptor, por lo que no puede cifrar el mensaje de la forma típica, solo puede hacerlo usando la clave K^s_s
- Cada etapa retira una capa de RPI, obteniendo la siguiente dirección y la clave de la siguiente dirección K^s_i, la cual se usa para volver a cifrar el mensaje restante.

Cadena de recifrado

Tipo de red mix basada en el sistema criptográfico ElGamal. El remitente cifra el mensaje m usando la clave pública K de la red mix:

$$E_k(m,r) = g^r || (A_x || m)K^r$$

Donde g es un generador y r es una cadena aleatoria. La clave pública K puede ser definida como:

$$K = ∏^n_{i=1} K_i = Π^n_{i=1} g^{d_i} = g^{Σ^n_{i=1}d_i}$$

Donde $K_i = g^{d_i}$ y d_i so las claves públcia y privadas de la etapa i.

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

Permanent link:
https://knoppia.net/doku.php?id=pan:comunicaciones_anonimas_v2&rev=1767737688

Last update: **2026/01/06 22:14**