REVELACIÓN DE IDENTIDADES EN SISTEMAS ANÓNIMOS

Carla Salazar Serrudo [1]

[1] Departamento de Informática y Sistemas
Facultad de Ciencias y Tecnología
Universidad Mayor de San Simón Cochabamba - Bolivia

Correo electrónico: Kanata99@hotmail.com

RESUMEN

Los mixes proveen protección a las redes de comunicación ocultando la apariencia de los mensajes, patrones, longitud y enlace entre emisores y receptores. Los ataques de descubrimiento estadístico tratan de revelar la identidad de los emisores y receptores en las redes de comunicación que son protegidas por mixes. El objetivo de nuestro proyecto es desarrollar un ataque de descubrimiento estadístico que permita identificar las relaciones entre usuarios. Se presenta un esquema teórico de modelado basado en tablas de contingencia que permite determinar las identidades de los usuarios de un sistema anónimo

PALABRAS CLAVE

Sistemas anónimos, redes mixes, ataques de revelamiento estadístico, tablas de contingencia.

INTRODUCCIÓN

En la actualidad, tanto la sociedad como las empresas, generan millones de datos a través de operaciones comerciales y mercantiles, redes sociales, dispositivos móviles y documentos, entre otros. La mayor parte de esta información es privada, puesto que se refiere al origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual o cualquier otra información personal que podría ser usada por terceros para generar daño [1].

En Bolivia, la privacidad está amparada en el artículo 21, artículo 2 de la Nueva Constitución Política del Estado (aprobada en fecha 25 de enero de 2009) que dice: "las bolivianas y los bolivianos tienen derecho: A la privacidad, intimidad, honra, honor, propia imagen y dignidad" [2]. Sin embargo, en el mundo online es difícil respetar la privacidad de las personas, ya que toda la información disponible acerca de una persona puede ser referenciada con otra y dar lugar a prácticas de violación de la intimidad [3]. También existen compañías especializadas que se dedican a compilar y vender la información, algunas con intereses comerciales y de mercadotecnia y otras con objetivos fuera de la ley. Desde la década pasada se observa una mayor preocupación por cómo se maneja la información privada de los usuarios en el ámbito gubernamental y de las empresas. Después de la filtración de información de un técnico estadunidense de la CIA al mundo, aumentaron las mesas de diálogo, investigaciones y fundamentalmente se creó toda una polémica en torno a la privacidad de los datos y lo expuestos que estamos a ser objetos de monitoreo.

PRIVACIDAD

La definición de privacidad de acuerdo a [4] es el derecho de un individuo a decidir qué información de él mismo puede ser comunicada a otro y bajo qué circunstancias. De acuerdo a los expertos, privacidad e intimidad son conceptos difíciles de definir; de cualquier forma, se considera parte de ello, a las condiciones de salud, identidad, orientación sexual, comunicaciones personales, preferencias religiosas, estados financieros, además de muchas otras características.

Las bases de la legislación respecto a la privacidad datan del año 1948, en la Declaración Universal de Derechos Humanos donde se estableció que ninguna persona debía ser sujeta a interferencias arbitrarias en su privacidad, familia, hogar o correspondencia, así como a su honor y reputación [5]. Pero, a pesar de los avances políticos y legales que se han dado, no ha sido posible resolver algunos de los problemas fundamentales para evitar los abusos que se dan todos los días. La falta de claridad y precisión en los derechos a la libertad de expresión y los límites de información son aún un problema latente.

El desarrollo de los medios de comunicación

digital, el auge del uso de las redes sociales y la facilidad de acceso a dispositivos tecnológicos, están permeando la tranquilidad de miles de personas en su vida pública y privada. Ejemplos abundan, pero la indiferencia de la población y de los gobernantes parece ser la constante. El escándalo a expensas de la intrusión y diseminación de la vida privada e íntima de las personas es inaceptable. Es un círculo vicioso que tiene su origen en la violación de un derecho, pero más cuando se lleva a las redes sociales y de ahí a la mayoría de los medios de comunicación con el pretexto de ser noticia [6].

TECNOLOGÍAS QUE MEJORAN LA PRIVACIDAD

En la década de los 80, se inició el desarrollo de las Tecnologías que Mejoran la Privacidad, cuya traducción del inglés es Privacy Enhance Technologies (PETs). Estas tecnologías se orientan a crear aplicaciones que proporcionan seguridad en las comunicaciones y transferencia de datos. Asimismo, permiten ofrecer mecanismos que protegen la privacidad de usuarios, redes o servidores [7]. Las organizaciones privadas y públicas, así como las personas, deben incluir la protección de la privacidad más allá de los típicos aspectos de integridad confidencialidad y disponibilidad de los datos.

La Comisión Europea afirma que "El uso de los PETs puede ayudar a diseñar sistemas de comunicación y servicios de forma que disminuyan la recolección y uso de datos personales y faciliten el cumplimiento de la regulación de protección de datos" [8]. En general las PETs se enfocan en [10]:

a) Reducir el riesgo de romper principios de privacidad y cumplimiento legal.
b) Reducir al mínimo la cantidad de datos que se tienen sobre los individuos.
c) Permitir a los individuos a mantener siempre el control de su información.

Varios investigadores se han centrado en proteger la privacidad y los datos personales por medio de técnicas criptográficas. Las aplicaciones PETs, tales como seguros digitales individuales o administradores virtuales de identidad, se han desarrollado para plataformas confiables de cómputo. Tradicionalmente las PETs han estado limitadas para proporcionar pseudononimato [9]. En contraste a los datos totalmente anónimos, el pseudononimato permite que datos futuros o adicionales sean relacionados a datos actuales. Este tipo de herramientas son programas que permiten a individuos negar su verdadera identidad en sistemas electrónicos que operan dicha información y sólo la revelan cuando sea absolutamente necesario. Ejemplos incluyen: navegadores web anónimos, servicios email y dinero electrónico.

COMUNICACIONES ANÓNIMAS

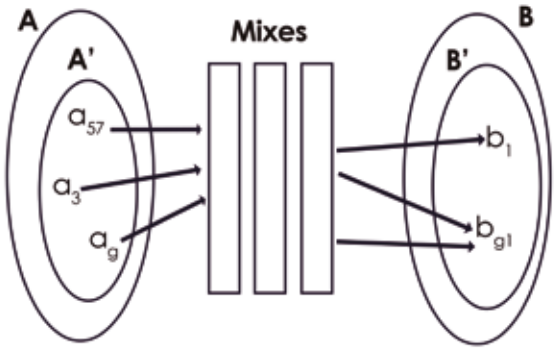
Las comunicaciones anónimas tienen como objetivo ocultar las relaciones en la comunicación. Dado que el anonimato es el estado de ausencia de identidad, las comunicaciones anónimas se pueden lograr removiendo todas las características identificables del sistema. Pitfzmann y Hansen [9] definieron el anonimato como el estado de ser no identificable dentro de un conjunto de sujetos, conocido como el conjunto anónimo.

La probabilidad de que un atacante pueda descubrir quién es el receptor de un mensaje es exactamente de $1/n$, siendo n el número de miembros del conjunto anónimo. La investigación en esta área se enfoca en desarrollar, analizar y llevar a cabo ataques de redes de comunicación anónimas. La infraestructura del Internet fue inicialmente planteado para ser un canal anónimo, pero ahora sabemos que cualquiera puede espiar la red. Un atacante externo puede identificar patrones de tráfico para deducir quién se comunica con quién, cuándo y con qué frecuencia.

REDES MIXES

En 1981, Chaum [11] introdujo el concepto de las redes mixes cuyo propósito es ocultar la correspondencia entre elementos de entrada con los de salida. Una red de mixes recolecta un número de paquetes desde diferentes usuarios llamado el conjunto anónimo y entonces cambia la apariencia de los paquetes de entrada a través de operaciones criptográficas, lo que hace imposible relacionar entradas y salidas. Las propiedades de anonimato serán más fuertes en tanto el conjunto anónimo sea mayor. Un mix es un agente intermediario que oculta la apariencia de un mensaje, incluyendo su longitud.

Figura 1. Modelo formal de un conjunto de anonimato



Fuente: Chaum, 1981 [11]

El proceso inicial para que un emisor envíe un mensaje a un receptor utilizando un sistema de mixes es preparar el mensaje. La primera fase es elegir la ruta de transmisión del mensaje; dicha ruta debe tener un orden específico antes de enviar el mensaje. La siguiente fase consiste en utilizar las llaves públicas de los mixes elegidos para cifrar el mensaje, en el orden inverso en que fueron elegidos. En otras palabras, la llave pública del último mix cifra inicialmente el mensaje, después el penúltimo y finalmente la llave pública del primer mix es usada. Cada vez que se cifra el mensaje, se construye una capa y se incluye la dirección del siguiente nodo. De esta manera, cuando el primer mix obtiene un mensaje preparado, dicho mensaje será descifrado a través de la llave privada correspondiente y será direccionado al siguiente nodo.

Las redes de mixes son una herramienta poderosa para mitigar los ataques externos al cifrar la ruta emisor- receptor. Los nodos participantes de una red mix transmiten y retardan los mensajes con el fin de ocultar su ruta. Pero es posible que puedan estar comprometidos y llevar a cabo ataques internos.

1. ATAQUES ESTADÍSTICOS

La familia de ataques estadísticos fue iniciada por Danezis en [12] donde se introdujo el ataque estadístico de revelación (SDA Statistical Disclosure Attack). En dicho trabajo se demuestra que, llevando a cabo un amplio número de observaciones por cierto período de tiempo en una red de mixes, se puede calcular la probabilidad de distribuciones de envío y recepción de mensajes y con ello revelar la identidad de los participantes en un sistema de comunicación anónimo. A partir de éste ataque se desarrollaron muchos más, tomando como base el análisis de tráfico para deducir cierta información a partir de los patrones de comportamiento en un sistema de comunicación.

Los ataques contra redes de mixes son conocidos también como ataques de intersección [13]. Se toma en cuenta la secuencia de un mensaje a través de una misma ruta en la red. El conjunto de los receptores más probables se calcula para cada mensaje en la secuencia e intersección de los conjuntos, lo que permite conocer quién es el receptor de un determinado mensaje. Los ataques de intersección se diseñan basándose en la correlación de los tiempos donde emisores y receptores se encuentran activos. Al observar los elementos que reciben paquetes durante las rondas en las que un emisor está enviando un mensaje, el atacante puede crear un conjunto de receptores más frecuentes de éste emisor. La información proporcionada a los atacantes es una serie de vectores representando los conjuntos de anonimato observados de acuerdo a los t mensajes enviados por el emisor.

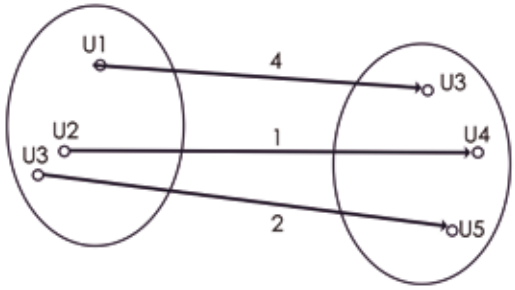
Dentro de la familia de ataques estadísticos, cada uno de ellos se modela con un escenario muy específico. En algunos casos poco semejantes al comportamiento de un sistema de comunicación real. Algunos asumen que el emisor tiene exactamente *m* receptores y que envía mensajes a cada uno de ellos con la misma probabilidad, o bien son ataques que se enfocan en un solo usuario como soluciones individuales que son interdependientes, cuando la realidad indica cuestiones diferentes.

2. ANTECEDENTES DE LA PROPUESTA DE ATAQUE

La propuesta de este trabajo se enfoca en obtener información de la comunicación entre usuarios de una red. La información utilizada es el número de mensajes enviados y recibidos por cada usuario. Esta información es obtenida en rondas determinadas por lotes de mensajes de igual tamaño.

El atacante obtiene información de cuántos mensajes envía y recibe cada usuario de cada ronda. Normalmente, el conjunto de emisores y receptores no es el mismo, aún cuando algunos usuarios puedan ser emisores y receptores en alguna ronda en particular. Además, el número total de usuarios en el sistema N no está presente en cada ronda, pues solo una fracción de ellos está recibiendo o enviando mensajes [15]¡Error! No se encuentra el origen de la referencia.. En la Figura 1 se muestra una posible ronda, que por razones didácticas se compone de un mínimo de usuarios.

Figura 2. Relación entre emisores y receptores.



Fuente: Silva, Portela y García Villalba, 2014 [1]

La información de esta ronda se puede representar en una tabla de contingencia (vea la Tabla I), donde el elemento (i, j) representa el número de mensajes enviados del usuario i al usuario j.

Tabla 1. Ejemplo de Tabla de Contingencia

Receptores	Emisores			
	U3	U4	U5	Total enviados
U1	4	0	0	4
U2	0	1	0	1
U3	0	0	2	2
Total recibidos	4	1	2	7

Fuente: Silva, Portela y García Villalba, 2014 [1]

El atacante solamente ve la información presente en las marginales agregadas donde, las filas representan el número de mensajes enviados por cada usuario, y las columnas, el número de mensajes recibidos por cada usuario, según aparece en la Tabla II.

Tabla 2. Ejemplo de Tabla de Contingencia con información de Marginales

Receptores	Emisores			
	U3	U4	U5	Total enviados
U1				4
U2				1
U3				2
Total recibidos	4	1	2	7

Fuente: Silva, Portela y García Villalba, 2014 [1]

Por medio de los valores marginales es posible obtener información importante. Las cotas de los elementos pueden ser útiles, ya que nos pueden proporcionar relaciones directas entre usuarios. Las cotas de Fréchet sobre tablas de contingencia son muy conocidas en estudios de revelación. Se denota con nij el contenido del elemento (i, j), n_{i+} el valor marginal de la fila i, n_{+j} el valor marginal de la columna j y n el total. Las cotas de Fréchet se establecen como se muestra en la ecuación 1.

$$max(n_{i+} + n_{+j} - n, 0) \leq n_{ij} \leq mín(n_{i+}, n_{+j}) \quad \textbf{(1)}$$

Por ejemplo, partiendo de la Tabla II, se obtienen las cotas presentadas en la Tabla III.

Tabla 3. Ejemplo de Tabla con Cotas Obtenidas

Receptores	Emisores			
	U3	U4	U5	Total enviados
U1	(1,4)	(0,1)	(0,2)	4
U2	(0,1)	(0,1)	(0,1)	1
U3	(0,2)	(0,1)	(0,2)	2
Total recibidos	4	1	2	7

Fuente: Silva, Portela y García Villalba, 2014 [1]

3. ALGORITMO DE ATAQUE

El objetivo del algoritmo que se propone es extraer información relevante sobre las relaciones entre cada par de usuarios. El atacante es capaz de observar cuántos mensajes son enviados y recibidos, es decir las sumas marginales por fila y columna de cada ronda 1,…, T donde T es el número total de rondas. En cada ronda sólo consideramos usuarios que reciben y envían mensajes. Por lo tanto, decimos que un elemento (i, j) está presente en una ronda si las marginales correspondientes son diferentes a 0. Se denomina "cero trivial" a los elementos que representan pares de usuarios que nunca han coincidido en ninguna ronda.

Algoritmo

1. Comenzar con la columna 1, fila 1: generar n_{11} de una distribución uniforme entera donde $i = 1, j = 1$.
2. Para cada elemento n_{k1} en esta columna, se calculan nuevas cotas para n_{k1} hasta k-1, a partir de la siguiente ecuación.

$$máx((0, (n_{+1} - \sum_{i=1}^{k-1} n_{i1}) - \sum_{f=k+1}^{r} n_{i+}) \leq n_{ij} \leq mín(n_{k+}, n_{+j} - \sum_{f=1}^{r} n_{i1}) \quad \textbf{(2)}$$

El elemento n_{k1} se genera entonces según un entero uniforme.

3. El último elemento de la fila se rellena automáticamente al coincidir las cotas superior e inferior, haciendo $n_{(k+1)}+ = 0$ por conveniencia.

4. Cuando se completa la columna, ésta se elimina de la tabla y se recalculan las marginales por fila n_{i+} y el valor n.

5. La tabla ahora tiene una columna menos y se repite el proceso hasta llenar todos los elementos.

Este algoritmo permite generar cualquier tamaño de tabla factible en tiempos absolutamente aceptables. Por ejemplo: se puede generar un millón de tablas factibles en menos de 3 minutos.

Al final, lo que se obtiene son una serie de tablas factibles generadas para cada ronda. Por lo que la media de cada elemento sobre todas las tablas para todas las rondas es una estimación de su valor real. La media obtenida por elemento y ronda se agrega sobre todas las rondas la cual representa un estimado de la tabla agregada $\hat{A}$. Para cada elemento, se estima la probabilidad de cero, calculando el porcentaje de tablas con elemento cero para cada ronda en que el elemento está presente y multiplicando las probabilidades obtenidas para todas esas rondas. En la tabla resultante los elementos se ordenan por su probabilidad de cero a excepción de los elementos que son cero triviales. De esta manera, los elementos con menor probabilidad de ser cero son los que se consideran candidatos a tener una relación.

Para llevar a cabo la clasificación, se selecciona un punto de corte p y se considera "*celdas cero*" si la probabilidad de cero > p, en tanto las "celdas positivas" son aquellas donde la probabilidad de cero < 1 – p. Aquellas celdas que no entran en estas dos categorías se les llama "no clasificadas".

Este ataque se tiene planificado realizar en un sistema de correo electrónico y en principio, se están simulando los datos de este sistema electrónico.

CONCLUSIONES

El objetivo de este trabajo es desarrollar un ataque estadístico para revelar la identidad de emisores y receptores de una red de comunicación que esté protegida por mixes. Para este efecto, se ha presentado un método basado en tablas factibles para detectar relaciones en un entorno de comunicaciones, donde la información obtenida es incompleta. Se obtienen una serie de tablas factibles no repetidas, se calcula la frecuencia relativa para cada celda y se obtiene una aproximación a la distribución de probabilidad del número de mensajes entre emisores y receptores.

En este trabajo se están simulando datos de un entorno de correo electrónico. El próximo paso, será conseguir los datos reales del sistema de correo electrónico de alguna institución para efectuar las pruebas reales.

Sin embargo, en las pruebas realizadas, se ha observado que el comportamiento del algoritmo es altamente eficiente y los resultados son muy alentadores al tiempo de detectar relaciones entre los usuarios del sistema de comunicación.

Finalmente, aún es necesario realizar mayor número de pruebas para determinar con cuántos usuarios, número de mensajes y rondas el algoritmo de tablas factibles da mejores resultados, dado que el algoritmo propuesto se ve afectado por estos factores.

BIBLIOGRAFÍA

- A.G. Silva Trujillo, J. Portela García-Miguel, L.J. García Villalba, "Refinamiento probabilístico del ataque de revelación de identidades", a presentarse en la XIV Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2014), Alicante, España, Septiembre 2014.

- Nueva constitución política del Estado Plurinacional de Bolivia, http://pdba.georgetown.edu/Constitutions/Bolivia/constitucion2009.pdf, extraído 25 mayo de 2014.

- B. Krishnamurthy. "Privacy and Online Social Networks: can color less green ideas sleep furiosly?" IEEE Security and Privacy, Vol. 11, No. 3, pp. 14-20, Mayo 2013.

- A. Westin. "Privacy and Freedom", Vol. 25, New York: Atheneum: Washington and Lee Law Review, 1968.

- Declaración de Universal de los Derechos Humanos de 1948, http://www.ohchr.org/Documents/Publications/ABCannexessp.pdf, extraído 25 mayo de 2014.

- R. Gross y A. Acquisti. "Information revelation and privacy in online social networks", Proc. of the 2005 ACM workshop on Privacy in the electronic society, Alexandria, VA, USA., pp.71-80, Noviembre 2005.

- L. Fritsch. "State or the art of privacy-enhancing technology (PET)", Norwegian Computing Center Report, Oslo, Norway, 2007.

- European Commission. "Press release: Privacy Enhancing Technologies (PETs)", 2 Mayo 2007.

- A. Pfitzmann y M. Hansen. "Anonymity,unlinkability, unobservability, pseudonymity, and identity management: a consolidated proposal for terminology", TU Dresden, Febrero 2008.

- C. Diaz y S. Gurses. "Understanding the landscape of privacy technologies", Proc. of the Information Security Summit, pp. 58-63, Prague, Czech Republic, Mayo, 2012.

- D. Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms", Comm. ACM, Vol. 24, No. 2, pp. 84-90, Febrero 1981.

- G. Danezis. "Statistical disclosure attacks: Traffic confirmation in open environments". Proc. Security and Privacy in the Age of Uncertainty, (SEC2003), Kluwer, pp. 421-426, May 2003.

- J. F. Raymond. "Traffic Analysis:

- Protocols, Attacks, Design Issues, and Open Problems", Proc. of International Workshop on Designing Privacy nhancing Technologies: Design Issues in Anonymity and Unobservability", New York, NY, USA, 2001.

- J. Portela García-Miguel, L.J. García Villalba, "Disclosing users relationships in anonymity systems", Computers & Security, October 2013.