¿Será que el remedio es peor que la enfermedad?

Peña Tarqui Rosmery
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
rosy06_05@hotmail.com

RESUMEN

En este trabajo se describe si el nuevo padrón electoral implementado en Bolivia podría ser vulnerable a delitos informáticos y qué papel jugaría en esta área la informática forense.

Palabras clave

Biometria, informatica forense, sistemas informaticos, sistemas biometricos.

1. INTRODUCCIÓN

La biometría es la ciencia que usa las características biológicas o de comportamiento para identificar una persona. Entre las biometrías más conocidas están: la biometría de la huella digital, facial, de la mano, del iris y retina, de la voz, de la firma, etc. Y otras que están en investigación como el DNA, los olores, ritmos de tecleado etc.

Es bien conocido que nada es perfecto y que ningún sistema es 100% seguro, de esta realidad no escapan los sistemas biométricos.

2. SEGURIDAD EN LO SISTEMAS BIOMETRICOS

Hay una serie de fuentes de ataque que a lo largo de los años han intentado burlar la seguridad de los sistemas biométricos. Un informe publicado en 1998 por Networking Computing acerca de la susceptibilidad en el uso de los sistemas biométricos y el uso de huellas falsas, estableció que 4 de 6 dispositivos probados fueron susceptibles a ataques de huellas falsas.

Adicionalmente Tsutomu Matsumoto publico el artículo titulado “dedos de goma” en 2002, en su investigación demostró que dedos falsos de gelatina tuvieron un alto porcentaje de aceptación en los dispositivos biométricos con un porcentaje entre 68 y 100 de aceptación por parte de los sistemas biométricos.

En noviembre de 2002 se publico los resultados de una investigación hecha sobre una variedad de dispositivos biométricos a partir de una serie de ataques spoofing exitosos, simulando ataques “man- in- the-middle” para capturar las tramas que eran transmitidas entre los dispositivos y los sistemas biométricos.

En diciembre de 2005 la universidad de Clarckson presentó los resultados de sus investigaciones en laboratorio donde se demostró un 90% de falsas verificaciones en el uso de los dispositivos biométricos a partir de impresiones digitales de cadáveres y huellas sintéticas. Sin embargo cuando se integraron controles de detección en vivo en los dispositivos el porcentaje de falsa verificación se redujo a menos del 10%. Estas investigaciones han venido a establecer métodos de spoofing en los lectores biométricos.

3. ATAQUES BIOMÉTRICOS.

Se han establecido una serie de puntos de ataque en los sistemas biométricos, además del uso de huellas falsas existen otra serie de ataques que requieren el acceso a los sistemas de procesamiento biométrico que tal vez representan una fuente de mayor riesgo, los cuales pueden resumirse en los siguientes apartados.

3.1. Biometría falsa

Es representada por cualquier huella falsa utilizada para burlar un sistema biométrico. Estos incluyen huellas de cadáveres, y huellas falsas hechas con silicona, gelatina, plástico, arcilla modelada o cualquier otra sustancia

3.2. Ataques de Reenvió/ Introducción de datos falsos

Consiste en la captura y reenvió de datos relacionados con la representación biométrica, se basa en la introducción de tramas de datos biométricos falsos entre el dispositivo biométrico y el sistema de procesamiento.

3.3. Reutilización de residuos

Algunos sistemas pueden retener en la memoria las imágenes y los modelos de las huellas capturadas, si un atacante puede acceder a memoria puede obtener valiosa información biométrica y reutilizarla. Limpiando la memoria y prohibiendo el uso de modelos iguales de manera consecutiva proporciona una efectiva forma de defensa.

3.4. Interferencia del proceso de extracción

Consiste en interferir el proceso de extracción de características biométricas para introducir datos falsos y forzar un nuevo procesamiento. Este ataque puede ser usado también para deshabilitar el sistema constituyéndose en una forma de ataque de denegación de servicio.

3.5. Interferencia de la verificación/Verificación falsa

Consiste en interferir o ignorar la decisión del proceso de verificación reemplazándola con una verificación valida. Ajustes en los controles de tolerancia del sistema biométrico en particular el porcentaje de falsa aceptación (FAR: false accept rate) puede dar lugar a que el sistema acepte huellas de baja calidad o huellas incorrectas. Por esta razón el departamento de defensa de los estados unidos recomienda un FAR no mayor a 1 en 100,000 y un porcentaje de rechazo false (FRR: false reject rate) no mayor a 5 en 100.

3.6. Intercepción del canal de almacenamiento e introducción de datos.

Tal vez el ataque que presenta las más significativas consecuencias, ya que puede comprometer el procesamiento del sistema y la base de datos biométrica.

3.7. Modificación no autorizada de un modelo biométrico

Los modelos biométricos pueden ser alterados, reemplazados o adicionados en el sistema. Adicionando estos modelos se puede burlar el sistema fácilmente presentando una huella real (pero no autorizada) y ser reconocida por el sistema como una característica biométrica válida.

3.8. Interferencia de la decisión / Falsa aceptación

Este tipo de ataque ignora la decisión del proceso de verificación e introduce un resultado de falsa aceptación entre el sistema biométrico y el dispositivo final (por ejemplo una puerta eléctrica o autorización para acceder a una base de datos con información confidencial, un cajero automático etc.).

4. DEFENSAS

Existen una serie de controles que permiten mitigar los riesgos de los ataques definidos anteriormente, estos son controles complementarios y la seguridad no debería centrarse en un método simple. Entre los controles más relevantes están:

4.1. Datos aleatorios.

El sistema requiere que el usuario registre múltiples características biométricas, posteriormente el proceso de verificación solicitara múltiples huellas al azar, de esta manera se adiciona complejidad a los intentos de ataque a los dispositivos biométricos, por otro lado reduce el riesgo de los ataques a los residuos dejados en los dispositivos o el uso de huellas sintéticas.

4.2. Detección en vivo

Un elemento clave para la defensa de un ataque spoofing es la implementación de controles en vivo para verificar que la huella presentada corresponde a una persona viva y no una persona muerta, o una huella falsa. Estos controles pueden estar incorporados en los dispositivos biométricos o ser parte de dispositivos adicionales por ejemplo: oximetría del pulso donde Patrones de medición respiratoria; espectroscopia corporal, el pulso y la oxigenación de la sangre son medidas, determinando la absorción calorífica de los cuerpos, grasas, pigmentación de la medición térmica, etc.

4.3. Biometría múltiple

Al igual que los datos aleatorios este control adiciona un nivel mayor de complejidad a los ataques, este control requiere el uso de más de una tecnología biométrica por ejemplo: biometría de la huella y del iris. Sin embargo este control adiciona también complejidad a los procesos de autenticación.

4.4. Criptografía y firmas digitales

La encriptación proporciona un medio efectivo para cifrar y proteger la información que atraviesa la red de ataques de intercepción e introducción de datos falsos, por otro lado las firmas digitales proporcionan un medio para garantizar que los datos no fueron modificados por el atacante.

4.5. Limpieza de la red

Así como con todas las tecnologías existen un conjunto de buenas prácticas para el buen manejo de la red que son aplicables tanto a la biometría como a otras tecnologías, ejemplos incluyen ITIL, ISO 17799 y/o COBIT.

4.6. Seguridad Física

La seguridad física es a menudo el sistema más barato y más efectivo sobre todo para proteger el acceso físico a los dispositivos biométricos, al mismo tiempo la presencia de guardias puede proteger a los usuarios autorizados de ataques coercitivos (obligar o convencer al usuario autorizado a colocar su huella para facilitar el acceso a otro usuario no autorizado).

Al mismo tiempo una revisión periódica de los dispositivos permitirá mitigar el riesgo de usar los residuos de las impresiones digitales y también para sanitizarlos a efectos de protección de la salud de los usuarios.

Por último el acceso físico a los dispositivos biométricos constituye el medio más fácil de iniciar un ataque al sistema.

5. ¿QUÉ ES LA INFORMÁTICA FORENSE O FORENSIC?

El valor de la información en nuestra sociedad, y sobre todo en las empresas, es cada vez más importante para el desarrollo de negocio de cualquier organización. Derivado de este aspecto, la importancia de la Informática forense -sus usos y objetivos- adquiere cada vez mayor trascendencia.¿En qué consiste esta técnica relativamente reciente?

- Garantiza la efectividad de las políticas de seguridad y la

protección tanto de la información como de las tecnologías que facilitan la gestión de esa información. Consiste en la investigación de los sistemas de información con el fin de detectar evidencias de la vulneración de los sistemas.

- Cuando una empresa contrata servicios de informática forense puede perseguir objetivos preventivos, anticipándose al posible problema u objetivos correctivos, para una solución favorable una vez que la vulneración y las infracciones ya se han producido.
- Las distintas metodologías forenses incluyen la recogida segura de datos de diferentes medios digitales y evidencias digitales, sin alterar los datos de origen. Cada fuente de información se cataloga preparándola para su posterior análisis y se documenta cada prueba aportada. Las evidencias digitales recabadas permiten elaborar un dictamen claro, conciso, fundamentado y con justificación de las hipótesis que en él se barajan a partir de las pruebas recogidas.
- Todo el procedimiento debe hacerse tenido en cuenta los requerimientos legales para no vulnerar en ningún momento los derechos de terceros que puedan verse afectados. Ello para que, llegado el caso, las evidencias sean aceptadas por los tribunales y puedan constituir un elemento de prueba fundamental, si se plantea un litigio, para alcanzar un resultado favorable.

6. ¿PODRÍAMOS HABLAR DE INFORMÁTICA FORENSE EN ESTE PROCESO DE EMPADRONAMIENTO ELECTORAL?

Será que "el remedio sea peor que la enfermedad!", es un viejo dicho que fácilmente podría ser utilizado en pleno proceso del nuevo registro electoral, bajo la tecnología biométrica. Por un lado es una gran cosa para un país tercermundista como el nuestro que estemos alineándonos a la tecnología, sin embargo es importante que hagamos las siguientes reflexiones:

1. Hay otro dicho que dice que dice: "Si UD cree que la tecnología resolverá sus problemas, entonces no ha entendido sus problemas y tampoco a la tecnología". Con el nuevo registro biométrico, algunos creen que vamos a superar uno de nuestros grandes males, como es la "corrupción y el fraude electoral", creer esto, es simplemente pensar ingenuamente, porque si no hacemos las cosas correctamente y seguimos ciertos patrones, la corrupción y el fraude será mayor, y lo que es peor, más difícil de ser detectado. (pe. Manipulación informática).

2. Vemos publicidad para "registrar nuestra huella" y se dice que con eso estamos aportando a la democracia. Efectivamente por nuestra parte seguro que queremos aportar a la democracia, pero, y ¿que, de las medidas de seguridad que deberían ser implementadas para nuestra posterior seguridad ?

3. Cuando hablo de este último punto, me estoy refiriendo que tanto las autoridades de la corte electoral, del gobierno, políticos y todos cuantos opinan, no se están refiriendo a un enorme riesgo que trae consigo el nuevo sistema de registro electoral como el es "la protección de nuestra identidad".

4. Si señores, la protección de nuestra identidad, nuestra información, nuestros datos, es una obligación del gobierno y de sus autoridades y es un derecho que nosotros debemos exigir antes de ir como "corderitos" a los puntos de registro biométrico.

5. En términos sencillos, lo que esperamos con esta reflexión es llegar al ciudadano común, que merece que se les explique de manera clara que la seguridad de su información en estas circunstancias, podría, NO ESTAR ASEGURADA, y que se corre UN GRAN RIESGO, con nuestros datos.

6. Existen normas, estándares y certificaciones que nos permiten evaluar los procedimientos de la recolección de datos, el traslado de información digital, el almacenacimiento de esa información, la protección y otros aspectos que no hemos escuchado de ninguna autoridad electoral que diga que se están cumpliendo y mejor mostrarnos evidencias de ello. Y de los políticos, peor, como siempre solo nos utilizan para la hora del voto.

7. CONCLUSIONES

Los sistemas biométricos han sido comúnmente usados en los últimos años como medios de autenticación en muchas culturas, países y jurisdicciones, al mismo tiempo las mejoras tecnológicas, precios más bajos e innovaciones principalmente en la biometría de huella digital va creciendo cada año. Finalmente la seguridad física y las buenas prácticas en la administración de la red permitirán establecer controles adecuados para mitigar el riesgo de ataques a los sistemas biométricos.

Reflexionemos…Y ojala que nuestras autoridades mejoren esta situación y se lleve una auditoria informática al finalizar el proceso de empadronamiento y se haga uso de la informática forense para resguardar nuestros datos y no tengamos enfrentar un escenario crítico semejante a lo descrito.

8. REFERENCIAS

[1] **www.yanapti.com/fca**

[2] Anonymous. Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network, Second Edition. Indianapolis, Indiana: Sams, 1998.

[3] Casey, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. San Diego: Academic Press, 2000.