Ataque de trazabilidad a pasaporte electrónico venezolano

Medición y análisis de resultados

Antonio R. Quirós S.
Modelado, Simulación y Optimización
Máster en Ciencia y Tecnología Informática
Universidad Carlos III de Madrid

***Abstract*—Los e-Passports han sido emitidos desde 2004 como una alternativa electrónica a lo documentos de identificación de viajeros, tradicionalmente emitidos en papel. Estos pasaportes cuentan con un tag RFID y un protocolo de seguridad que protege la información en el almacenada. Sin embargo, Tom Chothia y Vitaliy Smirnov lograron probar que, sin necesidad de vulnerar el protocolo de autenticación, se puede hacer un ataque de trazabilidad a los pasaportes de diferentes nacionalidades si cuentan con una vulnerabilidad en las respuestas emitidas[1]. En este trabajo se reproduce el ataque presentado por Chothia y Smirnov sobre pasaportes Venezolanos y determinar, analizando los resultados obtenidos, la existencia de la vulnerabilidad.**

Keywords—e-passport, pasaporte venezolano, trazabilidad.

I. Introducción

El e-Passport es un pasaporte combinado (papel – electrónico) el cual contiene información biométrica del titular que puede ser usada para autenticar la identidad del portador. Utiliza tecnología contact-less smart card con un chip RFID que permite almacenar la información que se encuentra impresa así como también un conjunto de datos adicionales. Los pasaportes electrónicos están desarrollados bajo las especificaciones de la International Civil Aviation Organization (ICAO) para los MRTD (Machine Readable Travel Document).

Estos pasaportes utilizan un protocolo de autenticación llamado BAC (Basic Access Control Authentication), el cual garantiza que solo partes autorizadas puedan acceder de forma remota a la información almacenada en el pasaporte. La autenticación la realiza mediante comunicación de mensajes entre el pasaporte y el lector. Para esto, el pasaporte está preparado con un set de posibles mensajes de respuesta ante cada solicitud realizada con el lector.

Richter, Mostowski y Poll lograron comprobar la posibilidad de determinar la nacionalidad de un pasaporte, dado los mensajes de respuesta que emitía; esto debido a la "libertad" existente en la implementación del estándar de la ICAO para este protocolo.

Chothia y Smirnov extendieron este trabajo y comprobaron que es posible realizar un ataque de trazabilidad a un pasaporte usando los mensajes de respuesta emitidos ante ciertas consultas; y, en los casos donde no se detecta vulnerabilidad, hacen una medición de los tiempos de respuesta ya que, de haber diferencia, el pasaporte es trazable.

En este trabajo replicamos el ataque de trazabilidad realizado por Chothia y Smirnov sobre pasaportes electrónicos venezolanos. En primer lugar se prueba si existe posibilidad de trazar un pasaporte venezolano por sus mensajes de error; comprobándose que no existe tal vulnerabilidad. Se continúa el trabajo entonces, haciendo una medición de los tiempos de respuesta del pasaporte y ver si existe diferencia significativa entre ambas respuestas; de ser así, el pasaporte venezolano sería vulnerable. Después del análisis de resultados se comprueba que no se puede concluir la inexistencia de tal vulnerabilidad en estos pasaportes.

A continuación, en la Sección II se explica detalladamente el protocolo de autenticación BAC; en la Sección III se detalla brevemente el trabajo de Richter, Mostowski y Poll; en la Sección IV el ataque de trazabilidad propuesto por Chothia y Smirnov; en la Sección V se detalla la implementación llevada a cabo para este trabajo; en la Sección VI se muestran los resultados obtenidos y el análisis de los mismos y en la Sección VII se plantean las conclusiones obtenidas.

II. Basic Access Control Authentication

Basic Access Control es un mecanismo creado para garantizar que solo partes autorizadas puedan leer de forma remota la información personal almacenada en los pasaportes con RFID.

Este protocolo utiliza el número del pasaporte, fecha de nacimiento y fecha de vencimiento para negociar una clave de sesión. Esta clave se usa para encriptar la comunicación entre el pasaporte y el lector. Estos datos usados para negociar la clave se encuentran impresos físicamente en el pasaporte; por lo que para iniciar la comunicación, es necesario tener acceso físico al documento.

La comunicación comienza con el Lector enviando un "challenge" al pasaporte; éste responde con un número aleatorio NT. Luego el lector genera su parte de la clave KR y un número aleatorio propio NR; y usando la información almacenada en el pasaporte (Número de pasaporte, fecha de nacimiento y fecha de vencimiento) encripta su mensaje (NR, NT y KR; además calcula una MAC del paquete enviado usando los mismos datos y los envía al pasaporte; al recibirlos el pasaporte verifica que la MAC sea correcta, es decir, que haya sido calculada usando los datos correctos impresos en el pasaporte y que concuerde con el mensaje recibido; de ser así, el pasaporte calcula su parte de la clave KT y la envía en un mensaje al lector junto con el número aleatorio recibido (NT, NR, KT); este mensaje, una vez más, va encriptado usando los datos impresos en el pasaporte; además junto con el mensaje envía una MAC calculada del paquete, tal como lo hizo el

Lector anteriormente. Al recibirlo; el lector usa su parte de la clave (KR) junto con la que recibió (KT) y calcula la clave general para la comunicación; este mismo procedimiento es realizado por el pasaporte.

III. Identificación de nacionalidad

La ICAO ha especificado el estándar para la emisión de pasaportes electrónicos; sin embargo, cada país cuenta con una implementación diferente del estándar. Richter et al. explotaron este detalle para demostrar que es posible deducir la nacionalidad de un pasaporte, de acuerdo a los mensajes de error que éste arroja. Chothia y Smirnov probaron esta vulnerabilidad, específicamente analizando los mensajes "Answer to Reset" (ATR) devueltos por el pasaporte ante una solicitud de Reset.

IV. Ataque de Trazabilidad

Un ataque de trazabilidad no implica un riesgo para toda la información almacenada en el pasaporte, pero sin embargo, si representa una verdadera amenaza para la privacidad de cualquiera que porte tal dispositivo. Poder identificar al portador de un determinado pasaporte, y detectar su presencia en cierta ubicación puede ser usado con fines malintencionados, como para detonar una bomba, por ejemplo.

De acuerdo a la ICAO todos los pasaportes deben responder a los mensajes retornando un código de error si el mensaje fue incorrecto o inesperado. En un caso específico, los pasaportes franceses presentan una vulnerabilidad en el protocolo BAC debido a los mensajes de error que retorna dependiendo de la consulta realizada.

Si se consulta al pasaporte con una MAC errónea, este responde con código 6300 "No information given". Si por el contrario, se consulta con una MAC correcta pero con con el número aleatorio NT incorrecto la respuesta será 6A80 "Incorrect parameters".

Para poder explotar esta vulnerabilidad, el atacante debe escuchar una comunicación exitosa entre el pasaporte y un lector (en un aeropuerto, por ejemplo); y almacenar un mensaje correcto. Después, para intentar identificarlo, debe reenviar ese mensaje almacenado; si recibe como respuesta "6300", se sabe que la MAC fue calculada con datos incorrectos, por lo que no se trata del mismo pasaporte; por el contrario, si se recibe como respuesta "6A80", significa que la MAC es correcta (Datos correctos para cálculo de la clave) pero el número aleatorio interno es incorrecto; esto indica que efectivamente se ha comunicado con el mismo pasaporte y ha sido ubicado.

El pasaporte venezolano (como en algunas otras naciones) no cuenta con esta vulnerabilidad, debido a que en ambos casos, el mensaje de respuesta es el mismo ("6300"); sin embargo Chothia y Smirnov proponen otro ataque, basado en los tiempos de respuesta.

Este ataque se basa en la idea de que, el pasaporte emite una respuesta a una MAC errónea más rápido de lo que lo hace por una MAC correcta pero número aleatorio incorrecto. Es decir; si se logra almacenar un mensaje correcto, como se explicó anteriormente, luego hay que enviar un mensaje incorrecto (MAC errónea) al pasaporte y medir el tiempo de respuesta. Luego se envía el mensaje (correcto) almacenado y se mide el tiempo de respuesta. Si ambos tiempos de respuesta son diferentes, se habría ubicado un pasaporte.

Este fenómeno se daría debido a que el pasaporte (teóricamente) primero verifica la MAC y, si es correcta verifica el contenido; por ende, se tienen dos escenarios: a) El pasaporte recibe una MAC errónea, la detecta y envía una respuesta inmediatamente, cancelando cualquier otro cómputo, en un tiempo T1; b) La MAC es correcta, por lo que el pasaporte continúa su procedimiento y verifica el contenido, donde determina que es incorrecto y envía entonces una respuesta; esto lo hace en un tiempo T2. Teóricamente si T2 es mayor a T1 (Debido al cómputo adicional de verificar el contenido) el pasaporte es vulnerable.

V. Implementación

Para llevar a cabo este ataque se desarrolló una aplicación en Android para establecer la comunicación con el pasaporte via NFC. Esta aplicación se autentica correctamente mediante el protocolo BAC y almacena un mensaje y MAC correcta, simulando así lo que haría el atacante al "escuchar" una comunicación entre el pasaporte y el lector. Este mensaje y MAC correctos son usados luego en el ataque.

La aplicación luego cuenta con dos funciones para hacer el ataque de trazabilidad por tiempo al pasaporte. "Replay Timing" reenvía el mensaje correcto previamente almacenado, un número parametrizable de veces y calcula el tiempo medio.

"Wrong Data Timing" reenvía un mensaje de autenticación con datos incorrectos (Específicamente encripta los mensajes usando como número de pasaporte "000000000"); esto lo hace el mismo número parametrizable de veces usado anteriormente, y también calcula el tiempo medio.

Ambas funciones, además del tiempo medio obtenido, reportan cada uno de los tiempos medidos en cada mensaje enviado; esta salida es la que usamos para el análisis.

Esta implementación se desarrolló usando Android Studio y la librería JMRTD para la comunicación con dispositivos RFID y tarjetas inteligentes.

VI. Pruebas y Resultados

Para las pruebas, se hizo la ejecución de la aplicación usando un teléfono LG Google Nexus 5, con Sistema Operativo Android 6.0.1. Como objeto de prueba se utilizó un pasaporte electrónico venezolano.

Se parametrizó el número de repeticiones de cada ataque en 100 y se realizó la ejecución un total de 5 veces cada ataque, de esta forma se obtuvieron 500 mediciones de tiempo de respuesta para el Replay Attack (MAC Correcta) y 500 mediciones de tiempo de respuesta para el Wrong Data Attack (Mensaje con MAC incorrecto).

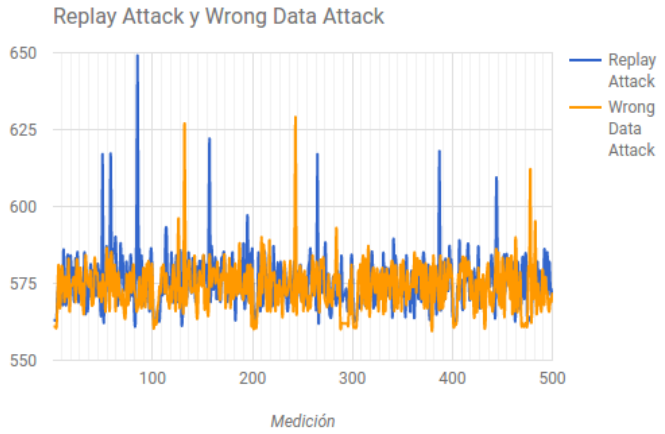
Con esto podemos plantear una prueba de comparación de medias ya que tenemos dos muestras independientes (Respuestas de Replay Attack y Wrong Data Attack) y una variable dependiente (Tiempo de respuesta). Para la prueba, definimos entonces la hipótesis nula como:

$$H_0: \mu_1 = \mu_2$$

Es decir, ambas muestras pertenecen a la misma población, o, en otras palabras, no existe diferencia significativa entre ambas muestras. Por consiguiente, la hipótesis alternativa la definimos como:

$H_a: \mu_1 \neq \mu_2$

Es decir, existe una diferencia significativa entre ambos grupos de datos; por ende, pertenecen a diferentes poblaciones.



Mediciones de Replay y Wrong Data

Una vez definidas las hipótesis, se realiza una prueba t-Student haciendo uso de la herramienta R, con el comando "t.test"; esta ejecución nos da como resultado un p-value = 0.002912, siendo este valor menor a 0.05, por lo que no se puede aceptar la hipótesis nula, es decir, no se puede asegurar que ambas muestras pertenezcan a la misma población y por ende son diferentes.

```
        Two Sample t-test

data:  replay$V1 and wrong$V1
t = 2.9843, df = 998, p-value = 0.002912
alternative hypothesis: true difference in means is not equal to 0
95 percent confidence interval:
 0.5287301 2.5592699
sample estimates:
mean of x mean of y
  575.428   573.884
```

Prueba t-Student en R

Sin embargo, la prueba t-Student requiere que las muestras sigan una distribución gaussiana; en este caso no podemos asegurar que las muestras sigan esta distribución, por lo que se ejecuta un test de normalidad, específicamente la prueba Shapiro-Wilks, para determinar si los datos siguen una distribución normal.

H_0: Los datos siguen una distribución normal

Esta prueba fue ejecutada usando el comando "shapiro.test" en R y se obtuvo un p-value=2.2e-16; es decir, se rechaza la hipótesis nula y por ende los datos no están distribuidos normalmente.

```
        Shapiro-Wilk normality test

data:  replay$V1
W = 0.8245, p-value < 2.2e-16
```

Prueba de normalidad

Se procede entonces a ejecutar una prueba no paramétrica; en este caso se usa la prueba de Mann-Whitney para probar la igualdad en distribución de dos muestras independientes que no (necesariamente) siguen una distribución normal. Se plantea la hipótesis nula como:

H_0: Ambas muestras siguen la misma distribución.

Esta prueba se ejecutó con el comando "wilcox.test" en R, obteniendo un p-value=0.003583; por ende, no se puede aceptar la hipótesis nula, concluyendo entonces que ambas muestras son, efectivamente, diferentes.

```
        Wilcoxon rank sum test with continuity correction

data:  replay$V1 and wrong$V1
W = 137266, p-value = 0.003583
alternative hypothesis: true location shift is greater than 0
```

Prueba Mann-Whitney

VII. Conclusiones

Los pasaportes electrónicos representan una alternativa a los pasaportes tradicionales en papel; sin embargo esta solución presenta grandes retos a la hora de resguardar tanto la información almacenada en el, como la integridad del viajero que lo porta.

Estos retos han sido solventados correctamente con un protocolo de autenticación llamado BAC; con el cual se obliga a que la parte que desea leer la información dentro del pasaporte deba tener acceso físico al mismo.

Al margen de este protocolo, se han propuesto ataques en los cuales no se compromete la información dentro del pasaporte, pero si la privacidad del portador, ya que pudiera realizarse trazabilidad sobre el pasaporte y determinar, por ejemplo, el momento preciso en el que el portador se aproxime a una ubicación específica.

El primer ataque se plantea haciendo uso de los mensajes de respuesta recibidos ante diferentes mensajes de entrada enviados desde el lector. Sin embargo esta prueba se mostró como inefectiva con los pasaportes venezolano ya que no presentaron diferencias en los mensajes de respuesta.

Se plantea entonces un segundo ataque basado en la diferencia de los tiempos de respuesta ante un mensaje incorrecto (MAC incorrecta) y un mensaje correcto capturado previamente (MAC correcta).

Se desarrolló una aplicación en Android para hacer la experimentación sobre un pasaporte venezolano y determinar la presencia o ausencia de tal vulnerabilidad. Se hicieron 500 mediciones de tiempos de respuesta ante un mensaje incorrecto y 500 mediciones ante un mensaje correcto y se condujeron diferentes pruebas de contraste de medias para determinar si existe diferencia significativa entre ambos grupos de datos.

Al finalizar las pruebas se concluye que no es posible asegurar que ambas grupos de datos sean iguales por lo que se asume que el pasaporte venezolano cuenta con la vulnerabilidad explotada por este ataque.

Sin embargo, es importante acotar que el entorno sobre el cual se realizaron estas pruebas no es el ideal para la medición

de tiempos de respuesta, debido a la no disponibilidad de un dispositivo diseñado específicamente para esta tarea; por lo que pudiera extenderse este trabajo, haciendo uso de equipos más sofisticados para la medición de los tiempos.

Referencias

[1] T. Chothia and V. Smirnov, “A Traceability Attack Against e-Passports,” *14th Int. Conf. Financ. Cryptogr. Data Secur. FC10*, pp. 1–15, 2010.