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.