Universidad
Carlos III de Madrid

ATAQUE DE TRAZABILIDAD CONTRA PASAPORTES ELECTRÓNICOS

Técnicas y Protocolos Criptográficos
Trabajo Práctico

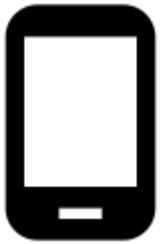
Antonio Quirós
Departamento de Informática
Escuela Politécnica Superior

e-Passport

BAC Authentication

Vulnerabilidad y Ataque

Implementación



Demo

Pruebas y Resultados

e-Passports

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.

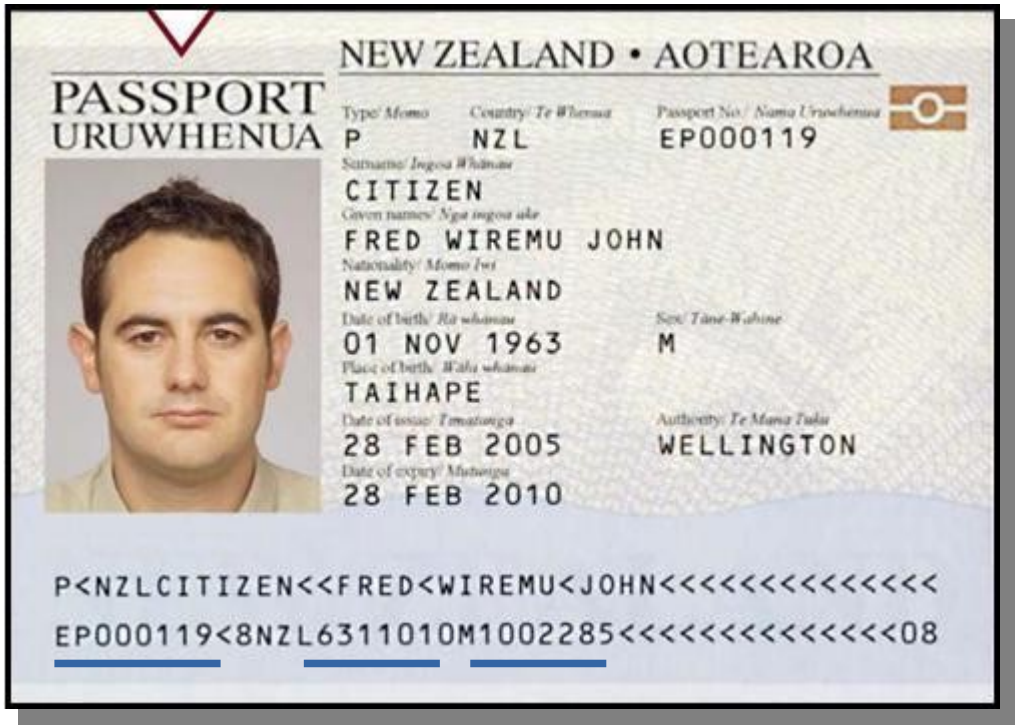
Utiliza tecnología *contact-less smart card* con un chip RFID que permite almacenar la información que se encuentra impresa así como también un conjunto de datos adicionales.

Los pasaportes electrónicos están desarrollados bajo las especificaciones de la Internation Civil Aviation Organization (ICAO) para los MRTD (Machine Readable Travel Document).

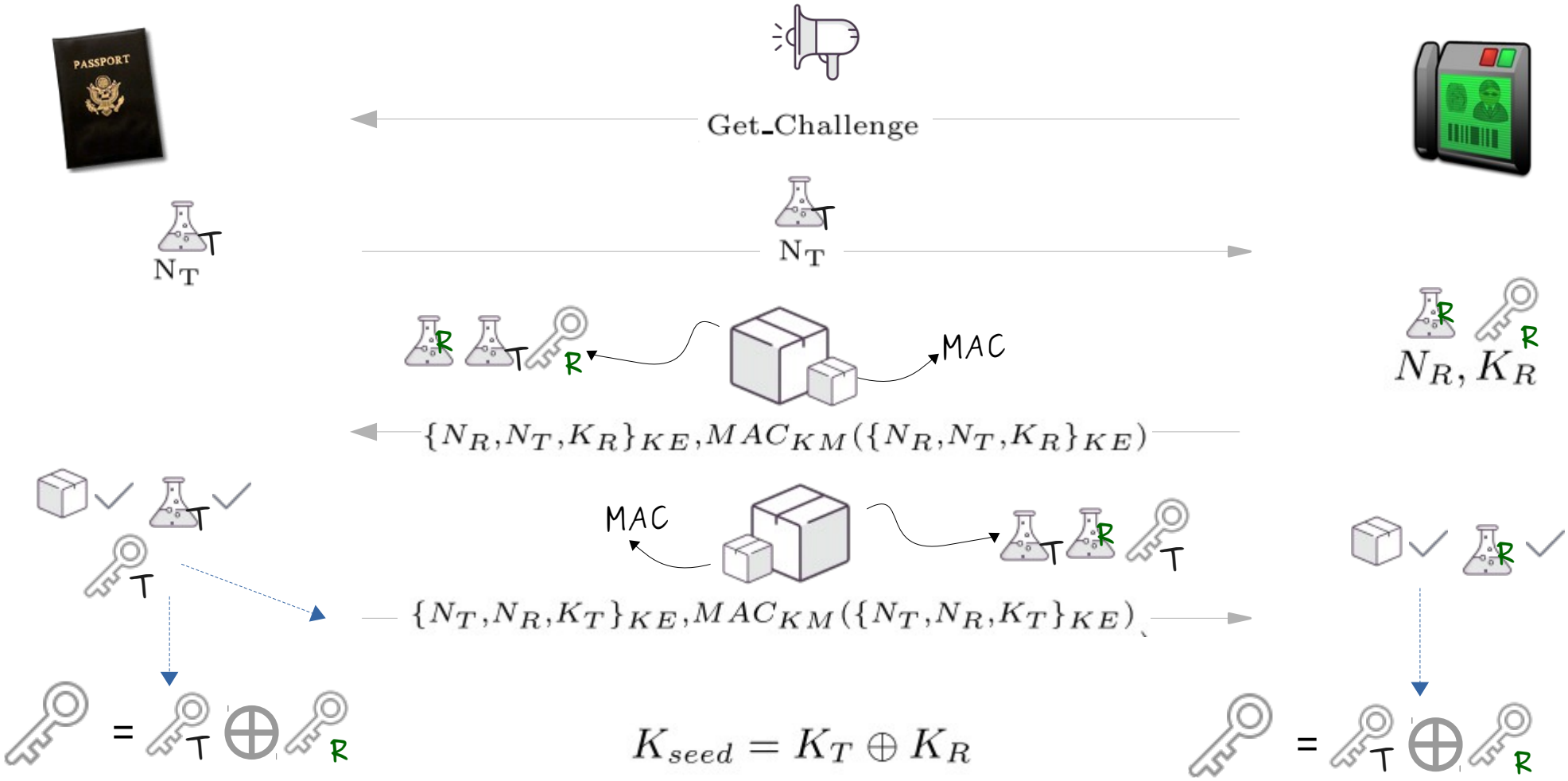
BAC Authentication

Basic Acess 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.

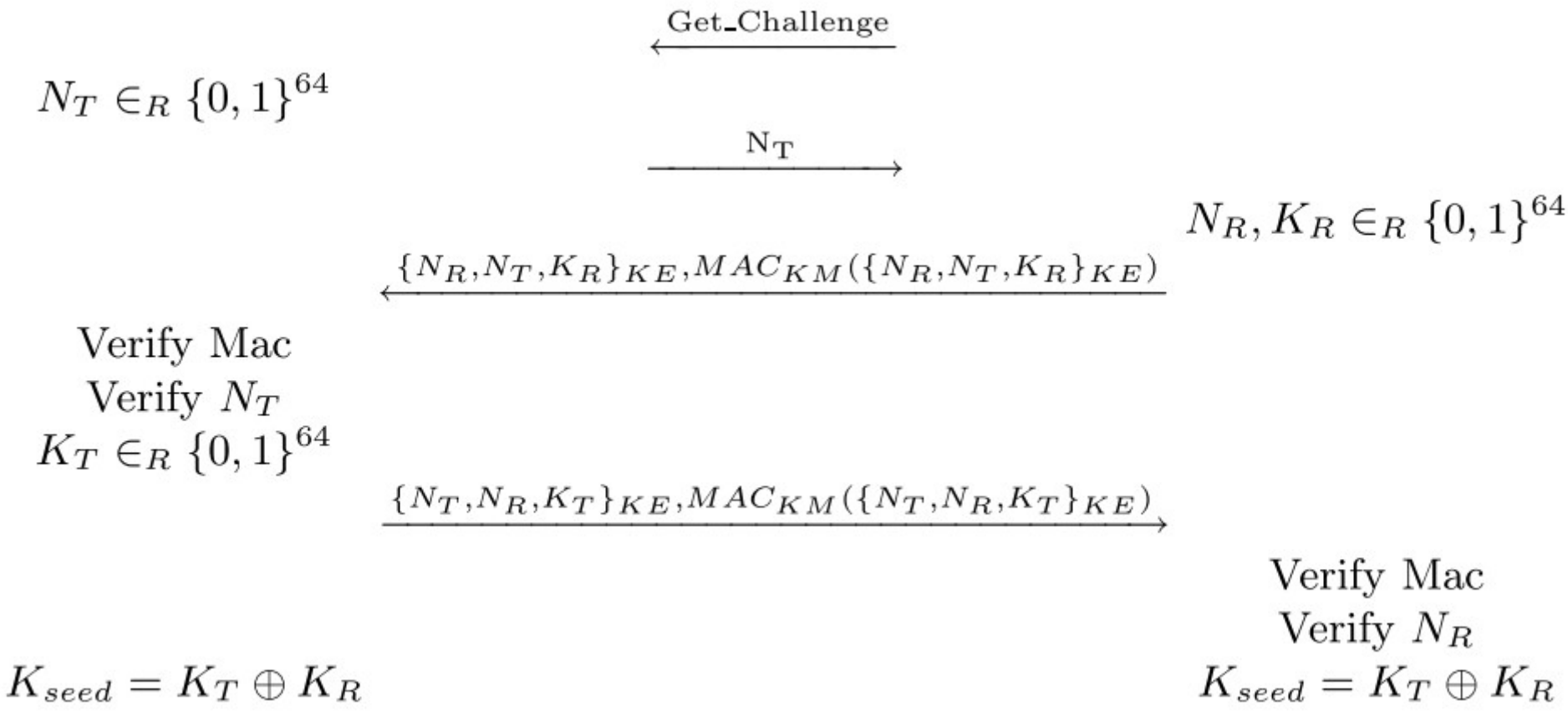
Este protocolo utiliza información como el número del pasaporte, fecha de nacimiento y fecha de vencimiento para negociar una clave de sesión. Esta clave se usa para encruptar la comunicación entre el pasaporte y el lector.



BAC Authentication



BAC Authentication



Universidad Carlos III de Madrid

Fingerprinting e-Passports

Henning Richter, Wojciech Mostowski, Erik Poll

```
No Error (9000)                    Wrong Length (6700)
Unknown (6F00)                     Counter reached zero (63C0)
CLA Not Supported (6E00)           Instruction Not Supported (6D00)
Incorrect P1P2 (6A86)              Conditions Not Satisfied (6985)
Command Not Allowed (6986)         Security Status Not Satisfied (6982)
```

	Commands						
	44	**82**	**84**	**88**	**A4**	**B0**	**B1**
	Rehab. CHV	Ext. Auth.	Get Chall.	Int. Auth.	Select File	Read Binary	Read Binary
Australian	6982	6985	6700	6700	9000	6700	6700
Belgian	—	6E00	—	6700	6A86	6986	6700
Dutch	—	6700	6700	6982	6A86	6982	6982
French	6982	6F00	6F00	6F00	6F00	6F00	6F00
German	—	6700	6700	—	6700	6700	—
Greek	6982	63C0	6700	6982	9000	6986	6700
Italian	—	6700	—	—	—	—	—
Polish	6982	6700	6700	6700	9000	6700	—
Swedish	6982	6700	6700	—	9000	6700	—
Spanish	—	6700	6700	—	6700	6700	—

Ataque de trazabilidad

Tom Chothia, Vitaliy Smirnov

Un ataque de trazabilidad no implica un riesgo para toda la información almacenada en el, pero sin embargo, si representa una verdadera amenaza para la privacidad de cualquiera que porte tal dispositivo.

Universidad
Carlos III de Madrid

Ataque de trazabilidad

Tom Chothia, Vitaliy Smirnov

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.

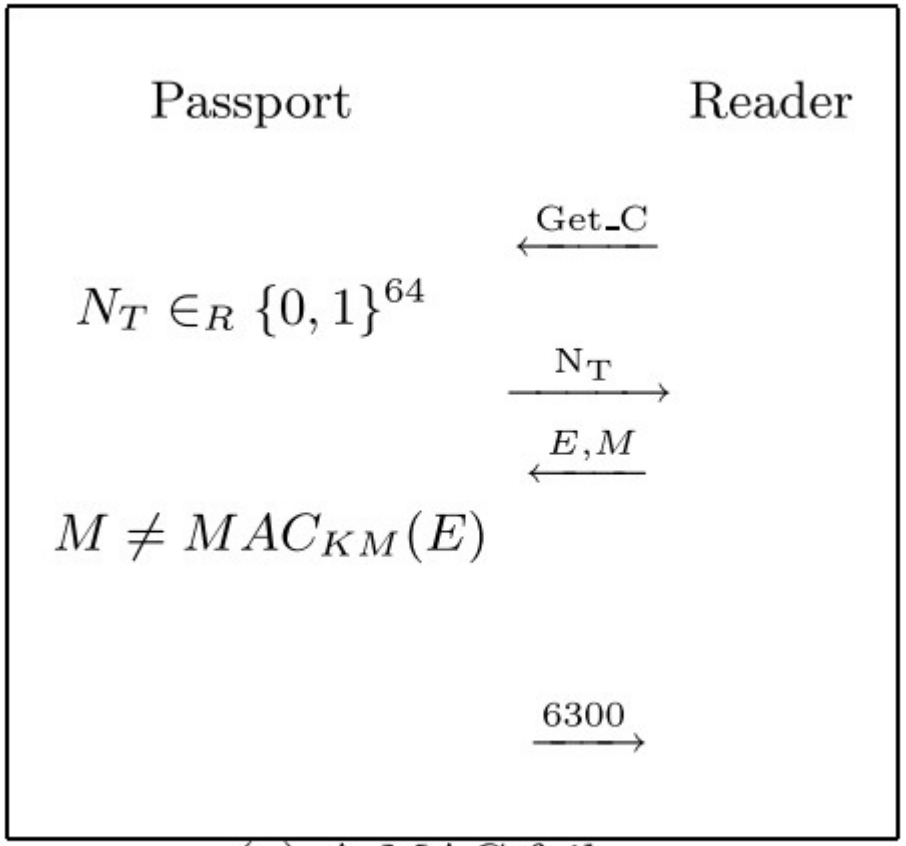
En un caso específico, los pasaportes franceses presentan una vulnerabilidad en el protocolo BAC debido a los mensajes de error que retorna dependiendo de la consulta realizada.

Si se consulta al pasaporte con una MAC errónea, este responde con código 6300 “No information given”.

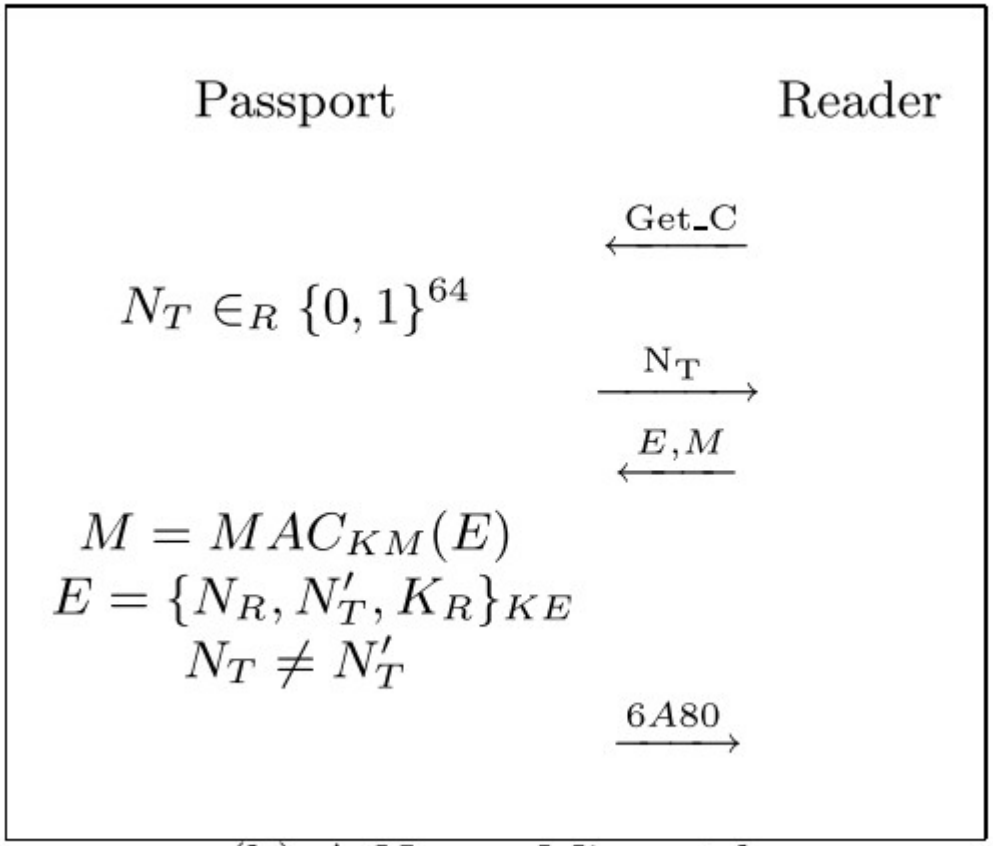
Si por el contrario, se consulta con una MAC correcta pero con con el número aleatorio incorrecto la respuesta será 6A80 “Incorrect parameters”.

Ataque de trazabilidad

Tom Chothia, Vitaliy Smirnov



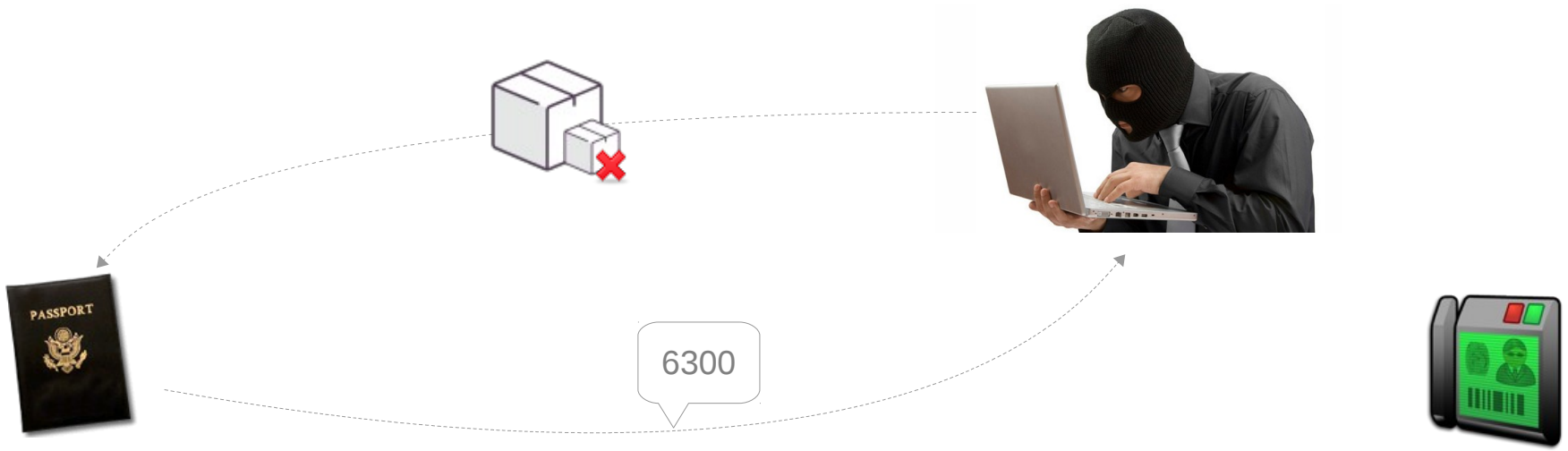
(a) A MAC failure



(b) A Nonce Mismatch

Ataque de trazabilidad

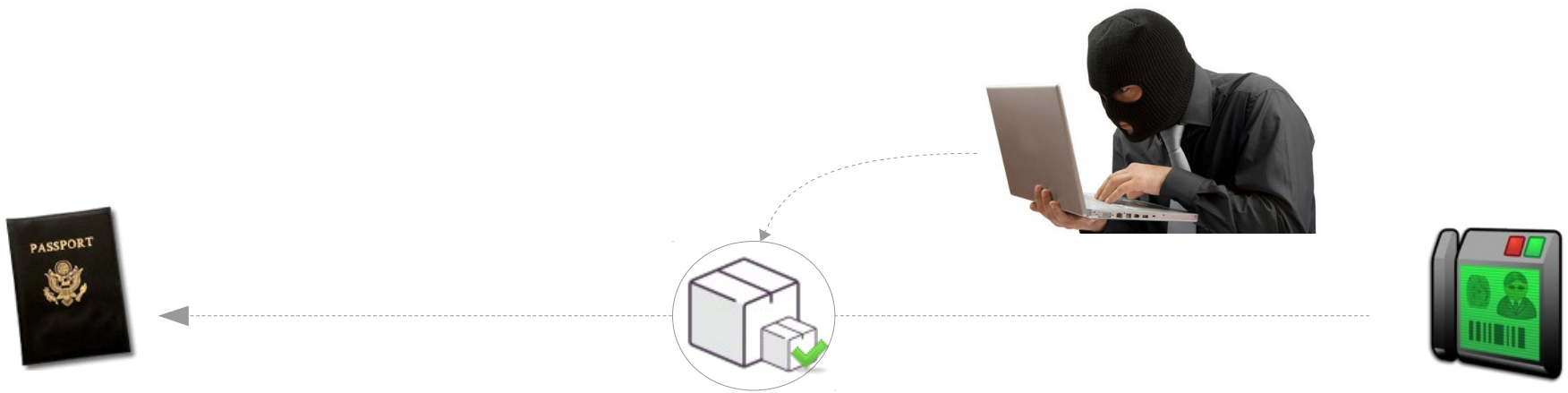
Tom Chothia, Vitaliy Smirnov



Paso 1: Se intenta una autenticación con datos incorrectos, lo cual genera una MAC errónea debido a que los valores usados para encriptar el paquete (Número de documento, Fecha de Nacimiento y Fecha de vencimiento) difieren a los usados por el pasaporte.

Ataque de trazabilidad

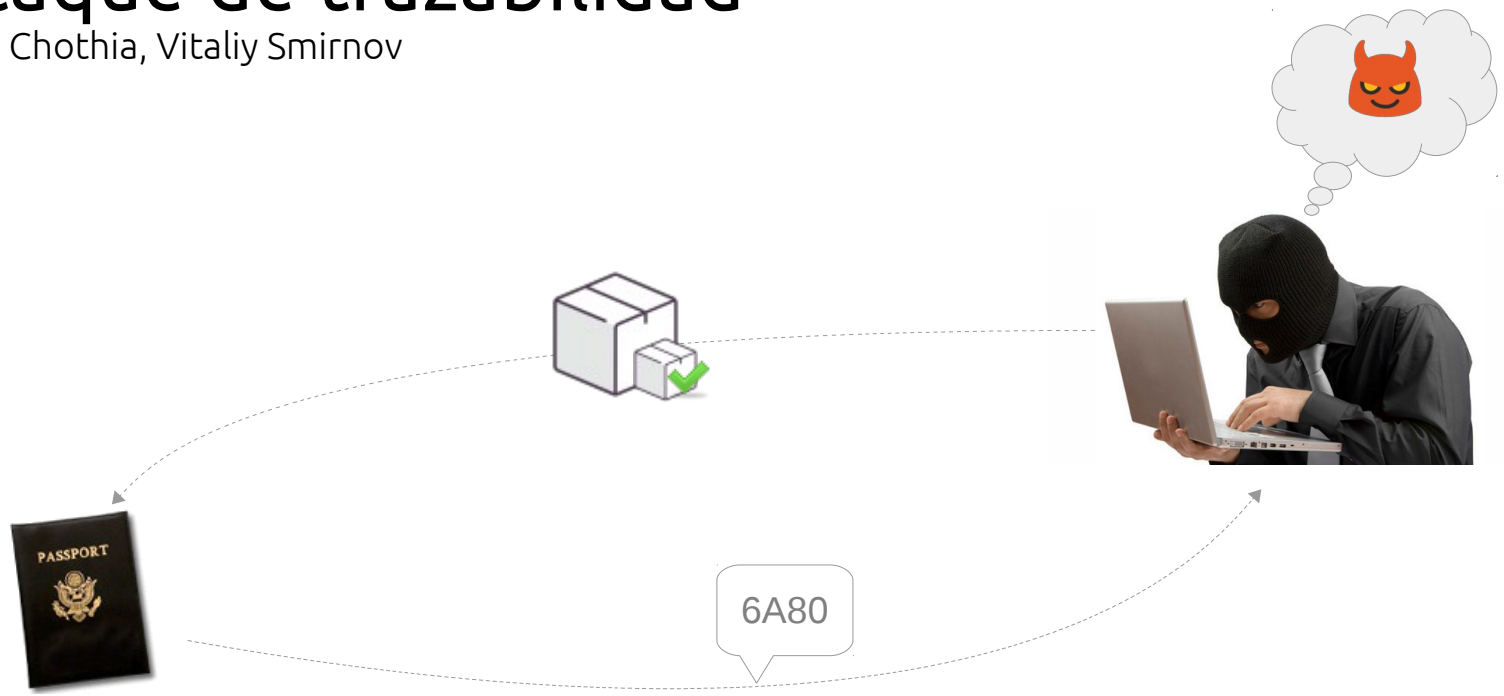
Tom Chothia, Vitaliy Smirnov



Paso 2: El atacante logra capturar un mensaje correcto enviado entre el lector y el pasaporte y lo almacena. Este mensaje será utilizado luego para identificar el pasaporte.

Ataque de trazabilidad

Tom Chothia, Vitaliy Smirnov



Paso 3: El atacante reproduce el mensaje almacenado. Si el pasaporte responde con código 6300 sabemos que los datos usados para encriptarlo no son los mismos del documento, por ende es otro pasaporte; pero si el mensaje devuelto es '6A80' significa que la MAC es correcta, por ende el pasaporte ha sido ubicado.

Ataque de trazabilidad

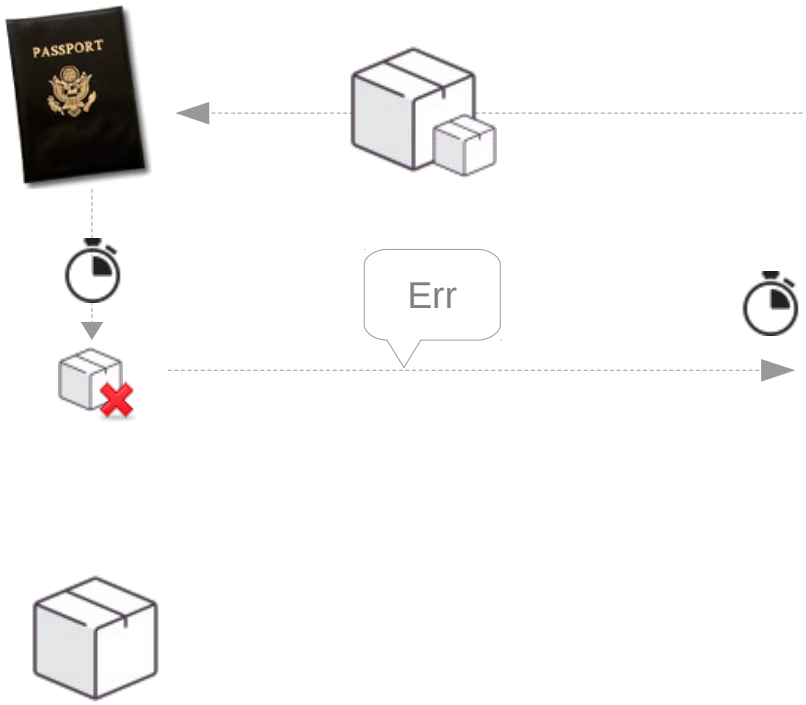
Tom Chothia, Vitaliy Smirnov

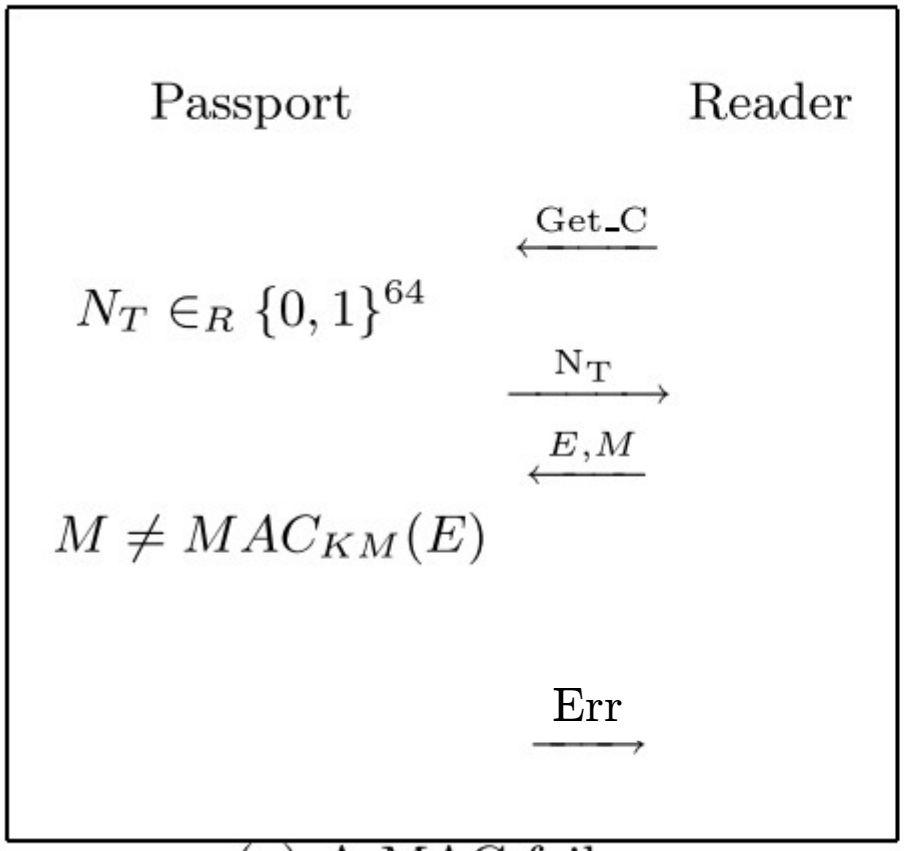
Existen pasaportes que no cuentan con esta vulnerabilidad ya que el mensaje devuelto para ambos casos (MAC errónea o MAC correcta y Nonce incorrecto) es el mismo.

Sin embargo otra vulnerabilidad ha sido analizada: Los tiempos de respuesta.

Ataque de trazabilidad

Tom Chothia, Vitaliy Smirnov

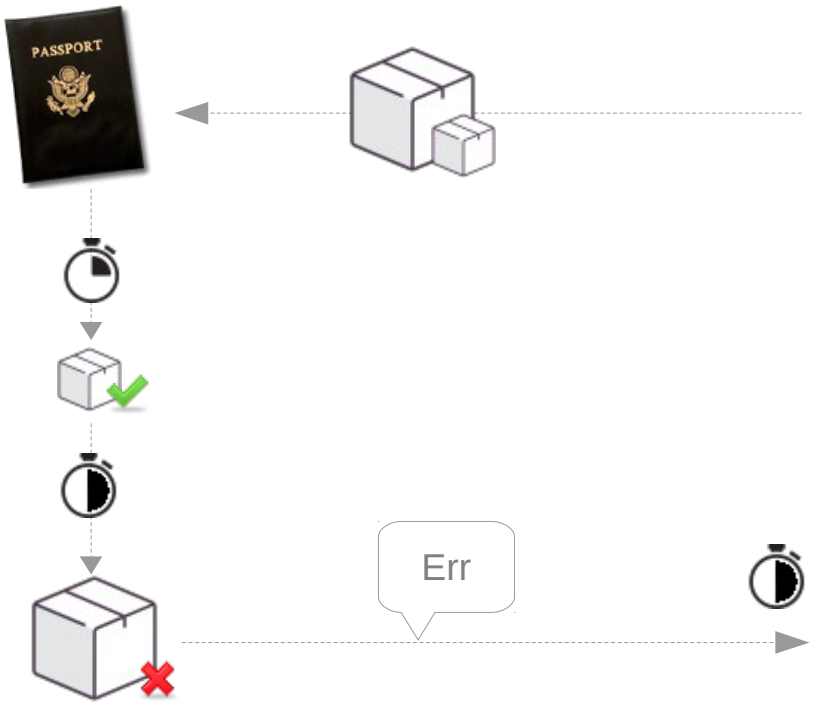


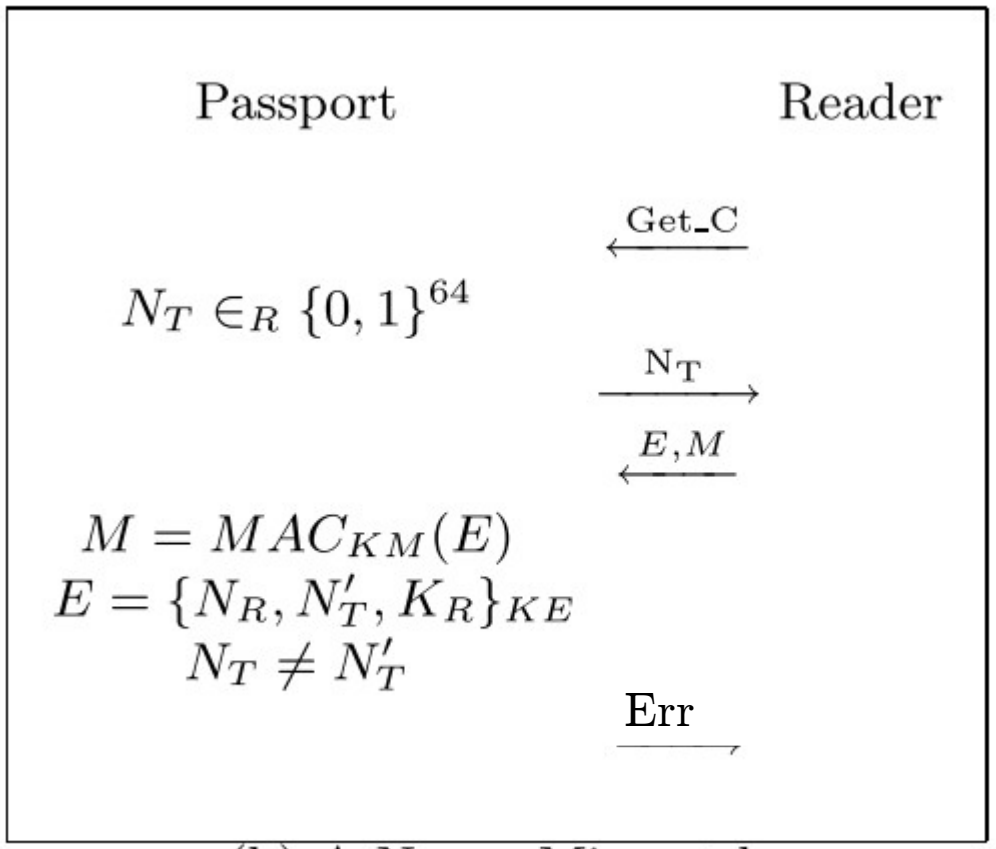


(a) A MAC failure

Ataque de trazabilidad

Tom Chothia, Vitaliy Smirnov





(b) A Nonce Mismatch

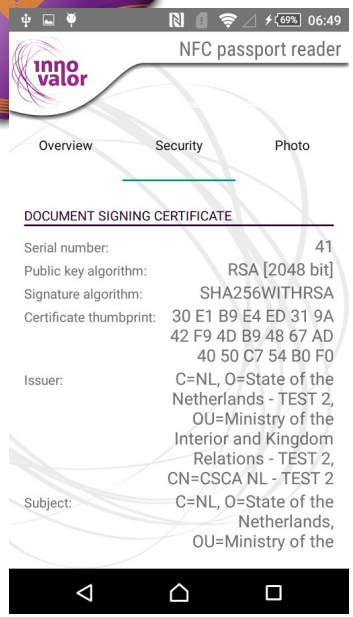
Implementación del ataque

Implementación del ataque

Buscar implementaciones ya realizadas.

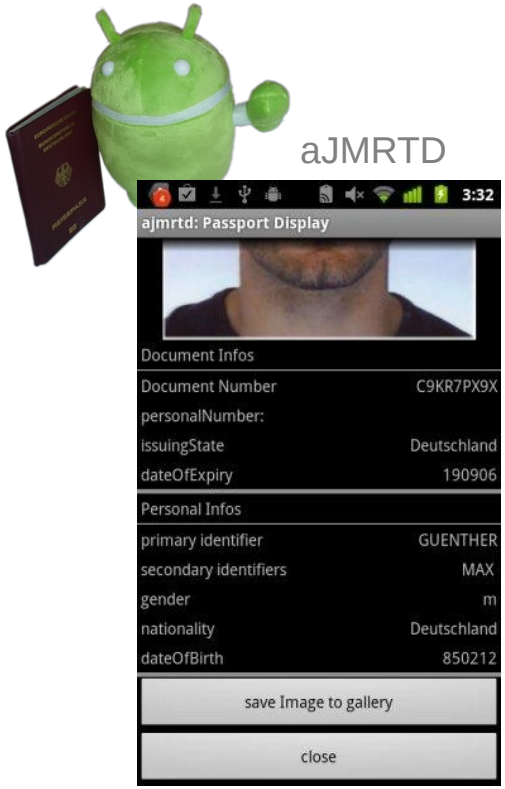
Implementación del ataque

NFC Passport Reader



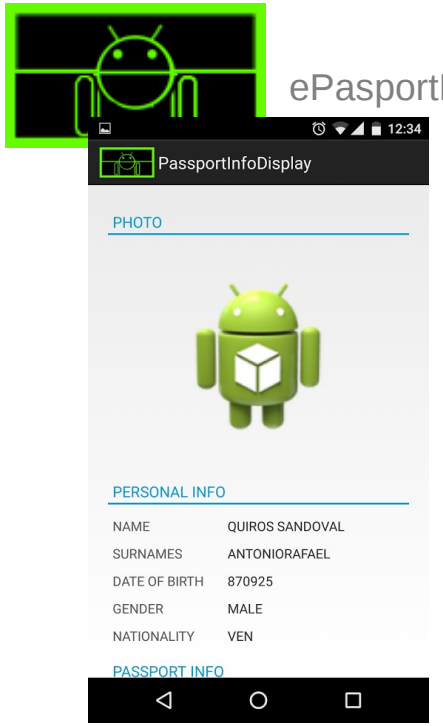
Compleja

aJMRTD



Buggy

ePasportReader



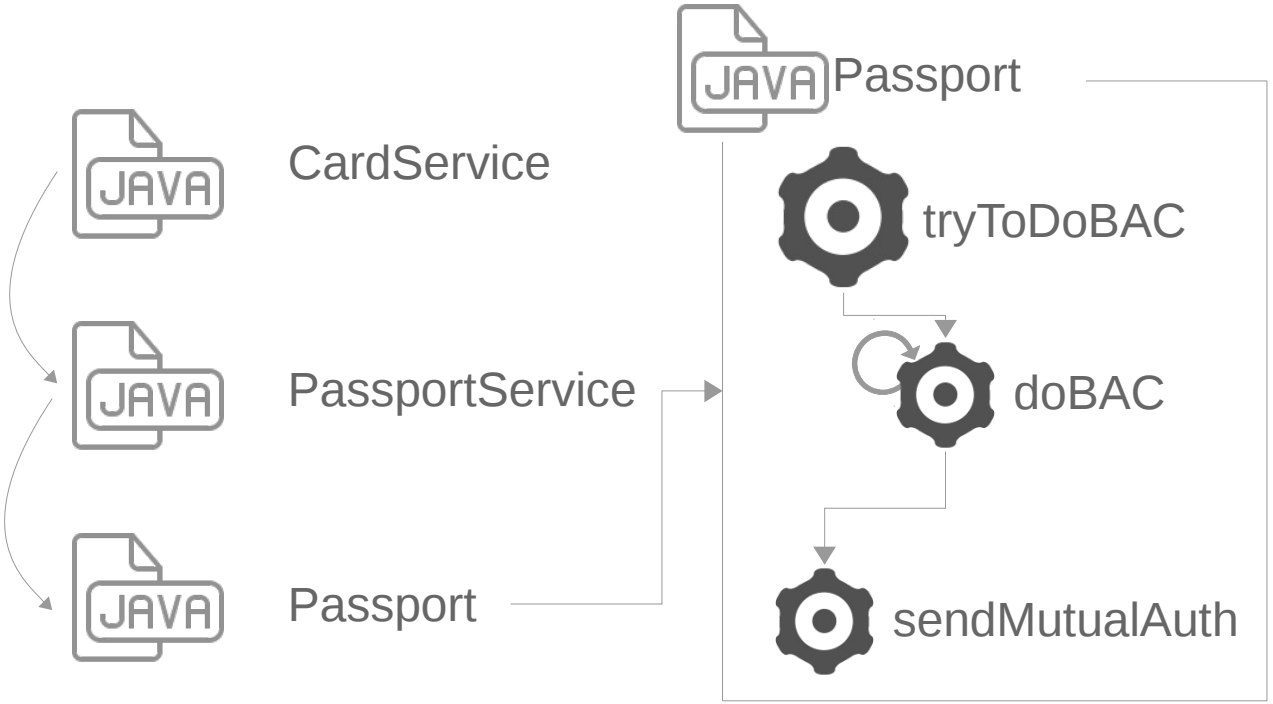
Ok

Implementación del ataque

ePassportReader

Registra

Espera

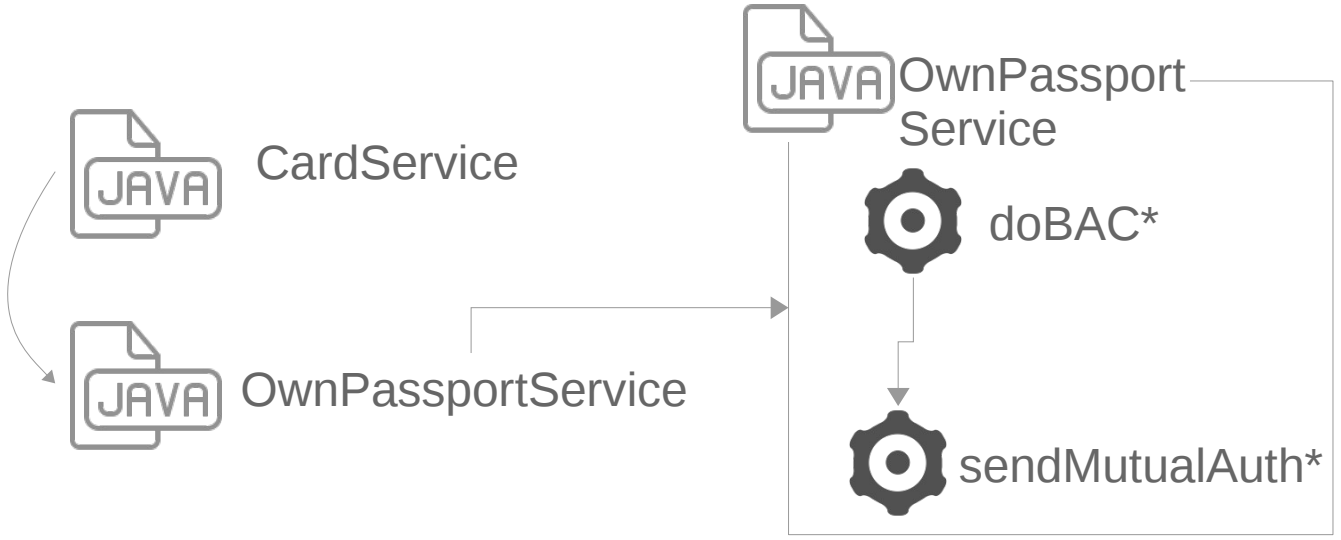


Implementación del ataque

Android Passport Reader

Registra

Espera



Implementación del ataque

SendMutualAuth:

Una vez realizada la autenticación correcta, captura y almacena el paquete.

Si se indica, inicia la autenticación con el paquete almacenado y registra el mensaje de error.

Se toman los tiempos de respuesta del pasaporte, midiendo el tiempo actual antes y después de la comunicación.

Implementación del ataque

Funciones desarrolladas:

- Challenge Test
- BAC Authentication Test
- Replay Attack
- Wrong Data Test
- Replay Timing
- Wrong Data Timing

Implementación del ataque

Experimentación y resusltados:

Replay Attack:

- Se experimentó con un pasaporte venezolano.
- Se realizó la autenticación correcta y se almacenó el paquete.
- Se realizó el reenvío de ese paquete y se recibió el mensaje de respuesta **6300**.
- Se realizó la autenticación enviando datos erróneos y se recibió el mensaje de respuesta **6300**.
- Conclusión: **No es vulnerable**.

Implementación del ataque

Experimentación y resusltados:

Timing Attack:

Se realizaron 3 pruebas:
Cada prueba se realizaban
- 100 intentos de autenticación con replay.
- 100 intentos de autenticación con data errónea.

Se registran los tiempos de cada una y se calcula el tiempo medio de respuesta.

Implementación del ataque

Experimentación y resusltados:

Timing Attack:

	Replay	Wrong Data
Prueba 1	570,76	576,84
Prueba 2	570,01	571,92
Prueba 3	571,59	573,17
Medio:	**570,79**	**573,98**

Implementación del ataque

Experimentación y resusltados:

Timing Attack:

Tiempos Medios

	Replay	Wrong Data
Prueba 1	570,76	576,84
Prueba 2	570,01	571,92
Prueba 3	571,59	573,17
Medio:	**570,79**	**573,98**

Intervalos de Confianza

	Intervalo de Confianza	
Replay	568,30	573,22
Wrong Data	566,53	587,15

	Intervalo de Confianza	
Replay	568,18	571,84
Wrong Data	569,87	573,97

	Intervalo de Confianza	
Replay	569,49	573,69
Wrong Data	571,46	574,88

Implementación del ataque

Experimentación y resusltados:

Challenge Test:

Se ejecutaron 3 pruebas con 500, 500 y 1000 números aleatorios y se usó ENT Randomness Test para probar la calidad de estos números

	Prueba 1	Prueba 2	Prueba 3	Ideal
Muestras	500	500	1000	--
Entropía	7,952	7,952	7,975	8
Media Aritmét.	126,14	128,93	127,21	127,5
Correlación	0,001	-0,01	-0,004	0

Implementación del ataque

Preguntas