Universidad Zaragoza
1542

Escuela de Ingeniería y Arquitectura Universidad Zaragoza

Trabajo de Fin de Grado

Análisis de la resistencia del DNIe3.0 ante el robo de identidad mediante tecnología NFC

Security analysis of DNIe3.0 against NFC-based identity theft

---

Autor: Víctor Sánchez Ballabriga (602665)
Director: Ricardo J. Rodríguez

ÍNDICE

1. Introducción

- Evolución del DNI
- Creci e NFC
- DNI + NFC = DN 3.0

1. Introducción

- Trabajo relacionado
- ¿Qué [illegible]?

El [illegible] de
rob[illegible]

21 ene[illegible]

afectada[illegible]

- *Más de 4,5 millones de personas se han visto afectadas por el robo de datos personales. España es el país de la Unión Europea que ha sufrido más robos de identidad*

2. Conocimientos Previos

Near Field Comunication (NFC)

- Deriva de RFID
- Elementos activos (PDC) y pasivos (PICC)
- ISO/IEC 14443

2. Conocimientos Previos

Ataques de fuerza bruta

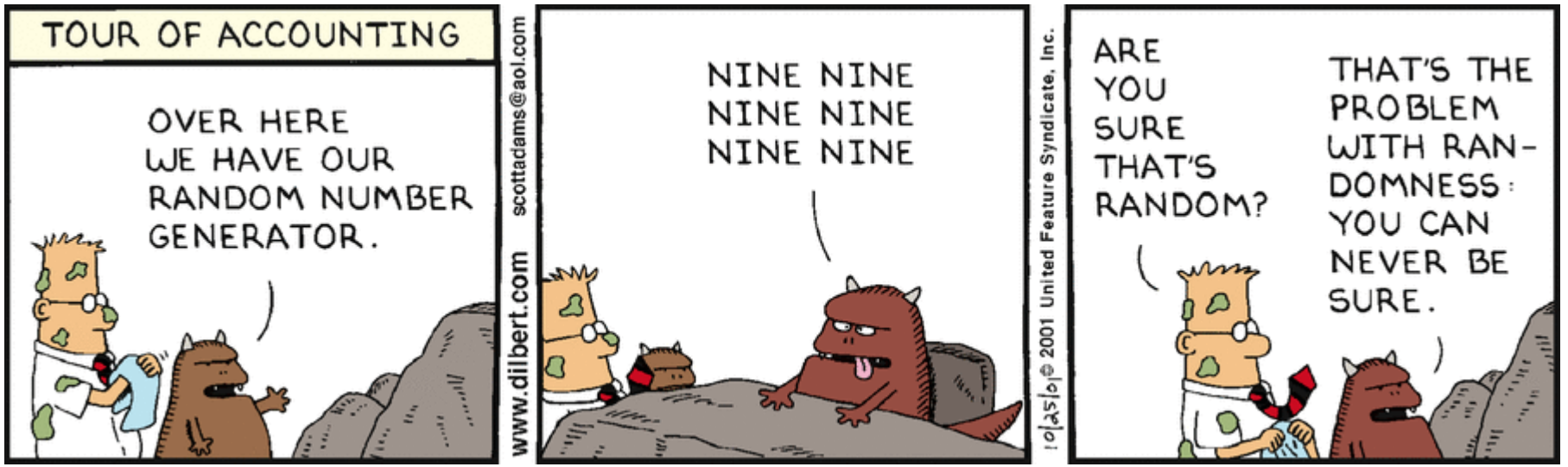
- Suelen combinarse con ataques de diccionario
- Inconvenientes:

1) Fáciles de detectar
2) Fáciles de contrarrestar

2. Conocimientos Previos

Trazabilidad de números aleatorios

- Los ordenadores son máquinas deterministas
- RNG trazable = mal RNG



3. Análisis del DNIe3.0

Información impresa:

1) Foto facial
2) NIF
3) Apellidos
4) Nombre
5) Sexo (“M”/”F”)
6) Nacionalidad (“ESP”)
7) Fecha de nacimiento
8) Número de soporte
9) Fecha de expiración
10) Firma manuscrita
11) Código CAN

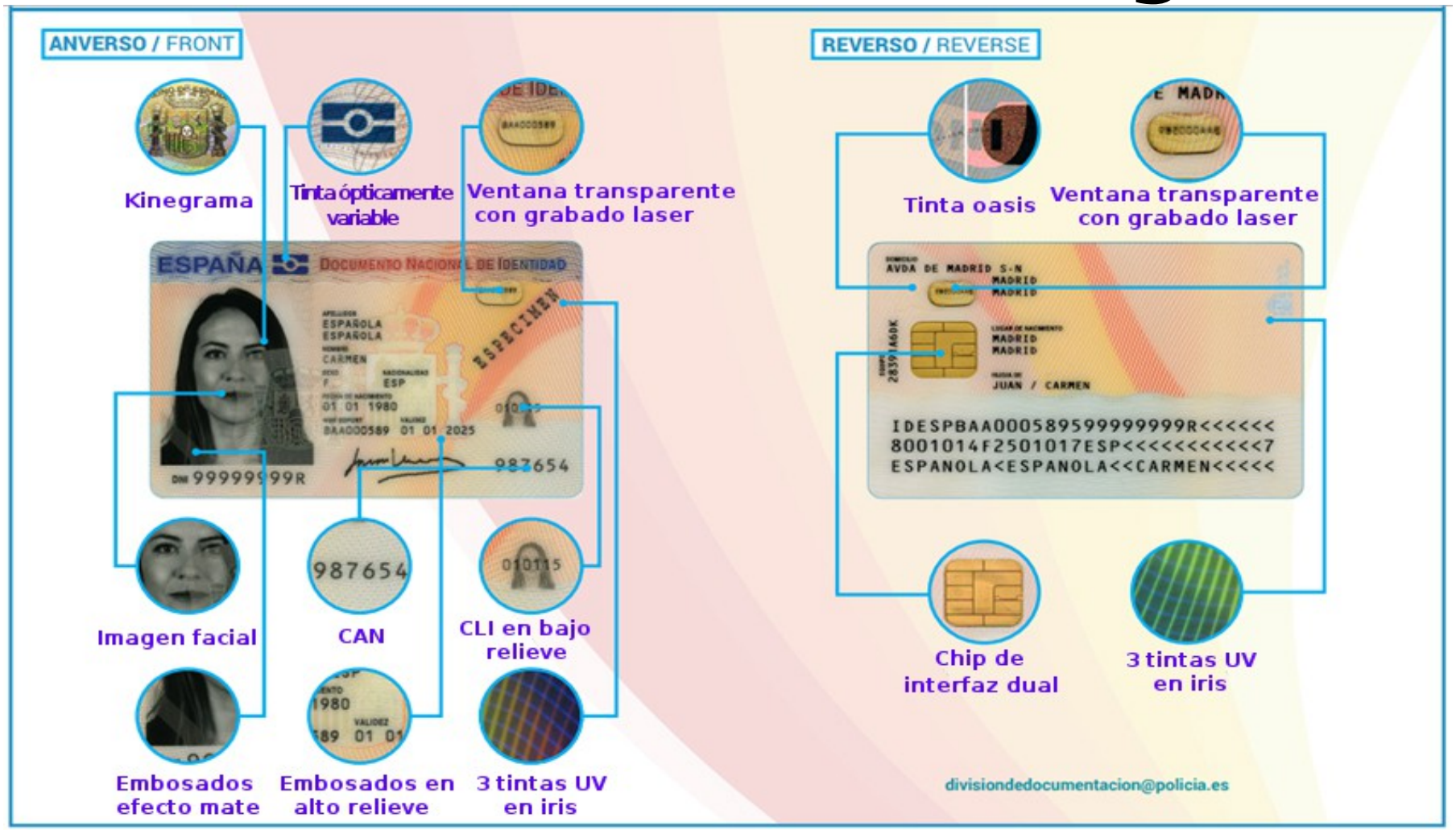
3. Análisis del DNIe3.0

Información impresa:

1) Dirección
2) Número de equipo de expedición
3) Ciudad y provincia de nacimiento
4) Nombre de los progenitores
5) MRZ

3. Análisis del DNIe3.0

Elementos físicos de seguridad:



4. Métodos de acceso NFC

- Basic Access Control (BAC)
- Password Authenticated Connection Establishment (PACE)

4. Métodos de acceso NFC

Protocolo BAC:

- Fecha de nacimiento
  (en formato “aaaammdd”)

$$2002 - 1946 = 57\ años$$
$$57 \cdot 365 = 20805$$

- Fecha de expiración
  (en formato “aaaammdd”)

$$365 \cdot 10 = 3650$$

- Número de soporte
  (3 letras y 6 dígitos)

$$26^3 \cdot 10^6 \simeq 2^{34}$$

$$20805 + 3650 + 2^{34} \simeq 2^{34}$$

4. Métodos de acceso NFC

Protocolo PACE:

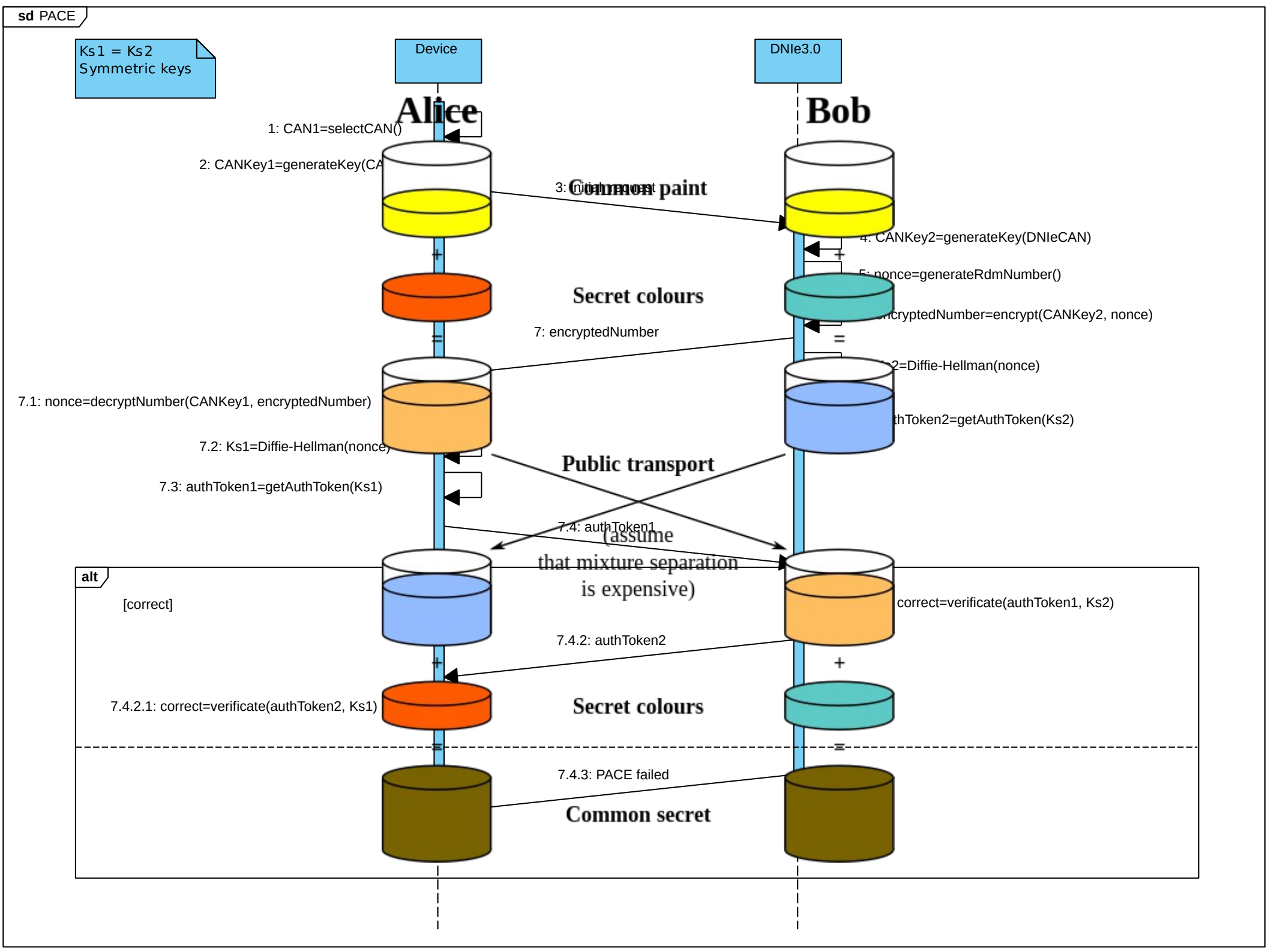
- Código CAN 10^6

Elección del protocolo de estudio

BAC PACE

2^3 >> 10^6

4


sd PACE
Ks1 = Ks2
Symmetric keys
Device
DNIe3.0
Alice
Bob
1: CAN1=selectCAN()
2: CANKey1=generateKey(CA
3: initialRequest
Common paint
4: CANKey2=generateKey(DNIeCAN)
5: nonce=generateRdmNumber()
Secret colours
ncryptedNumber=encrypt(CANKey2, nonce)
7: encryptedNumber
2=Diffie-Hellman(nonce)
7.1: nonce=decryptNumber(CANKey1, encryptedNumber)
thToken2=getAuthToken(Ks2)
7.2: Ks1=Diffie-Hellman(nonce)
Public transport
7.3: authToken1=getAuthToken(Ks1)
7.4: authToken1
(assume
that mixture separation
is expensive)
alt
[correct]
correct=verificate(authToken1, Ks2)
7.4.2: authToken2
7.4.2.1: correct=verificate(authToken2, Ks1)
Secret colours
7.4.3: PACE failed
Common secret

5. Vulnerabilidades estudiadas

- Ataque de sniffing 
- Trazabilidad de los números aleatorios 
- Ataque de fuerza bruta 

5. Vulnerabilidades estudiadas: Ataque de Sniffing

5. Vulnerabilidades estudiadas

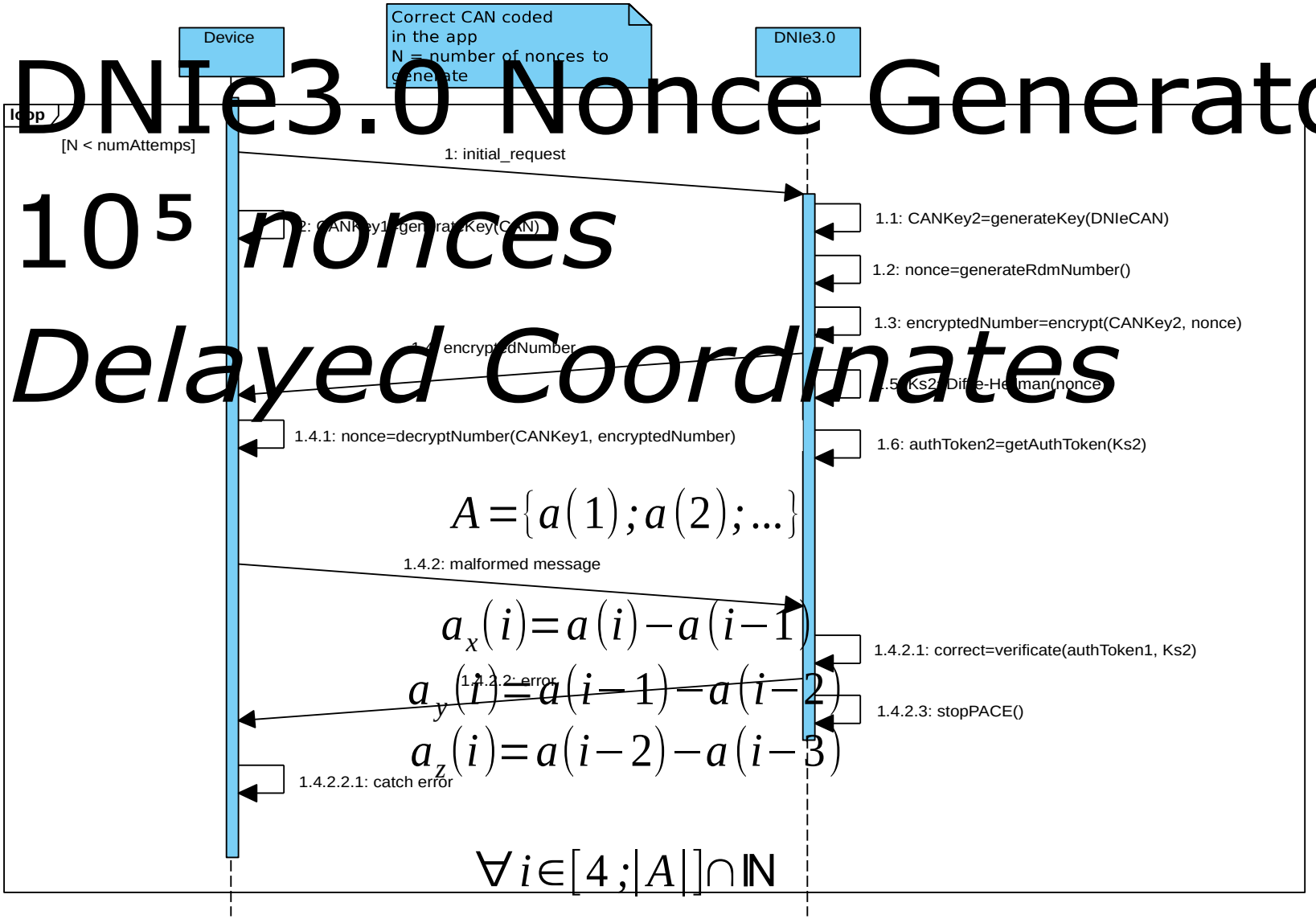
- Ataque de sniffing

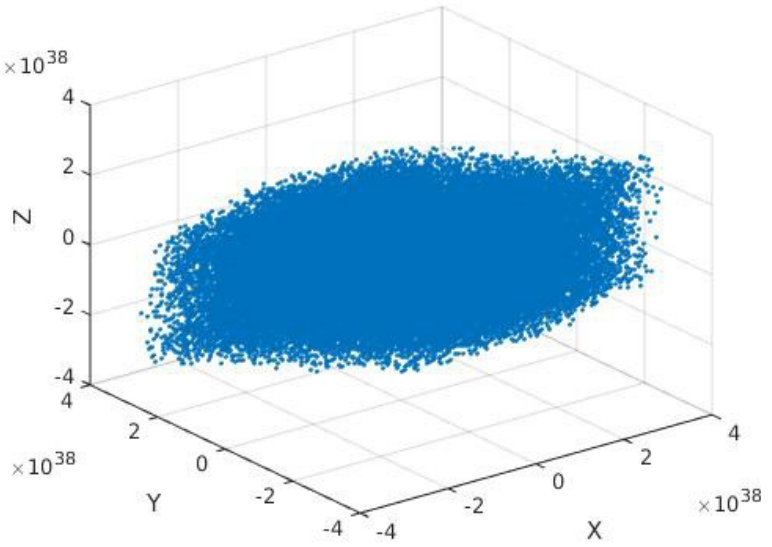
- Trazabilidad de los números aleatorios

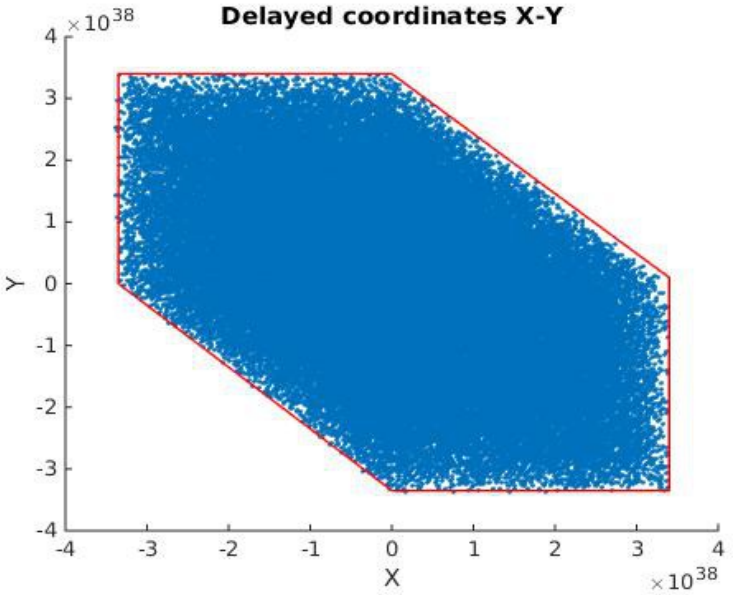
- Ataque de fuerza bruta

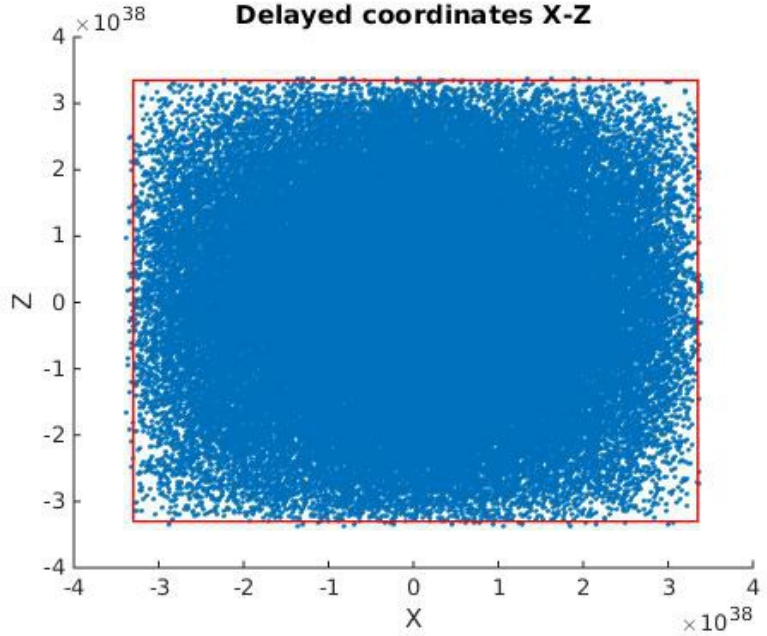
5. Vulnerabilidades estudiadas:Trazabilidad de los números aleatorios

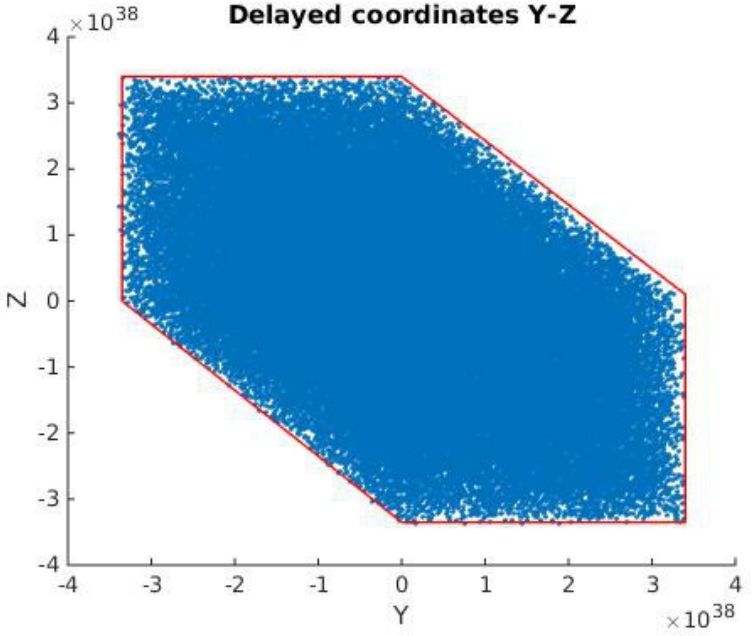
- DNIe3.0 Nonce Generator
- 10^5 *nonces*
- *Delayed Coordinates*




×10^38
4
2
0
-2
-4
Z
4
2
0
-2
-4
×10^38
Y
-4
-2
0
2
4
×10^38
X


Delayed coordinates X-Y
×10^38
4
3
2
1
0
-1
-2
-3
-4
Y
-4 -3 -2 -1 0 1 2 3 4
X
×10^38


Delayed coordinates X-Z
×10^38
4
3
2
1
0
-1
-2
-3
-4
Z
-4 -3 -2 -1 0 1 2 3 4
X
×10^38

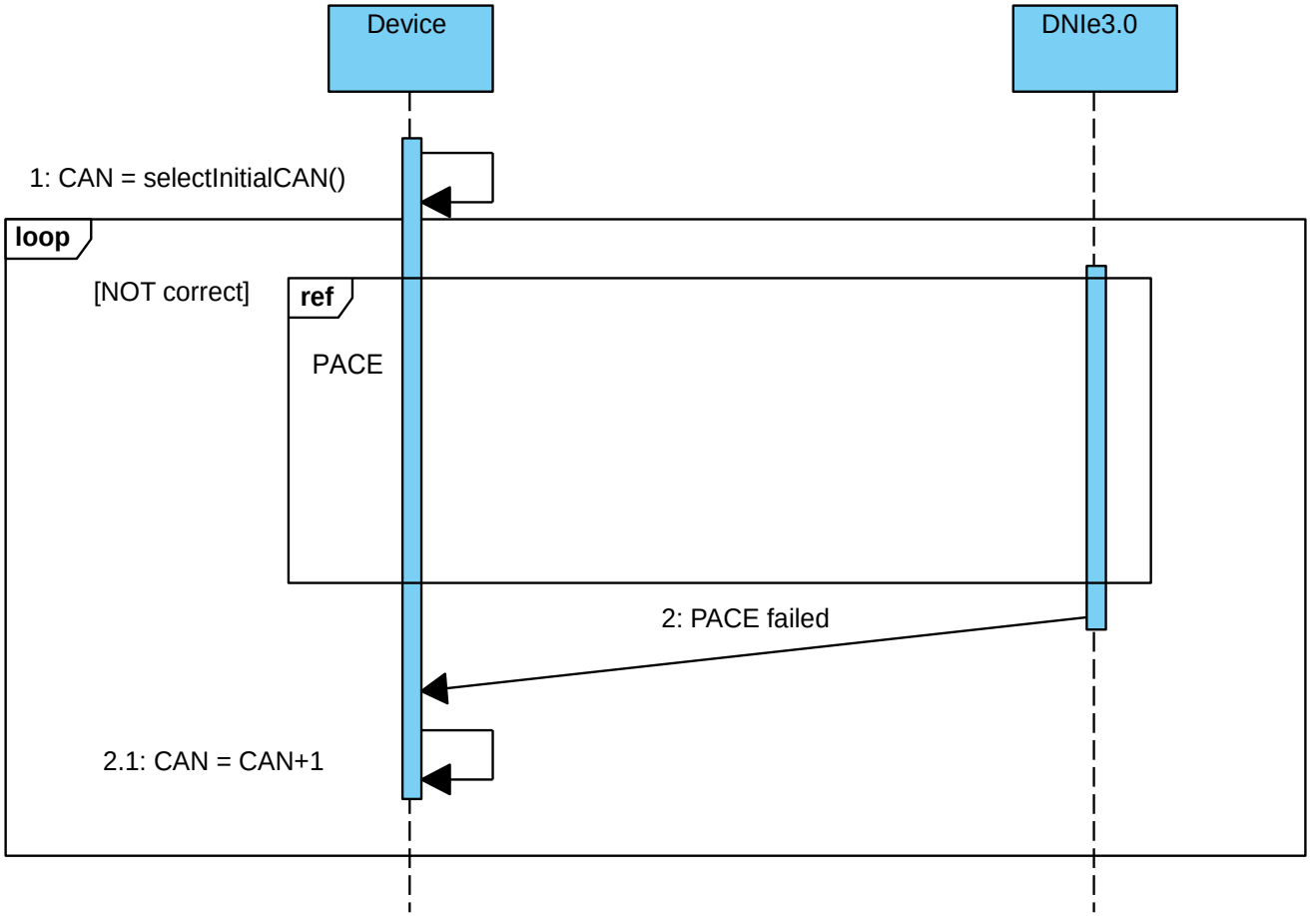

Delayed coordinates Y-Z
×10^38
4
3
2
1
0
-1
-2
-3
-4
Z
-4 -3 -2 -1 0 1 2 3 4
Y
×10^38

5. Vulnerabilidades estudiadas

- Ataque de sniffing 
- Trazabilidad de los números aleatorios 
- Ataque de fuerza bruta 

5. Vulnerabilidades estudiadas: Ataque de fuerza bruta

DNIe 3.0 Brute Force



Title:/home/victor/Universidad/TFG/log

Creator:(MATLAB, The Mathworks, Inc. Ver

CreationDate:2016-08-02T13:12:05

LanguageLevel:2

Ataque de fuerza bruta
Conclusiones

- Cada intento: 1,5 s
  - 200 ms para tratar el *nonce*
  - 1,2 s para resolver Diffie-Hellman
  - 100 ms para comprobar *tokens* de sesión
- Cardinalidad del espacio de claves muy baja: 10^6
- No cuenta con ninguna defensa contra ataques de fuerza bruta
- En el peor caso:

$$10^6 \cdot 1{,}5\,s \approx 17\,días$$

Situación en la que una app maliciosa podría actuar

5. Vulnerabilidades estudiadas

- Ataque de sniffing 
- Trazabilidad de los números aleatorios 
- Ataque de fuerza bruta 

6. Propuestas de mejora

Aumento de longitud del código CAN

6. Propuestas de mejora

Aumento del tiempo de respuesta tras fallos sucesivos

Title:/home/victor/Universidad/TFG/log
Creator:(MATLAB, The Mathworks, Inc. Ver
CreationDate:2016-08-02T13:13:03
LanguageLevel:2

$$f(i)=\begin{cases} t(i) & i\leqslant 5, \\ 1.1^{i} & t(i)\leqslant 15, \\ 15 & i>15 \end{cases}$$

6. Propuestas de mejora

Bloqueo hardware

7. Conclusiones

- Dos protocolos de comunicación NFC
  - BAC
    - ✔ Teóricamente seguro
  - PACE
    - ✔ Comunicaciones cifradas
    - ✔ RNG no trazable
    - ✗ Defensa contra fuerza bruta

8. Demostración

Conclusiones personales

- NFC
- Cómo un proyecto de
- C
de investigación

FIN


DANKSCHEEI
SPASSIBO
SHUKRIA
TINGKI
BİYA
YAQHANYELAY
TASHAKKUR ATU
GRACIAS
THANK
SUKSAMA
EKHMET
ARIGATO
SHUKURIA
GOZAIMASHITA
EFCHARISTO
MAAKE
GRAZIE
MEHRBANI
PALDIES
KOMAPSUMINIDA
PAXAR
YOU
ROLZİN