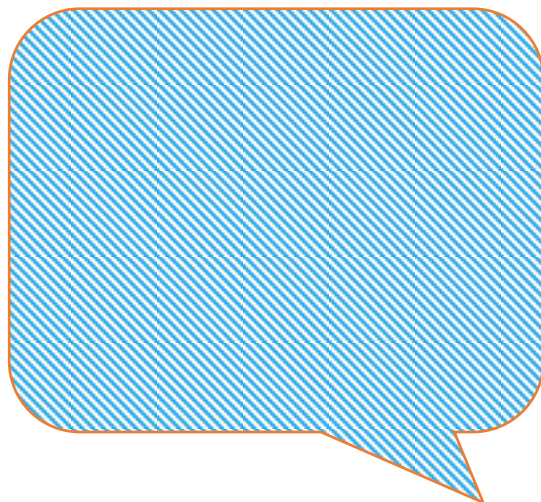




DNle3.0: vulnerabilidades, ataques y contramedidas

DIEZ AÑOS FORTALECIENDO LA
CIBERSEGURIDAD NACIONAL



- Víctor Sánchez, BSc
Universidad de Zaragoza
602665@unizar.es
(estudiante)



- Ricardo J. Rodríguez, PhD
Universidad de Zaragoza
rjrodriguez@unizar.es

Índice

- 1. Introducción**
- 2. Documento Nacional de Identidad español**
- 3. Protocolos de comunicación NFC del DNle3.0**
- 4. Análisis de seguridad NFC del DNle3.0. Experimentación (DEMO)**
- 5. Conclusiones**

1. Introducción

Robo de identidad / suplantación de identidad

- Definición: **apropiación de la identidad de una persona**
 - Problema creciente. En 2014, 117 casos denunciados (<http://www.voluntaddigital.com/suplantacion-de-identidad-y-delitos-en-internet/>)
 - **Delito según Código Penal español**
 - **Artículo 401**
 - Uso de información personal para suplantación de identidad. Hasta tres años
 - Sólo aplica si lo que se usurpa es el estado civil de otro
 - **Artículo 197** (“hacking”)
 - Acceso a una cuenta ajena (i.e., revelación de secretos)
 - Relacionado: artículo 264 (saltarse protecciones del sistema para acceder a los datos de interés)

1. Introducción

Robo de identidad / suplantación de identidad

- **¿Quién?**
 - Criminales comunes, terroristas, crimen organizado
- **¿Para qué?**
 - Contratar un préstamo, una hipoteca, línea de teléfono/Internet, ...
 - Estimación España: 4.5M de casos. Cantidad media robada de 8000€.
(<http://www.infoderechopenal.es/2015/10/delito-robo-identidad.html>)
 - **Generar trazas falsas de “localización” ¿?**



victor 21 enero, 2012 @3:01 pm

yo llevo 7 años luchando contra la mafia que me robo el dni,falsificaron mi dni,se hicieron nominas a mi nombre y pidieron creditos de millones para comprar coches y venderlos para sacarse el dinero luego claro esta no pagaban ni las multas,pues todo me viene a mi,los jueces al ser los delitos en varias provincias se inhiben y no me amparan ante los embargos de las administraciones incluso teniendo a uno de los sujetos la declaracion de que lo hizo 7 años señores esto es un infierno todos se pasan la bola.esto es usurpacion de identidad 401

<http://www.pablofb.com/pabloburgueno.com/2009/07/colaborando-con-la-agencia-efe-para-un-articulo-sobre-identidades-falsas/>

1. Introducción

Ejemplos de robo de identidad en España

<http://www.abc.es/20120420/espana/abci-suplantacion-identidades-201204191917.html>

- Vecino de Barcelona, Francesc F.G.
 - *Hobby*: robo de documentación en taquillas de gimnasios
 - Con la documentación, pedía copia de declaración de Hacienda, certificado laboral y empadronamiento. Después, solicitaba préstamos bancarios y tarjetas de crédito
 - **Imputado por delitos de estafa, usurpación de estado civil y apropiación indebida**
- Álvaro G., madrileño, 39 años
 - Fotocopia de DNI en hotel permitió al atacante **abrir cuentas “online” bancarias, telefonía, y casas de apuestas**

1. Introducción

Ejemplos de robo de identidad en España

<http://www.abc.es/20120420/espana/abci-suplantacion-identidades-201204191917.html>

- Noelia Carmena, madrileña
 - Robo de DNI en metro en 2006
 - Acusada de formar parte de **mafia de matrimonios de conveniencia**
 - Detenida 24 horas y juzgada por delitos de suplantación de personalidad, estafa y falsificación de datos. Acusada de haber cobrado 3500€ por haber pactado una boda de conveniencia
- Óscar Sánchez, catalán
 - 626 días en prisión en Italia **acusado por un delito de tráfico de drogas**
 - Vendió su DNI, siendo usado por un criminal uruguayo asociado a la camorra napolitana para alojarse en hoteles

2. Documento Nacional de Identidad español

Genésis

Fuente: http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html

- Policía: creada en 1824 por Fernando VII
 - Otorgada **potestad para emitir padrones** con diversa información:
 - Edad
 - Sexo
 - Estado
 - Profesión
 - Naturaleza del vecindario

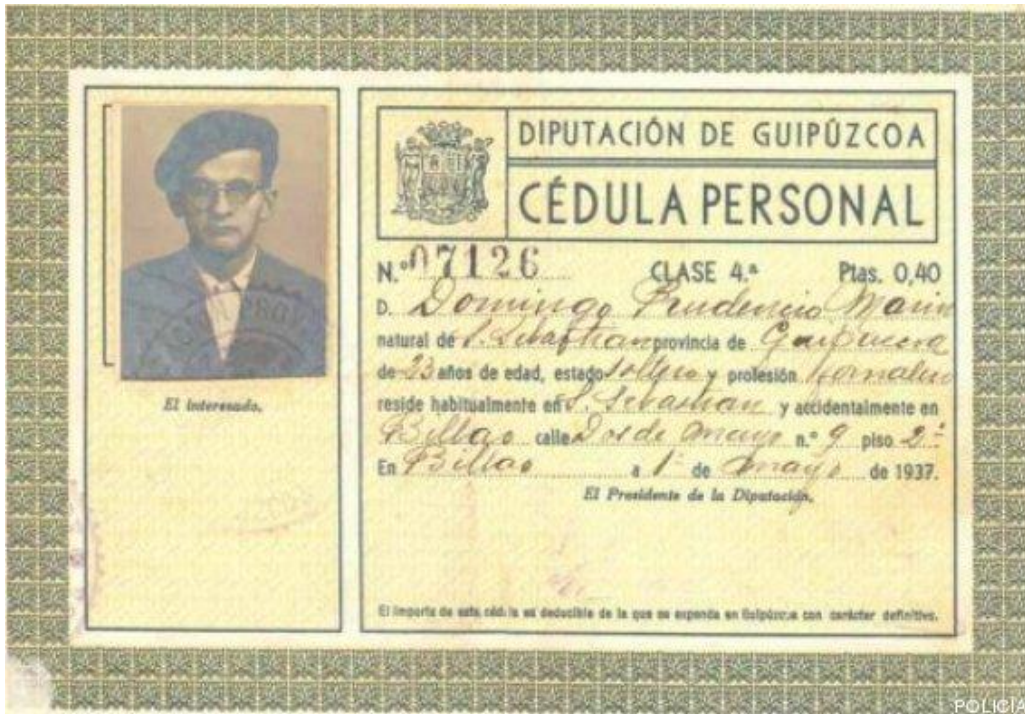
Modelo N.º 9.º

SEÑAS	
Edad	CUARTEL DE 
Estatura	Carta de seguridad por el presente año á
Pelo	favor de
Ojos	de esta vecindad, que vive
Cara	n.º c.º
Color	Dada en á de
	de 182
Firma del Portador.	El Comisario de Policía.
Pagó cuatro rs.	Gratis por ser pobre.

2. Documento Nacional de Identidad español

Éxodo

Fuente: http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html



- **Cédulas personales (1941)**
 - Emitidos por los Ayuntamientos
 - Foto opcional
 - Datos diferentes, según el sitio

2. Documento Nacional de Identidad español

Levítico (1): 1951-1961

Fuente: http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html,
<http://www.abc.es/espana/20140918/abci-historia-primer-numero-curiosidades-201409171629.html>



- **DNI versión 0.0**
- Decreto del 2 de marzo de 1944
 - Convocado concurso público. 30000 ptas!
 - Ganador: Aquilino Riusset Planchón
 - **Requisitos:** adaptarse a la cartera de bolsillo, tener espacio para impresión dactilar y una fotografía del titular. Tintas inalterables
- **1951. Primer DNI expedido: “tío Paco”**
 - Carmen Polo, nº2; Carmen Franco, nº3

2. Documento Nacional de Identidad español

Levítico (2): 1951-1961

Fuente: http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html,
<http://www.abc.es/espana/20140918/abci-historia-primer-numero-curiosidades-201409171629.html>



- **Proceso de asignación:**
 1. Presos y libertad vigilada
 2. Personal masculino que por su profesión o negocio mudaba con asiduidad de domicilio
 3. Varones residentes en ciudades de más de 100.000 habitantes
- **Zaragoza: primera ciudad de provincia**
- **1961: la Casa Real reserva del 10 al 99**
 - 10: Rey Juan Carlos; 11: Doña Sofía. El 13 se eliminó por supersitición (...)

2. Documento Nacional de Identidad español

Números

Fuente: http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html

- **1962-1965**

- Cambio a color azul
- **Añadido grupo sanguíneo y estado civil. Eliminado el sexo**

- **1965-1980**

- **Eliminado la firma del director**

- **1981-1985**

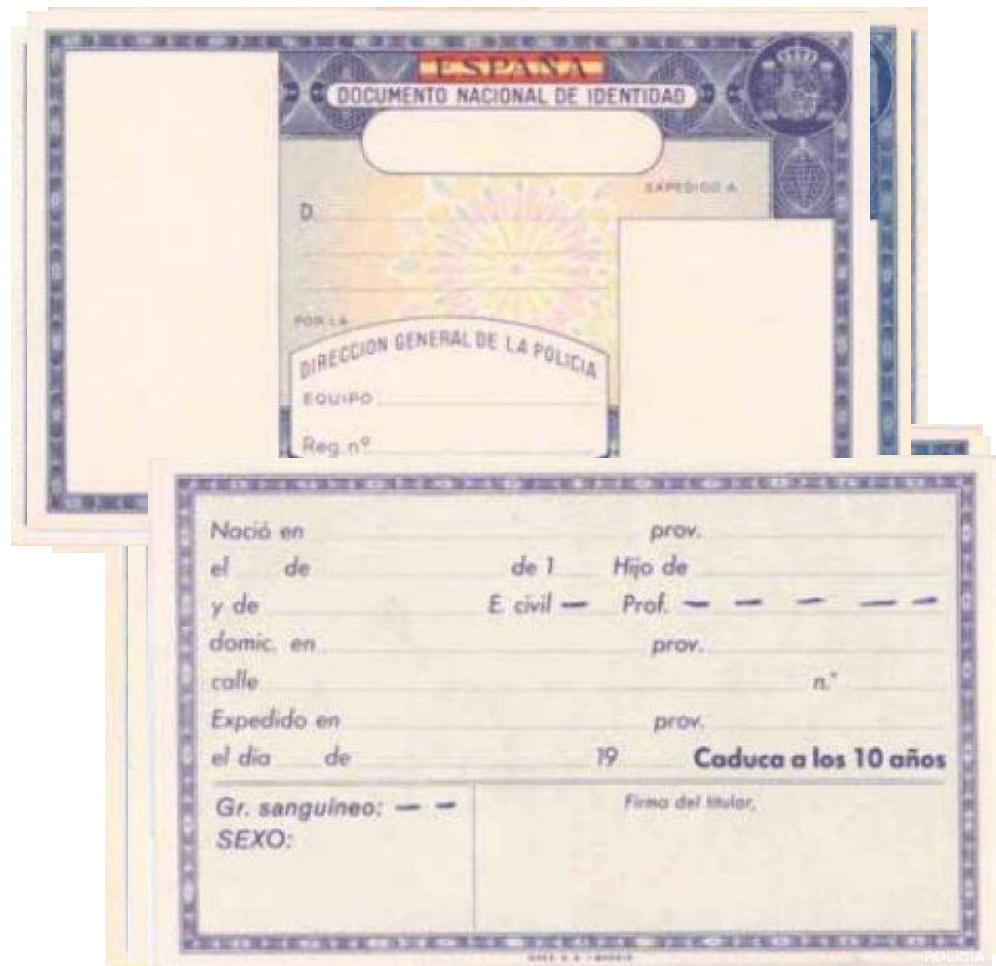
- **Añadido el escudo Constitucional y sexo**

- **1985-1991**

- Caducidad a los 10 años (>30 años)
- **Eliminados profesión, estado civil y grupo sanguíneo**
- Letra fiscal añadida en 1990
- Números repartidos manualmente. Informatizado en 1991

- Departamento creado para solucionar problema de “números erróneos”

www.ccn-cert.cni.es



2. Documento Nacional de Identidad español

Deuteronomio

Fuente: http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html



- **1991-1996:** DNI versión 1.0
 - Más pequeño
 - **Sin huella dactilar**
 - Caracteres OCR (primigenios)
- **1996-2000**
 - **Fotografía en color**
 - **Extensión datos OCR**
- **2000-2006**
 - Línea de identificación española (anverso)
 - **Sexo: M-F y V-M**

2. Documento Nacional de Identidad español

Nuevo Testamento

Fuente: http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html

- **2006-2015: DNI electrónico (versión 2.0)**
 - Elementos de seguridad física:
 - Tinta ópticamente variable
 - Microescritura
 - Fondos de seguridad
 - Kinegrama
 - Imagen láser cambiante
 - Relieves
 - **Caracteres OCR-B**
 - **Imagen en blanco y negro**

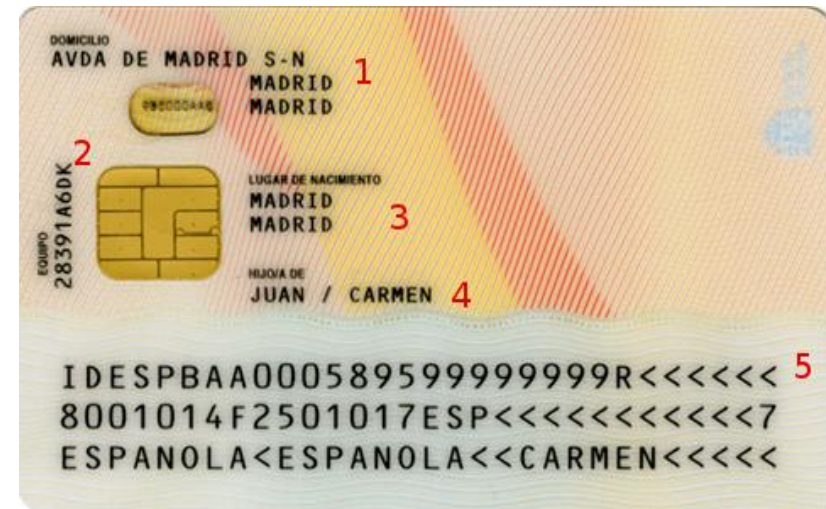


2. Documento Nacional de Identidad español

Apocalipsis (1)

Fuente: http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html

- **2015- ????: DNI electrónico (versión 3.0)**
 - Elementos de seguridad física añadidos
 - Chip electrónico: en el reverso
 - Nuevo “número” en el anverso (#11)
 - Primer DNle3.0: Mireia Belmonte
 - **Comunicación NFC (!!!)**
- **Dato:** 6M nuevos al año (datos de 2014)
- **Myth Hunters:**
 - Cifra “solitaria” del OCR es un dígito de control
 - El número de DNI es ÚNICO por ciudadano



- *Mytil*



3. Protocolos de comunicación NFC del DNle3.0

Interfaz NFC (1)

- **Nueva interfaz para comunicación sin contacto**
 - ¿Monitorizar manifestantes?
(http://www.elconfidencial.com/tecnologia/2015-01-16/identificar-a-distancia-con-el-nuevo-dni-3-0-la-n-de-nfc-significa-near_623075/)
 - **NO.** Mejor probabilidad de acierto: 0,000000020833333 ($=1/(48 \cdot 10^6)$)
- Recordemos los problemas de NFC:
 - **Eavesdropping**
 - **Modificación de información**
 - **Ataques de retransmisión**

Lectura recomendada: Informe de Amenazas CCN-CERT IA-05/16

<https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-publicos/1378-ccn-cert-ia-05-16-comunicacion-de-campo-cercano-near-field-communication-nfc-vulnerabilidades/file.html>

3. Protocolos de comunicación NFC del DNle3.0

Interfaz NFC (2)

- **¿A qué datos se puede acceder?**

- **Data Group 1**

- **Nombre y apellidos:** cadena
- Nacionalidad: cadena
- Sexo: cadena
- N° de soporte: cadena
- Fecha de expiración: cadena
- **Fecha de nacimiento:** cadena
- Emisor: cadena (valor "España")
- OptData: null
- Tipo de documento: cadena (valor "ID")

- **Data Group 2**

- **Imagen facial** (formato JPEG2000, sin metadatos)

- **Data Group 7**

- **Imagen de la firma** (formato JPEG2000, sin metadatos)

- **Data Group 11**

- Dirección: cadena
- N° DNI: cadena
- Lugar de nacimiento: cadena (e.g., valor "ZARAGOZA<ZARAGOZA")
- Title: null
- **Teléfono: null**
- **Profesión: null**
- CustodyInfo: null
- ICAOName: null
- OtherInfo: null
- Summary: null

3. Protocolos de comunicación NFC del DNle3.0

Protocolo *Basic Access Control* (BAC)

- **Estándar ICAO** (*Machine Readable Travel Documents - Part 11: Security Mechanisms for MRTDs*, 2015, http://www.icao.int/publications/Documents/9303_p11_cons_en.pdf)
 - Protege contra ataques de integridad y replay
- **Datos necesarios para empezar la comunicación:**
 - Número de soporte (3 caracteres alfabéticos + 6 numéricos)
 - Fecha de nacimiento (formato “aammdd”)
 - Fecha de expiración (formato “aammdd”)
- Deriva claves iniciales mediante SHA-1 aplicado sobre dichos datos
 - **La clave derivada tiene 16 bytes (128 bits).**
- **Protocolo de autenticación en tres pasos para establecimiento de clave simétrica de sesión**

3. Protocolos de comunicación NFC del DNle3.0

Protocolo *Password Authenticated Connection Establishment* (PACE)

- *Advanced Security Mechanisms for Machine Readable Travel Document and eIDAS Token - Part 2, 2015.* https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-2-V2_2.pdf?__blob=publicationFile
- **Protocolo Diffie-Hellman** para generar claves de sesión
 - Intercambio de claves seguro entre partes que no se “conocen” previamente
- **Datos necesarios para empezar la comunicación:**
 - Card Access Number (CAN): elemento #11. 6 dígitos
 - Del CAN se deriva otra clave con SHA1 usada para cifrar **un número aleatorio único (nonce) de 16 bytes**
- Permite obtener una clave de sesión de gran tamaño a partir de una “semilla” de tamaño pequeño: $10^6 \rightarrow 2^{128}$

3. Protocolos de comunicación NFC del DNIE

Protocolo *Password Authenticated Connection Establishment*

- *Advanced Security Mechanisms for Machine Readable Travel Documents*, 2015. <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI-TR03110.pdf>
- **Protocolo Diffie-Hellman** para generar claves
 - Intercambio de claves seguro entre partes que no se conocen previamente
- **Datos necesarios para empezar la comunicación:**
 - Card Access Number (CAN): elemento #11. 6 dígitos
 - Del CAN se deriva otra clave con SHA1 usada para cifrar **un número aleatorio único (nonce) de 16 bytes**
- Permite obtener una clave de sesión de gran tamaño a partir de una “semilla” de tamaño pequeño: $10^6 \rightarrow 2^{128}$



4. Análisis de seguridad NFC del DNle3.0. Experimentación (DEMO)

Cardinalidades del espacio de claves

• Protocolo BAC

- Número de soporte (3 caracteres alfabéticos + 6 numéricos)
 - $\log_2(26^3 \cdot 10^6) = 34.0329$
- Fecha de nacimiento (formato “aammdd”)
 - $\log_2(10^2 \cdot 365.25) = 15.1566$
 - Técnicas OSINT reducirían este valor hasta cero
- Fecha de expiración (formato “aammdd”)
 - Caducidad: 5 años si < 30 años, 10 en otro caso. Permanente > 70 años
 - $\log_2\left(10 \cdot 365.25 \cdot \frac{5}{7} - 8\right) = 11.3448$

$$34.0329 + 15.1566 + 11.3448 = 60.5343 \text{ bits}$$

• Protocolo PACE

- Número CAN (6 dígitos)
 - $\log_2(10^6) = 19.9316$

$$19.9316 \text{ bits}$$

(Ojo: ambos cumplen recomendación NIST y ECRYPT contra eavesdropping y otros ataques offline, semillas > 80bits)

4. Análisis de seguridad NFC del DNle3.0. Experimentación (DEMO)

Resistencia a fuerza bruta de códigos de acceso

- Aplicación Android realizada para atacar el protocolo PACE
 - SONY Xperia Z3 Tablet Compact. Chip NFC de Broadcom
- **PACE no informa del error hasta el final del protocolo**
 - ¡Esto es bueno!
- Medición de 500 intentos de claves. **Media: 1.4509 segundos**
 - 200ms nonce, 1200ms protocolo Diffie-Hellman, 100ms tokens de sesión
- **Conclusiones:**
 - **NO implementa defensas.** Ni aumenta tiempo, ni bloquea comunicación
 - **Ataque de fuerza posible** en $1.4509 \cdot 10^6 = 16.7928 \approx 17$ días** (caso peor)
 - Comunicación “continua” con el mismo DNI. ¿Es posible *fingerprinting*?

4. Análisis de seguridad

Resistencia a fuerza bruta

- Aplicación Android re
- SONY Xperia Z3 T

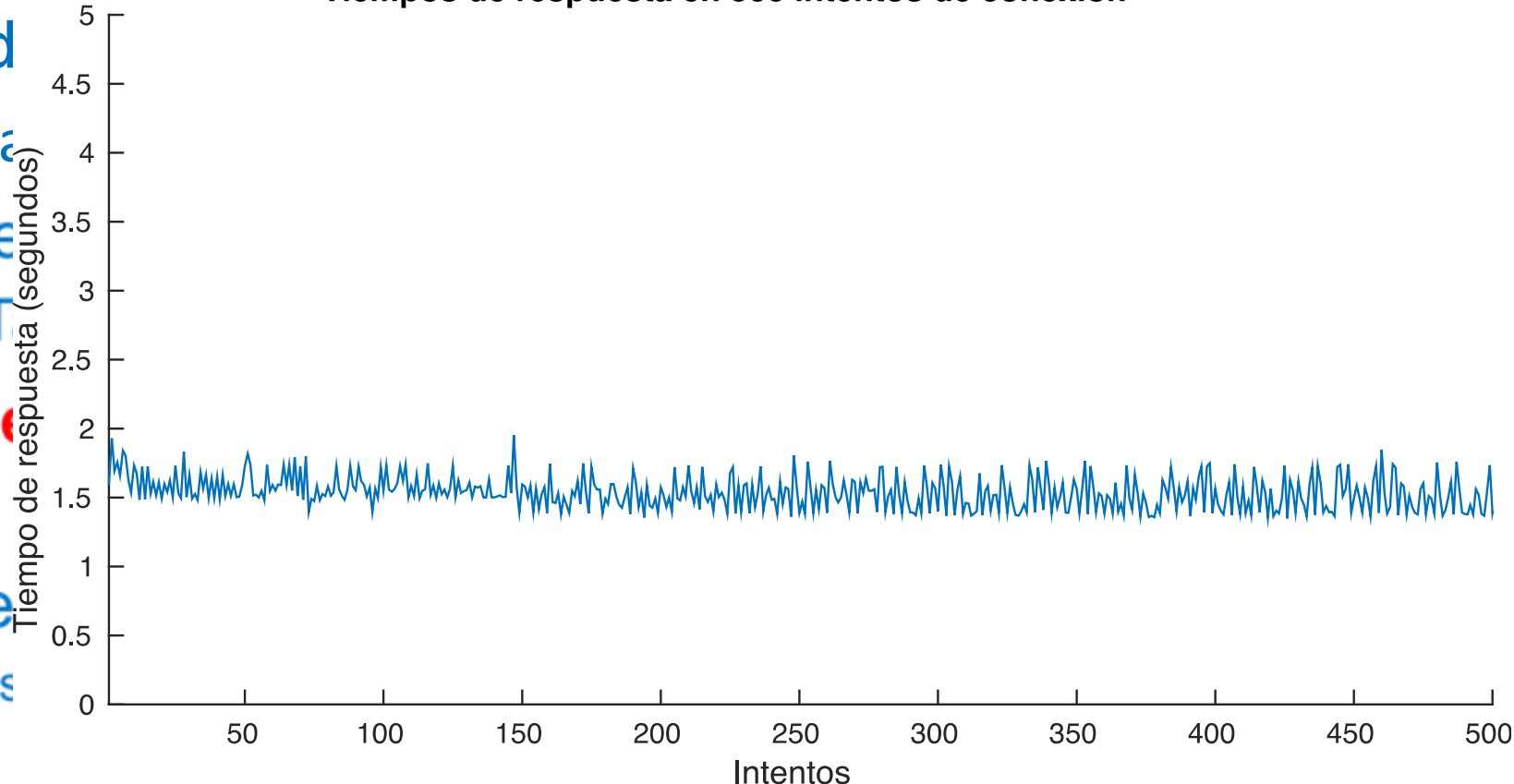
• PACE no informa de

- ¡Esto es bueno!
- Medición de 500 inte
- 200ms nonce, 1200ms

• Conclusiones:

- **NO implementa defensas.** Ni aumenta tiempo, ni bloquea comunicación
- **Ataque de fuerza posible** en $1.4509 \cdot 10^6 = 16.7928 \approx 17$ días** (caso peor)
 - Comunicación “continua” con el mismo DNI. ¿Es posible *fingerprinting*?

Tiempos de respuesta en 500 intentos de conexión



4. Análisis de seguridad NFC del DNle3.0. Experimentación (DEMO)

Generador de números aleatorios

- Aplicación Android creada para captura de nonces en PACE
 - Envío de mensaje erróneo tras recibir nonce para resetear comunicación
 - 10^5 nonces capturados
- **Necesario un buen generador de números aleatorios (PRNG)**
 - **Un mal PRNG introduce una vulnerabilidad en criptografía**
- **Test de aleatoriedad** realizados *(en colaboración con J.C. García-Escartín, UVA)*
 - NIST FIPS 1402: OK!
 - Dieharder: necesitamos más datos (¿ok?)
 - Test de entropía: 7.999894 bits/byte (OK!)
 - No se observan repeticiones (ok, ¿ciclo largo?)
- **Conclusiones:**
 - **El PRNG NO tiene ningún sesgo apreciable**
 - Está bien hecho. ¡La distribución forma un paralelepípedo perfecto!

4. Análisis de seguridad NFC de Generador de números aleatorios

- Aplicación Android creada para
 - Envío de mensaje erróneo tras recibir
 - 10^5 nonces capturados

- **Necesario un buen generador**

- Un mal PRNG introduce una

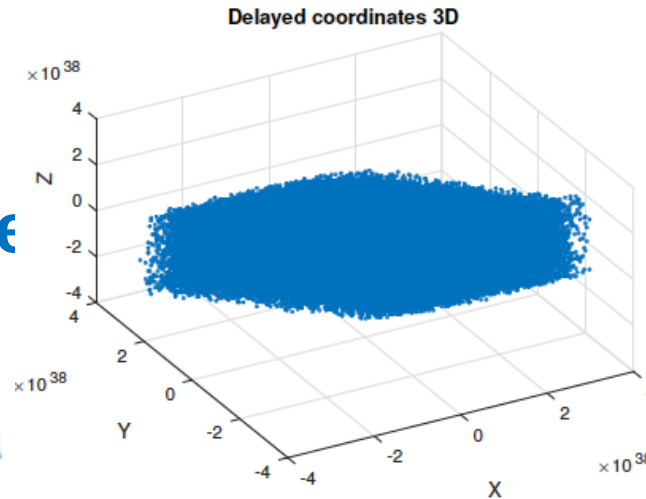
- **Test de aleatoriedad realizado:**

- NIST FIPS 1402: OK!
 - Test de entropía: 7.999894 bits/byte

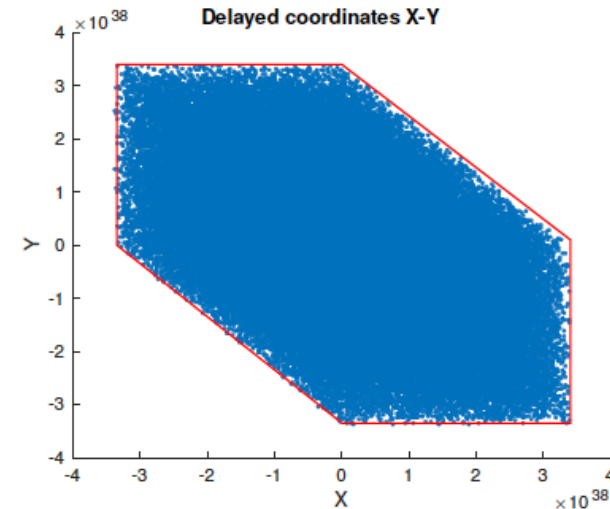
- **Conclusiones:**

- **El PRNG NO tiene ningún sesgo apreciable**

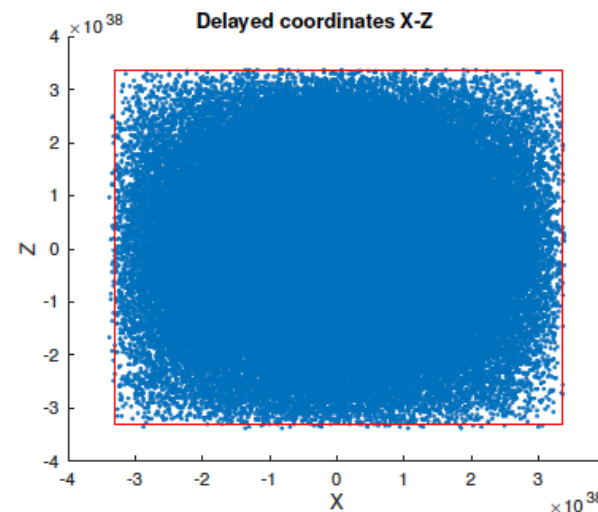
- Está bien hecho. ¡La distribución forma un paralelepípedo perfecto!



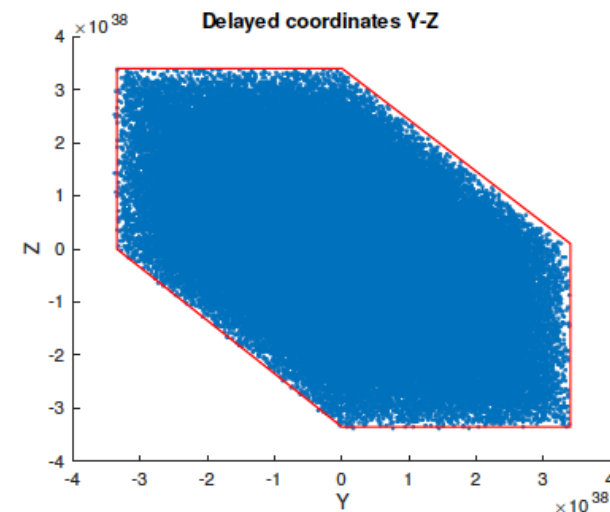
(a) Delayed coordinates 3D



(b) Delayed coordinates ejes X-Y



(c) Delayed coordinates ejes X-Z



(d) Delayed coordinates ejes Y-Z

4. Análisis de seguridad NFC del DNle3.0. Experimentación (DEMO)

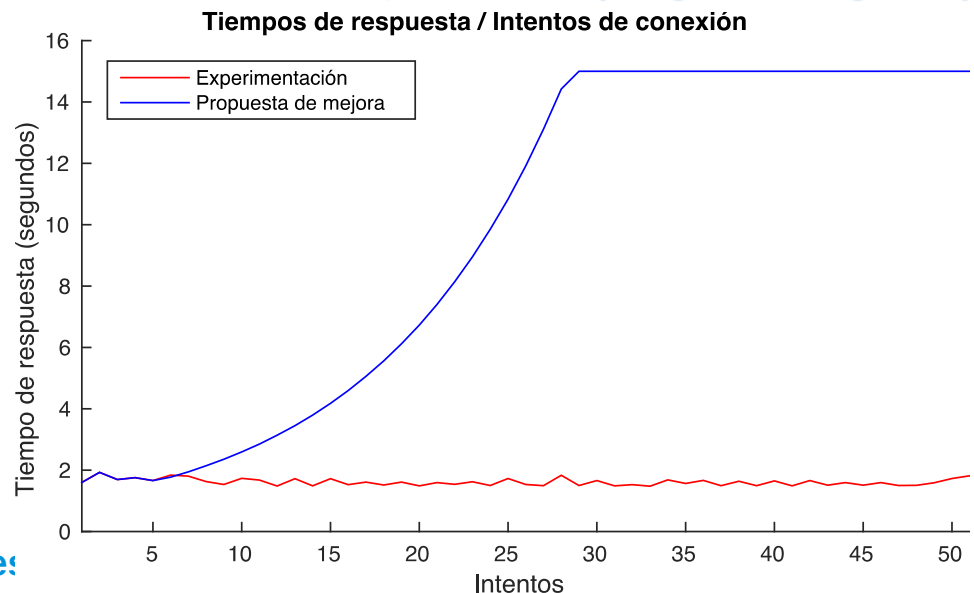
DEMO – ataque de fuerza bruta a protocolo PACE



4. Análisis de seguridad NFC del DNle3.0. Experimentación (DEMO)

Soluciones de mejora

- **Aumento de cardinalidad de CAN**
 - Aumentando órdenes de magnitud, conseguimos:
 - 17 días → 168 días (1 orden); 17 días → 46 años (3 órdenes)
- **Aumento de tiempo de respuesta tras error en establecimiento PACE**
 - Implementado en pasaportes electrónicos de otros países (e.g., Bélgica)
 - $$f(x) = \begin{cases} t(x), & x < 5 \\ \max(t(x), 1.1^x), & x \leq 15 \\ 15, & x > 15 \end{cases}$$
- **Bloqueo NFC hardware**
 - Como bloqueo de SD cards
 - Huella dactilar como 2FA : ?



5. Conclusiones

- **DNle3.0 incorpora chip NFC: “hereda” vectores de ataque**
 - **Eavesdropping**
 - Posible, dado que es RFID. Se mantiene confidencialidad por la criptografía
 - **Modificación**
 - No es posible, dada la criptografía que hay debajo
 - **Retransmisión:** *No experimentado en este trabajo, pero seguro que sí (¿voluntarios?)*
- **¿Es seguro?**
 - **Las semillas cumplen recomendaciones NIST/ECRYPT** ☐
 - **Generador de números aleatorios:** pasa diversos test de aleatoridad ☐
 - La distribución forma un paralelepípedo perfecto ☐
 - **Espacio de claves pequeño, en el caso de PACE** ☐
 - Ojo, cumple con el estándar ICAO. No es implementación (léase decisión) propia
 - **No hay protección frente a ataques de fuerza bruta** ☐
 - Permite extraer datos del DNI en 17 días, en caso peor (suponiendo comunicación continua)

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

