Ataques de retransmisión inteligente en protocolos de pago NFC

Trabajo Fin de Grado Ingeniería Informática

Guillermo Cebollero Abadías
Director: Ricardo J. Rodríguez
Ponente: José Merseguer Hernáiz

Universidad de Zaragoza. Septiembre 2018

Tabla de contenidos

Introducción

Introducción (I)

Tarjetas crédito/débito

- ISO/IEC 7810
- Los pagos se realizaban inicialmente con la banda magnética
- Sustituidas actualmente por las tarjetas ꞇ ꞩ ꝛ ʙ ◭ ℰ ɕ Lj ◭ ʙ ꝛ ɕ

Introducción (I)

Tarjetas crédito/débito

- ISO/IEC 7810
- Los pagos se realizaban inicialmente con la banda magnética
- Sustituidas actualmente por las tarjetas ƚ ʂ ʐ ʙ ◭ Ɛ ɞ Lj ◭ ʙ ʐ ɞ

Tarjetas ƚ ɬ ʒ ɞ ʔ Ɛ ƚ ʔ ɸ Ù r r

- ƚ ʂ ʐ ʙ ◭ Ɛ ɞ Lj ◭ ʙ ʐ ɞ + comunicación por NFC

Introducción (II)

Comunicación de campo cercano o NFC

- Comunicación inalámbrica a 13.56 Mhz y hasta 10 cm
- Sin restricciones de uso

Introducción (II)

Comunicación de campo cercano o NFC

- Comunicación inalámbrica a 13.56 Mhz y hasta 10 cm
- Sin restricciones de uso

Dos elementos

- **Activo**: Genera el campo electromagnético. (PCD = datáfono)
- **Pasivo**: Modula la información usando el campo (PICC = tarjeta)

Introducción (II)

Comunicación de campo cercano o NFC

- Comunicación inalámbrica a 13.56 Mhz y hasta 10 cm
- Sin restricciones de uso

Dos elementos

- **Activo**: Genera el campo electromagnético. (PCD = datáfono)
- **Pasivo**: Modula la información usando el campo (PICC = tarjeta)

Modos de interacción

- Lector/Escritor
- ĖÙÙ◭²ɀ◭ĖÙÙ◭
- «ɀʳ²◭GƐ◭Lj◭_ ɔ ·ɆƐ²ʐɀɞ

Introducción (III)

EMV (EUROPAY, MASTERCARD Y VISA)

- Estándar de interoperabilidad
- Implementaciones propietarias
  $\dot{E}\mathcal{E}_{\lrcorner}\check{S}\,\mathcal{E}_{,}\grave{U}$ (VISA) y $\dot{E}\mathcal{E}_{\lrcorner}\dot{E}\mathcal{E}^{r\,r}$ (MASTERCARD)

Introducción (III)

EMV (EUROPAY, MASTERCARD Y VISA)

- Estándar de interoperabilidad
- Implementaciones propietarias
  $\dot{E}\mathcal{E}_{\lrcorner}\check{S}\,\mathcal{E}_{,}\grave{U}$ (VISA) y $\dot{E}\mathcal{E}_{\lrcorner}\dot{E}\mathcal{E}^{r\,r}$ (MASTERCARD)

ʙʙ₡ʒƐʔʒʒʁ Ėȼʒʔʒʂʒ₡ PƐʔƐ ı·ʁʒʔ o APDU

- ISO/IEC 7816
- Comando:
  5 bytes cabecera y 255 bytes de información opcionales
- Respuesta:
  256 bytes de información y 2 bytes de estado de terminación

Motivación

Según el CES

- 15.2% ha realizado pagos 𝔰𝔨𝔷𝔢²ℰ𝔰²ℙ𝕌̀ʳ ʳ
- 52.4% conoce la existencia de las tarjetas 𝔰𝔨𝔷𝔢²ℰ𝔰²ℙ𝕌̀ʳ ʳ

Motivación

Según el CES

- 15.2% ha realizado pagos ꞅɬʒɞ²Ɛꞅ²ɬÙʳʳ
- 52.4% conoce la existencia de las tarjetas ꞅɬʒɞ²Ɛꞅ²ɬÙʳʳ

Fácil acceso a la tecnología NFC

- 400+ móviles compatibles (según NFCWorld)
- Nuevos riesgos de seguridad añadidos:

  _Ɛ¸ÙʳLjȶɬʒʙʙɮɞÊ

  Ataques ɔƐɞ◮ɮɞ◮²ʂÙ◮ɔɮLjLjɬÙ

  Ataques de retransmisión

Motivación

Según el CES

- 15.2% ha realizado pagos ꞅɬʒɞ²Ɛꞅ²ɬÙʳʳ
- 52.4% conoce la existencia de las tarjetas ꞅɬʒɞ²Ɛꞅ²ɬÙʳʳ

Fácil acceso a la tecnología NFC

- 400+ móviles compatibles (según NFCWorld)
- Nuevos riesgos de seguridad añadidos:

  _Ɛ¸Ùʳ Lj¢ɬʒʙʙ ɮɞÊ

  Ataques ɔƐɞ◮ɮɞ◮²ʂÙ◮ɔ ɮLjLjɬÙ

  Ataques de retransmisión

Aumento del fraude

- $22.800 millones en 2016 (+4.4% respecto a 2015)

Objetivos

Objetivos

1. Verificar si es necesario retransmitir todas las tramas
2. Intentar aumentar el tiempo máximo de transacción
3. Mejorar y añadir funcionalidades a la aplicación NFCLeech

Ataques de retransmisión

Ataques de retransmisión

- ~ȼƐɞLj GṣÜ ʳ ʳ ÚƐ ʳ ²Üȼ ĖȼƘƴƑÜ ɔ, Conway 1976.

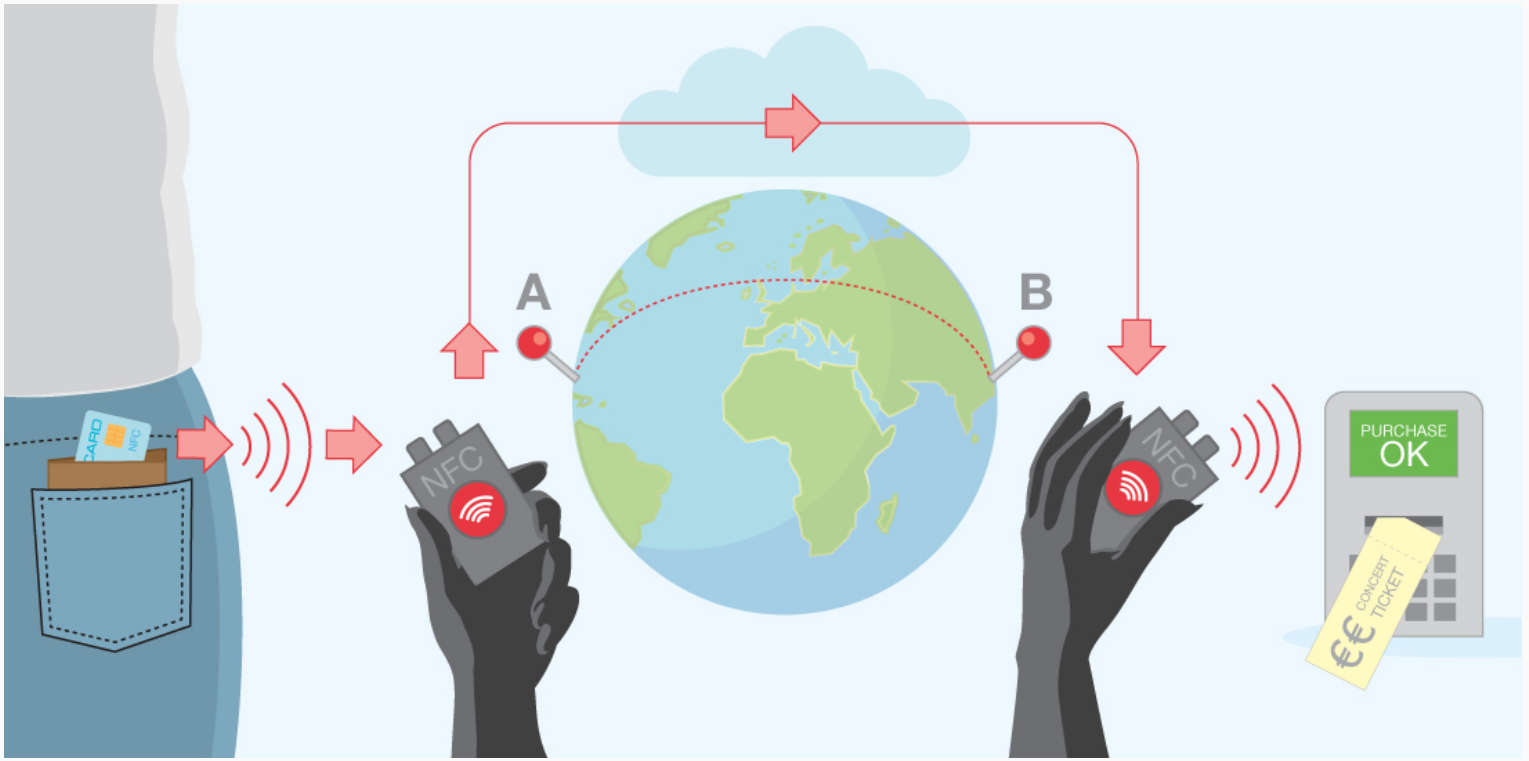
Ataques de retransmisión

‹~¢Ɛ¢Lj GşÜʳ ʳÚƐ ʳ²Ü¢ Ė¢ƗƵƳ¢Ü ɔ ›, Conway 1976.

Introducir agentes artificiales

Mole Emula un $\dot{E}GP$ y se comunica con la tarjeta (Punto A)

Proxy Emula una $\dot{E}^3GG$ y se comunica con el TPV (Punto B)



Ataques de retransmisión inteligente (I)

Es necesario definir qué tramas es necesario retransmitir

Ataques de retransmisión inteligente (I)

Es necesario definir qué tramas es necesario retransmitir

Cacheables
Estáticas

No cacheables
Generadas dinámicamente
Firmadas digitalmente

Ataques de retransmisión inteligente (I)

Es necesario definir qué tramas es necesario retransmitir

Cacheables
Estáticas

No cacheables
Generadas dinámicamente
Firmadas digitalmente

Tramas dependientes del protocolo utilizado

Ataques de retransmisión inteligente (II)

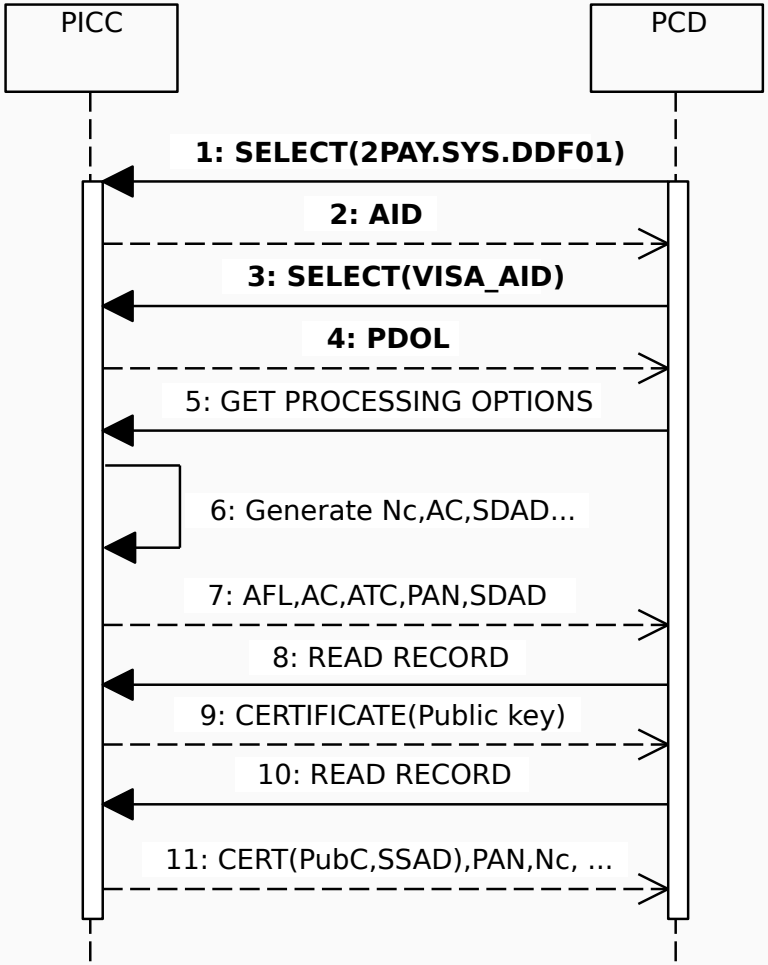


Figura 1: $\dot{E}\mathcal{E}_{\lrcorner}\check{S}\mathcal{E}_{\urcorner}\mathring{U}$ (VISA)

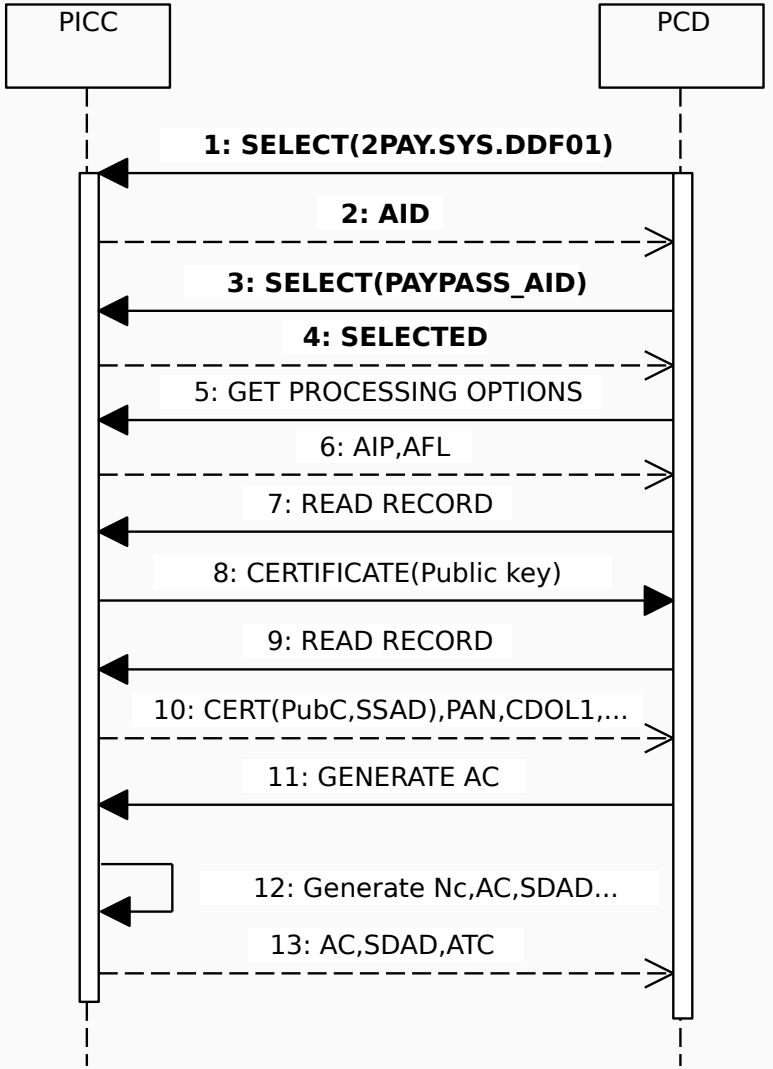


Figura 2: $\dot{E}\mathcal{E}_{\lrcorner}\dot{E}\mathcal{E}^{r\,r}$ (MASTERCARD)

Aplicación Android NFCLeech

Aplicación Android NFCLeech (I)

Prueba de concepto

- José Vila Bausili y Ricardo J. Rodríguez (2014)
- Retransmisión por WiFi y ~~WiFi Direct~~
- Retransmisión exitosa a más de 5700Km (Nueva York-Madrid) [presentado en 11th International Workshop on RFID Security (RFIDSec'15)]

Aplicación Android NFCLeech (I)

Prueba de concepto

- José Vila Bausili y Ricardo J. Rodríguez (2014)
- Retransmisión por WiFi y ~~WiFi Direct~~
- Retransmisión exitosa a más de 5700Km (Nueva York-Madrid) [presentado en 11th International Workshop on RFID Security (RFIDSec'15)]

Desventajas

- Uso complejo
- Aplicación inestable

Aplicación Android NFCLeech (II)

Mejoras introducidas

Aplicación Android NFCLeech (II)

Mejoras introducidas

- Nuevo sistema de registro

Figura 3: Captura de la aplicación

Aplicación Android NFCLeech (II)

Mejoras introducidas

- Nuevo sistema de registro
- Inclusión de los códigos de estado

Figura 3: Captura de la aplicación

Aplicación Android NFCLeech (II)

Mejoras introducidas

- Nuevo sistema de registro
- Inclusión de los códigos de estado
- Formateado de las tramas

Figura 3: Captura de la aplicación

Aplicación Android NFCLeech (II)

Mejoras introducidas

- Nuevo sistema de registro
- Inclusión de los códigos de estado
- Formateado de las tramas
- Modos de impresión dinámica

Figura 3: Captura de la aplicación

Aplicación Android NFCLeech (II)

Mejoras introducidas

- Nuevo sistema de registro
- Inclusión de los códigos de estado
- Formateado de las tramas
- Modos de impresión dinámica
- Lectura de datos de la tarjeta

Figura 3: Captura de la aplicación

Aplicación Android NFCLeech (II)

Mejoras introducidas

- Nuevo sistema de registro
- Inclusión de los códigos de estado
- Formateado de las tramas
- Modos de impresión dinámica
- Lectura de datos de la tarjeta
- Estabilidad

Figura 3: Captura de la aplicación

Aplicación Android NFCLeech (II)

Mejoras introducidas

- Nuevo sistema de registro
- Inclusión de los códigos de estado
- Formateado de las tramas
- Modos de impresión dinámica
- Lectura de datos de la tarjeta
- Estabilidad
- Refactorización del código

Figura 3: Captura de la aplicación

Aplicación Android NFCLeech (II)

Mejoras introducidas

- Nuevo sistema de registro
- Inclusión de los códigos de estado
- Formateado de las tramas
- Modos de impresión dinámica
- Lectura de datos de la tarjeta
- Estabilidad
- Refactorización del código
- Bluetooth

Figura 3: Captura de la aplicación

Estrategias para alargar la comunicación

WTX

WTX: Š ƐɻʔɻɞÊ ɪɻ ɘ Ů Ůt ʔŮɞ ʳɻʒɞ o Aumento del tiempo de espera

WTX

WTX: *Š ƐɻʔɻɷÊ ɪɻ ɔ Ů Ůŧ ʔŮɷ ʳɻʒɷ* o Aumento del tiempo de espera

Estrategia: Solicitar aumento del tiempo de procesamiento

WTX

WTX: *Š Ɛʅ²ʅɞÊ ɪʅ ɔ Ů Ůt²Ůɞ ʳʅƷɞ* o Aumento del tiempo de espera

Estrategia: Solicitar aumento del tiempo de procesamiento

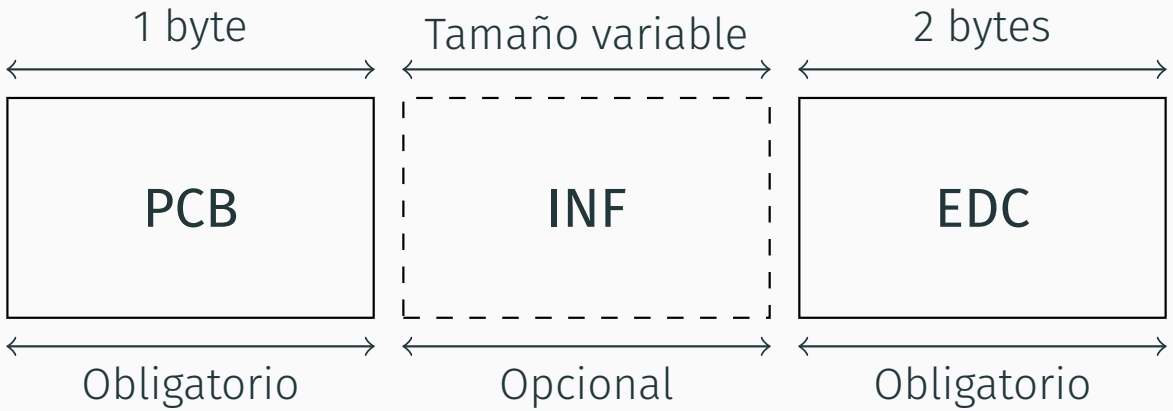


Figura 4: Bloque de transmisión de protocolo

PCB *ĖȡƷ²ƷsƷɆ GƷɞ²ȡƷɆ @ˍ²Ů.*
INF *³ɞâƷȡ ɔ Ɛ²ʅƷɞ {ʅŮɆLj.*
EDC *_ȡȡƷȡ PŮ²Ůs²ʅƷɞ GƷLjŮ.*

WTX

WTX: *Š Ɛʔʔɛ Ê ɪʔ ɔ Ù Ù t ʔÙ ɾʔʒ* o Aumento del tiempo de espera

Estrategia: Solicitar aumento del tiempo de procesamiento

	Byte(s)	Decimal	Hexadecimal
PCB	1 1 1 1 0 0 1 0	242	F2
INF	0 0 1 1 1 0 1 1	59	3B
$\_PG_1$	1 0 0 1 0 0 0	72	48
$\_PG_2$	1 1 0 1 1 1 1 0	222	DE

Tabla 1: Codificación del WTX antes del CRC

WTX

WTX: Š Ɛʔʔɛ Ê ɪʔ ɔ Ù Ù t ʔÙ ɾʔʒ o Aumento del tiempo de espera

Estrategia: Solicitar aumento del tiempo de procesamiento

	Byte(s)	Decimal	Hexadecimal
PCB	1 1 1 1 0 0 1 0	242	F2
INF	0 0 1 1 1 0 1 1	59	3B
$\_PG_1$	1 0 0 1 0 0 0	72	48
$\_PG_2$	1 1 0 1 1 1 1 0	222	DE

Tabla 1: Codificación del WTX antes del CRC

Estrategia descartada debido a que la implementación los considera errores del protocolo

NAK

NAK: ƤƷ² GÊɞƷ~ɆÜLjÊÜ ɘ Üɞ² o No reconomiento

NAK

NAK: ÞƷ² GÊɞƷ~ɬÜLjÊÙ ɘ Ùɞ² o No reconomiento

Estrategia: Introducir errores de recepción en la comunicación

NAK

NAK: $Þ\not{h}^{?}$ $G\hat{E}\mathfrak{s}\not{h}\sim\not{E}\grave{U}Lj\hat{E}\grave{U}\ \mathfrak{d}\ \grave{U}\mathfrak{s}^{?}$ o No reconomiento

Estrategia: Introducir errores de recepción en la comunicación

	Byte(s)	Decimal	Hexadecimal
PCB	1 0 1 1 0 0 1 0	178	B2
$\_PG_1$	0 1 1 0 0 1 1 1	103	67
$\_PG_2$	1 1 0 0 0 1 1 1	199	C7

Tabla 2: Codificación del NAK

NAK

NAK: Þƪ² GÊɞƪ~ɆÙLjÊÙ ɘ Ùɞ² o No reconomiento

Estrategia: Introducir errores de recepción en la comunicación

	Byte(s)	Decimal	Hexadecimal
PCB	1 0 1 1 0 0 1 0	178	B2
$\_PG_1$	0 1 1 0 0 1 1 1	103	67
$\_PG_2$	1 1 0 0 0 1 1 1	199	C7

Tabla 2: Codificación del NAK

Estrategia descartada debido a que únicamente reenvía la última trama

Cacheo de mensajes

Estrategia: Retransmitir mensajes antes de iniciar la comunicación

Cacheo de mensajes

Estrategia: Retransmitir mensajes antes de iniciar la comunicación

Mensajes cacheables

- SELECT(PPSE) y RESPONSE(PPSE)
- SELECT(AID) y RESPONSE(AID)

Cacheo de mensajes

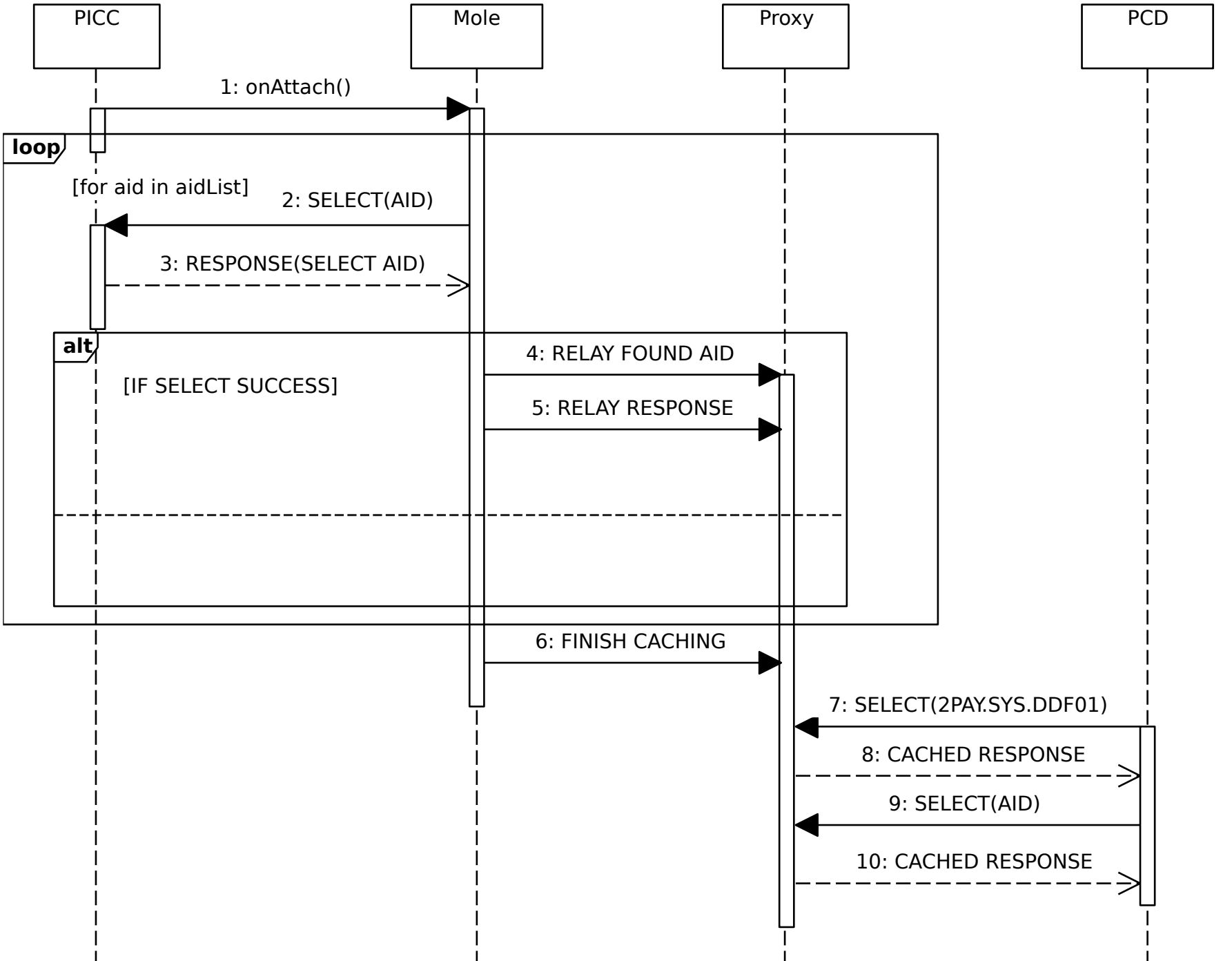
Estrategia: Retransmitir mensajes antes de iniciar la comunicación

Mensajes cacheables

- SELECT(PPSE) y RESPONSE(PPSE)
- SELECT(AID) y RESPONSE(AID)

Lista de AIDs pública y accesible en Internet

Cacheo de mensajes



Cacheo de mensajes

Estrategia: Retransmitir mensajes antes de iniciar la comunicación

Mensajes cacheables

- SELECT(PPSE) y RESPONSE(PPSE)
- SELECT(AID) y RESPONSE(AID)

Lista de AIDs pública y accesible en Internet

Estrategia viable

Experimentos

Experimentos (I)

Hardware utilizado

Experimentos (I)

Hardware utilizado

1. TPV Verifone VX680-G

Experimentos (I)

Hardware utilizado

1. TPV Verifone VX680-G
2. (x2) Samsung Galaxy Core 2 (Android 4.4.2)

Experimentos (I)

Hardware utilizado

1. TPV Verifone VX680-G
2. (x2) Samsung Galaxy Core 2 (Android 4.4.2)
3. Tarjeta ꞩƷɞˀƐꞩˀɆǛʳʳ Visa Electron

Experimentos (I)

Hardware utilizado

1. TPV Verifone VX680-G
2. (x2) Samsung Galaxy Core 2 (Android 4.4.2)
3. Tarjeta $\mathfrak{s}\mathfrak{k}\mathfrak{z}\mathfrak{e}^{?}\mathcal{E}\mathfrak{s}^{?}\mathbb{E}\grave{\mathcal{U}}^{r\,r}$ Visa Electron
4. Tarjeta $\mathfrak{s}\mathfrak{k}\mathfrak{z}\mathfrak{e}^{?}\mathcal{E}\mathfrak{s}^{?}\mathbb{E}\grave{\mathcal{U}}^{r\,r}$ Mastercard Debit

Experimentos (II)

VISA		MASTERCARD	
Exp	$\mathfrak{e}^r$	Exp	$\mathfrak{e}^r$
1	961	1	1221
2	1135	2	1001
3	1043	3	1138
$\bar{x}$	1041.52	$\bar{x}$	1112.45
s	87.05	s	111.10
G_x	8.36%	G_x	9.99%

Tabla 3: Tiempos con la versión inicial mediante WiFi

VISA		MASTERCARD	
Exp	$\mathfrak{e}^r$	Exp	$\mathfrak{e}^r$
1	698	1	803
2	740	2	710
3	619	3	696
4	679	4	707
5	759	5	837
$\bar{x}$	695.43	$\bar{x}$	746.30
s	54.96	s	64.69
G_x	7.90%	G_x	8.67%

Tabla 4: Tiempos tras la implementación del cacheado mediante WiFi

$\bar{x}$ Media aritmética | s Desviación estándar | G_x Coeficiente de variación

Experimentos (II)

VISA	
Exp	$\mathfrak{e}^r$
1	961
2	1135
3	1043
$\bar{\ }$	1041.52
s	87.05
$G_{\cdot}$	8.36%

MASTERCARD	
Exp	$\mathfrak{e}^r$
1	1221
2	1001
3	1138
$\bar{\ }$	1112.45
s	111.10
$G_{\cdot}$	9.99%

Tabla 3: Tiempos con la versión inicial mediante WiFi

Reducción 33% del tiempo de transacción

VISA	
Exp	$\mathfrak{e}^r$
1	698
2	740
3	619
4	679
5	759
$\bar{\ }$	695.43
s	54.96
$G_{\cdot}$	7.90%

MASTERCARD	
Exp	$\mathfrak{e}^r$
1	803
2	710
3	696
4	707
5	837
$\bar{\ }$	746.30
s	64.69
$G_{\cdot}$	8.67%

Tabla 4: Tiempos tras la implementación del cacheado mediante WiFi

$\bar{\ }$ Media aritmética | s Desviación estándar | $G_{\cdot}$ Coeficiente de variación

Experimentos (III)

VISA		MASTERCARD	
Exp	θ^r	Exp	θ^r
1	698	1	803
2	740	2	710
3	619	3	696
4	679	4	707
5	759	5	837
$\bar{x}$	695.43	$\bar{x}$	746.30
s	54.96	s	64.69
G_x	7.90%	G_x	8.67%

Tabla 5: Tiempos tras la implementación del cacheado mediante WiFi

VISA		MASTERCARD	
Exp	θ^r	Exp	θ^r
1	665	1	704
2	653	2	694
3	676	3	755
4	697	4	766
5	667	5	693
$\bar{x}$	671.28	$\bar{x}$	721.05
s	16.39	s	35.26
G_x	2.44%	G_x	4.89%

Tabla 6: Tiempos tras la implementación del cacheado mediante Bluetooth

$\bar{x}$ Media aritmética | s Desviación estándar | G_x Coeficiente de variación

Conclusiones

Conclusiones

Conclusiones

Conclusiones

- Las tarjetas $\mathfrak{s}\mathfrak{k}\mathfrak{z}\mathfrak{e}^{?}\mathcal{E}\mathfrak{s}^{?}\mathbb{E}\grave{\dot{U}}^{r\,r}$ tienen una mayor cuota de mercado cada día

Conclusiones

Conclusiones

- Las tarjetas $\mathfrak{sh}\mathfrak{z}\mathfrak{e}^{?}\mathfrak{E}\mathfrak{s}^{?}\mathfrak{U}^{r\,r}$ tienen una mayor cuota de mercado cada día
- La inclusión de NFC incluye nuevos vectores de ataque

Conclusiones

Conclusiones

- Las tarjetas $\mathfrak{s}\mathfrak{k}\mathfrak{z}\mathfrak{e}^{?}\mathcal{E}\mathfrak{s}^{?}\mathfrak{k}\grave{\mathcal{U}}^{r\,r}$ tienen una mayor cuota de mercado cada día
- La inclusión de NFC incluye nuevos vectores de ataque
- No es necesario un hardware especializado para realizar los ataques y/o pruebas de concepto

Conclusiones

Conclusiones

- Las tarjetas $\mathfrak{s}\mathfrak{k}\mathfrak{z}\mathfrak{e}^{?}\mathcal{E}\mathfrak{s}^{?}\mathfrak{k}\grave{U}^{r\,r}$ tienen una mayor cuota de mercado cada día
- La inclusión de NFC incluye nuevos vectores de ataque
- No es necesario un hardware especializado para realizar los ataques y/o pruebas de concepto
- El protocolo EMV no es resistente a ataques de retransmisión inteligentes

Conclusiones

Conclusiones

- Las tarjetas $\mathfrak{s}\mathfrak{k}\mathfrak{z}\mathfrak{e}^{?}\mathcal{E}\mathfrak{s}^{?}\mathbb{U}^{r\,r}$ tienen una mayor cuota de mercado cada día
- La inclusión de NFC incluye nuevos vectores de ataque
- No es necesario un hardware especializado para realizar los ataques y/o pruebas de concepto
- El protocolo EMV no es resistente a ataques de retransmisión inteligentes
- Viabilidad de los ataques reducida en entornos reales, pero posible con hardware especializado

¿Preguntas?