Prevenzione frodi e innovazione: la Multicanalità

Roma, 6 novembre 2015

Massimo Dossena

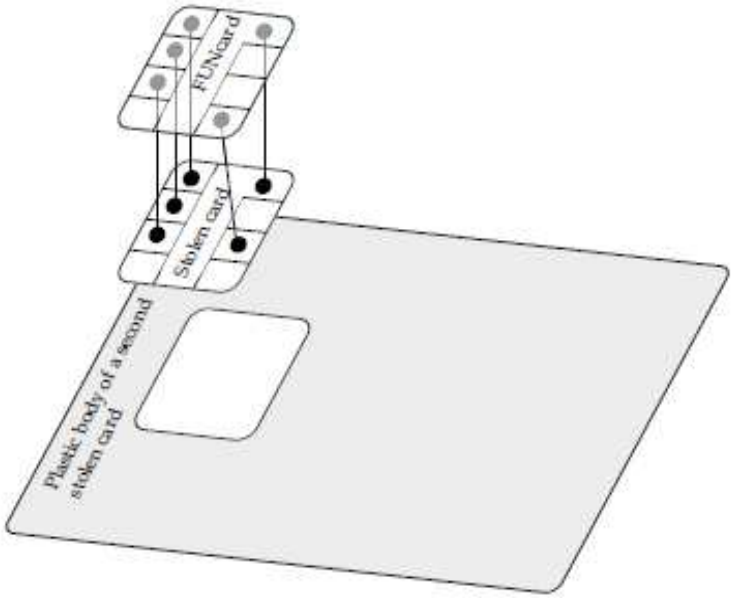
Resp. Prevenzione Frodi

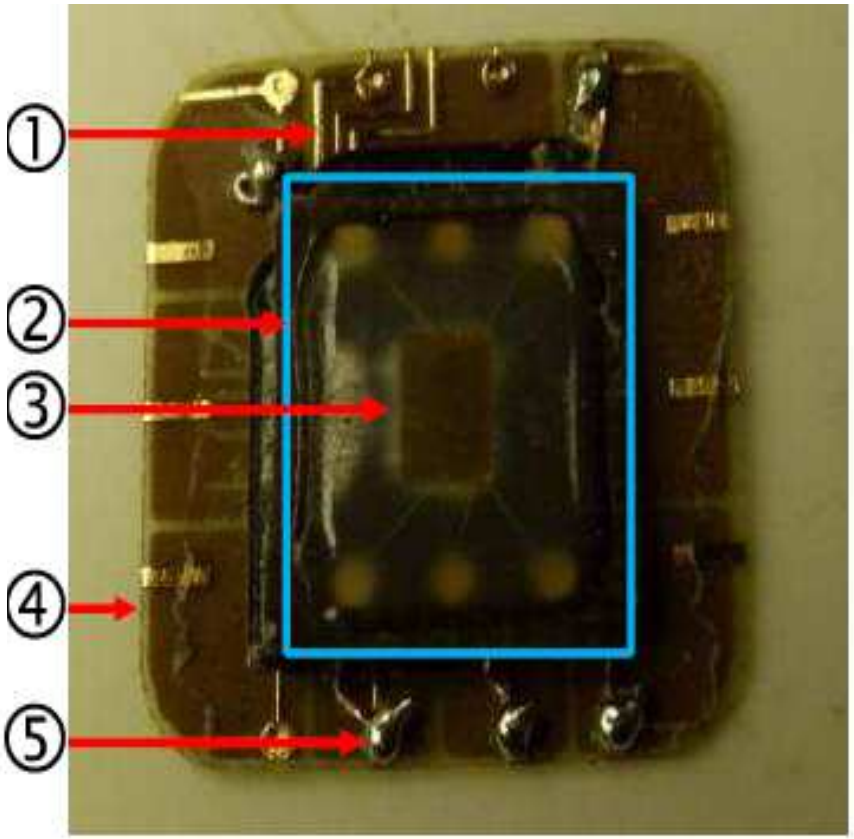
Gruppo Banco popolare

Man in the middle attack

- Maggio 2011 alcune carte di emittenti francesi vengono rubate e utilizzate in Belgio su POS con transazioni EMV.
- La frode viene effettuata alterando il colloquio tra il Pos e il chip presente sulla carta tramite un secondo chip (Fun) che viene posizionato sopra l'originale.
- L'autorizzazione delle transazioni avviene in modalità offline.
- Con 40 carte rubate sono state effettuate circa 7.000 transazioni per un valore di 600.000€.
- L'analisi della tecnica utilizzata è stata effettuata dall'École normale supérieure Computer Science Department di Parigi.

Man in the middle attack



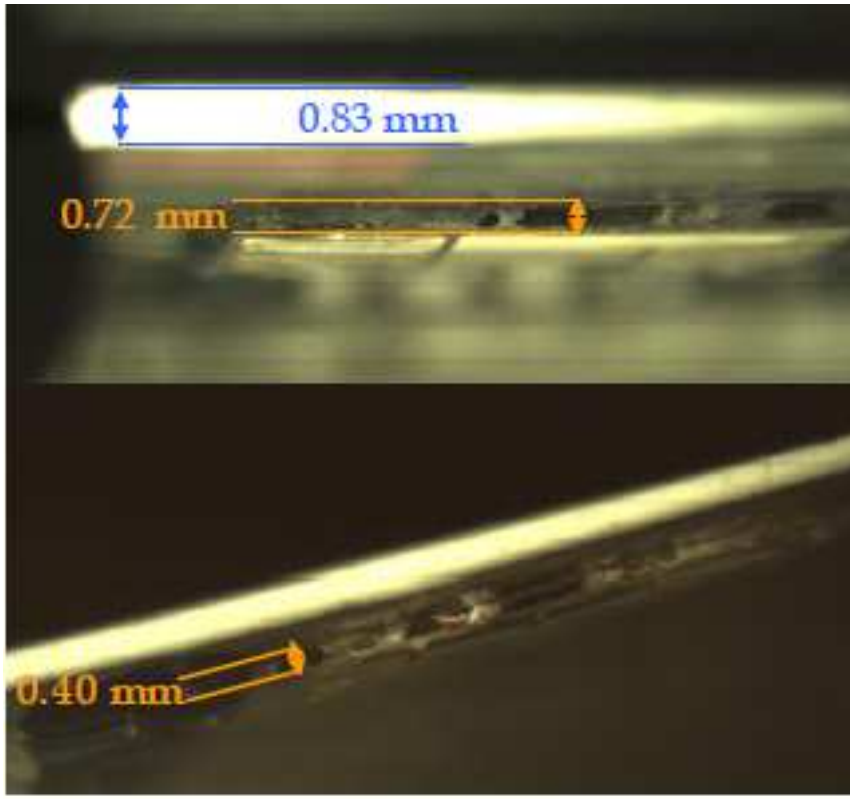


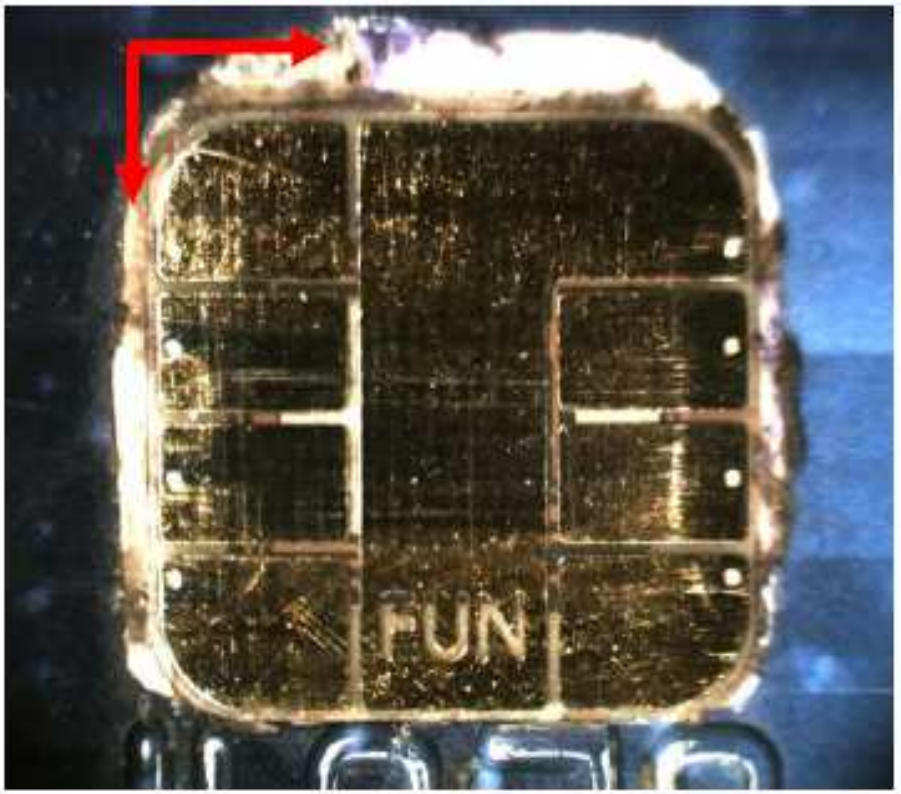
Man in the middle attack

Come agisce il chip Fun:

- altera alcuni parametri inviati dalla carta al POS, come ad es. l'ATC (application transaction counter), allo scopo di creare le condizioni per autorizzare in modalità offline.
- impedisce la verifica del pin da parte del chip genuino della carta (non inoltrando il comando "Verify PIN"disposto dal POS) restituendo al POS, in modo fittizio, un esito positivo alla verifica del PIN.
- induce il chip genuino a elaborare un crittogramma di autorizzazione in offline (TC).

Man in the middle attack





Man in the middle attack

Condizioni per attuare la frode:

- carta genuina regolarmente emessa da un issuer.
- la carta deve avere la possibilità di autorizzare una transazione, sia per importo che per numero di transazioni, in modalità offline.
- la CVM list della carta non deve prevedere come unici metodi di verifica il pin offline e/o il pin online.

Man in the middle attack

- Rilevamento e contromisure della frode
- Rilevamento:
  - Monitorare i log EMV presenti nei messaggi di clearing inoltrati all'issuer anche post blocco della carta.
  - Una volta rilevata la frode è necessario "caricare" il numero carta nelle Stop List dei circuiti.
- Contromisure:
  - Personalizzare la componente EMV della carta limitando l'autonomia della stessa ad operare in off line (agendo sui limiti per importo e sul numero di transazioni autorizzabili in offline).
  - Personalizzare la CVM limitando l'applicazione della "FIRMA" o del "NO CVM", come metodi di verifica del cliente.

Host card Emulation (HCE)

- Pagamento NFC
- Secure Element smaterializzato
- Generazione di Token per il pagamento
- App in grado di dialogare con NFC Controller
- Operazione EMV compliant card present
- Utilizzo del Wallet

Host card Emulation (HCE)

Host card Emulation (HCE)

Alcuni punti di attenzione per la prevenzione frodi:

1. Gestione dei token (generazione e utilizzo)
2. Analisi dello stato di sicurezza del device
3. Enrollment della carta sul wallet
4. Accesso/utilizzo del wallet
5. Cambio del telefono
6. Combinare gli elementi della transazione con le informazioni del device

Wallet

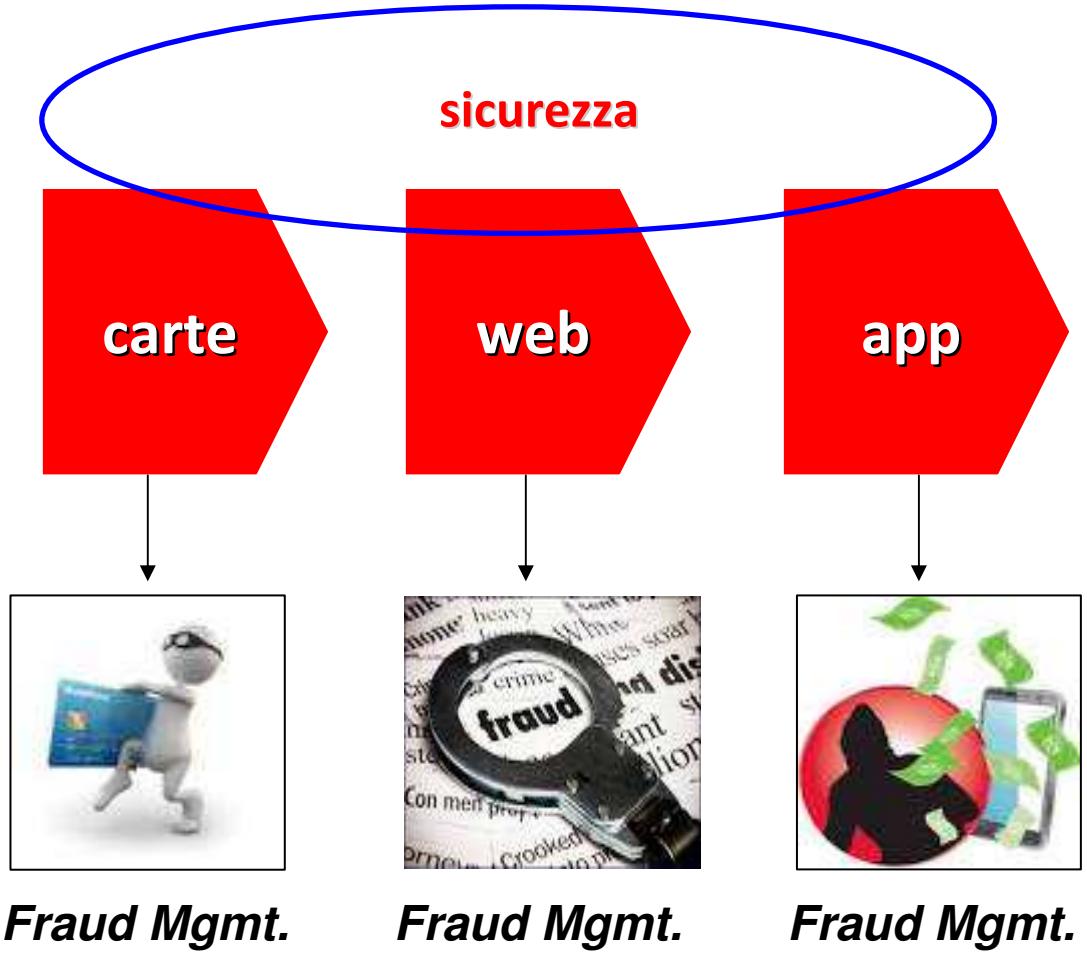
- Utilizzare una sola App di pagamento
- Multicanalità – Acquisto tramite canali internet, mobile e fisico
- Utilizzo carte di emittenti diversi
- Accesso a tutti i servizi con un unico set di credenziali
- Collegare il wallet ad altri sistemi di accettazione dei pagamenti

Wallet

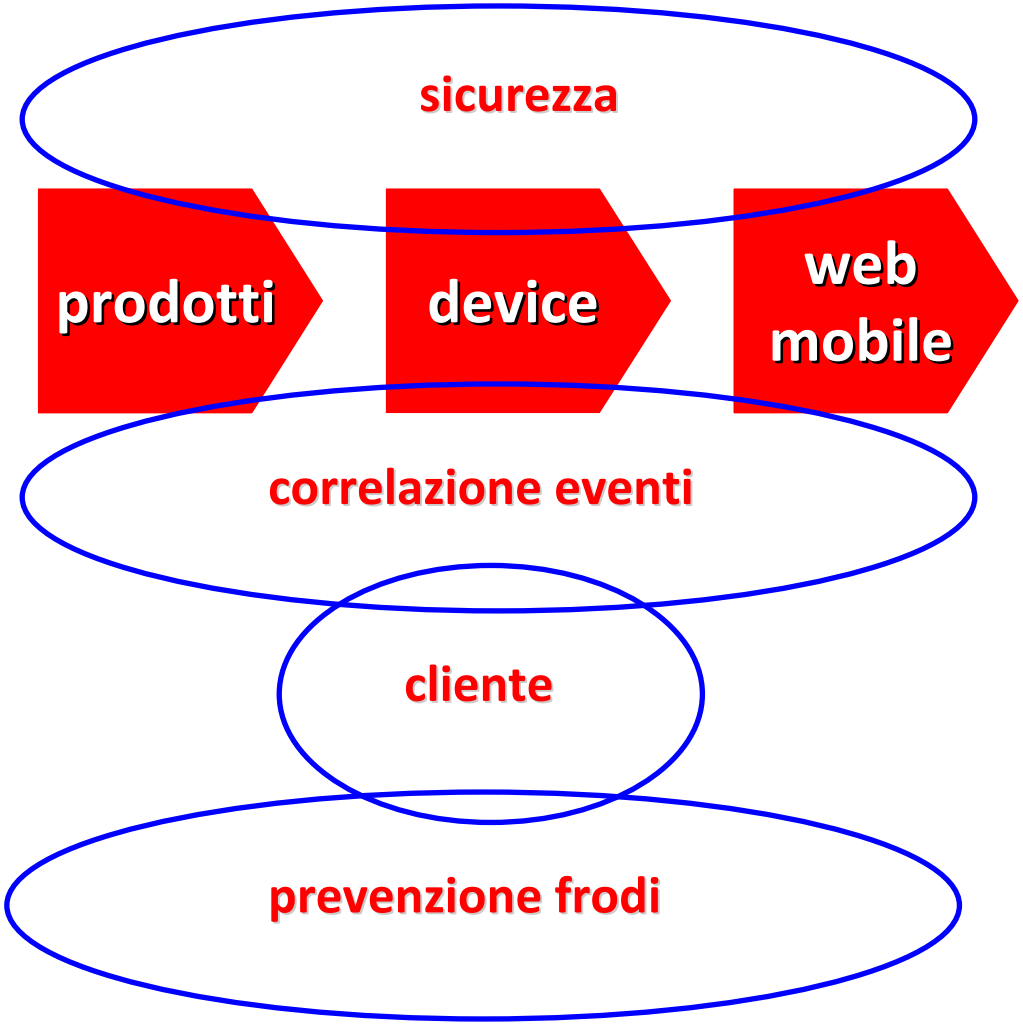
Alcuni punti di attenzione per la prevenzione frodi:

1. Analisi dello stato di sicurezza del device
2. Enrollment della carta sul wallet
3. Accesso/utilizzo del wallet
4. Cambio del telefono
5. Analisi dello stato di sicurezza del device
6. Combinare gli elementi della transazione con le informazioni del device
7. Il wallet deve consentire il mascheramento dei dati della carta
8. Certificazione PCI/DSS

Oggi


sicurezza
carte
web
app
fraud
Fraud Mgmt.
Fraud Mgmt.
Fraud Mgmt.

Multicanalità



La multicanalità è un processo articolato che richiede una analisi dettagliata e distintiva tramite una correlazione specifica

Massimo Dossena

Resp. Prevenzione Frodi

Gruppo Banco Popolare

massimo.dossena@sgsbp.it