E-money
dove sono i miei soldi?

Alessio Orlandi
Marco Valleri

Introduzione

Acronimi

- POS – Point Of Sale
- ATM – Automatic Teller Machine
- PAN – Personal Account Number
- PIN – Personal Identification Number
- OTP – One Time Password
- DMT – Digital Monetary Trust
- SSL – Secure Socket Layer

Introduzione
Agenda

- Credit/Debit Card, POS e ATM, On-line Payment
- PayPal
- DMT-ALTA
- Conclusioni e riferimenti

Credit/Debit Card
POS e ATM
On-line Payment

Moneta di Plastica
Credit Card e Debit Card

- Credit Card
  - Concetto limite d'utilizzo
  - Addebito differito
  - Informazioni "embossed"
  - Utilizzo tramite PAN e informazioni satellite
- Debit Card (Bancomat)
  - Banda Magnetica
  - Protezione con PIN

Moneta di Plastica
Elementi identificativi (1/3)

- Identificazione manuale
  - PAN – Identificativo carta
    - Codice di lunghezza variabile (16-19 cifre)
    - Presenza di “checksum” – possibilita’ di generare codici algoritmicamente validi
  - Expiration Date
  - Nome Intestatario
  - Address Verification System*
  - Card Security Code*

*utilizzabile in assenza del possessore

Moneta di Plastica

Elementi identificativi (2/3)

- Identificazione “strisciata”
  - Track 1 – codice alfanumerico (210 BpI)
  - Track 2 – codice alfanumerico (75 BpI)
  - Track 3 – codice alfanumerico (210 BpI)

ISO 7811

Moneta di Plastica
Elementi identificativi (3/3)

- PIN
  - Quando viene richiesto?
  - Come viene generato?
  - Come viene verificato?
- Metodi anti frode
  - Random Number

POS e ATM
Elementi in gioco

- Credit/Debit Card
- Transazione
- Sportello/Negoziante
- Infrastruttura di comunicazione
- Circuito (Inter)Bancario

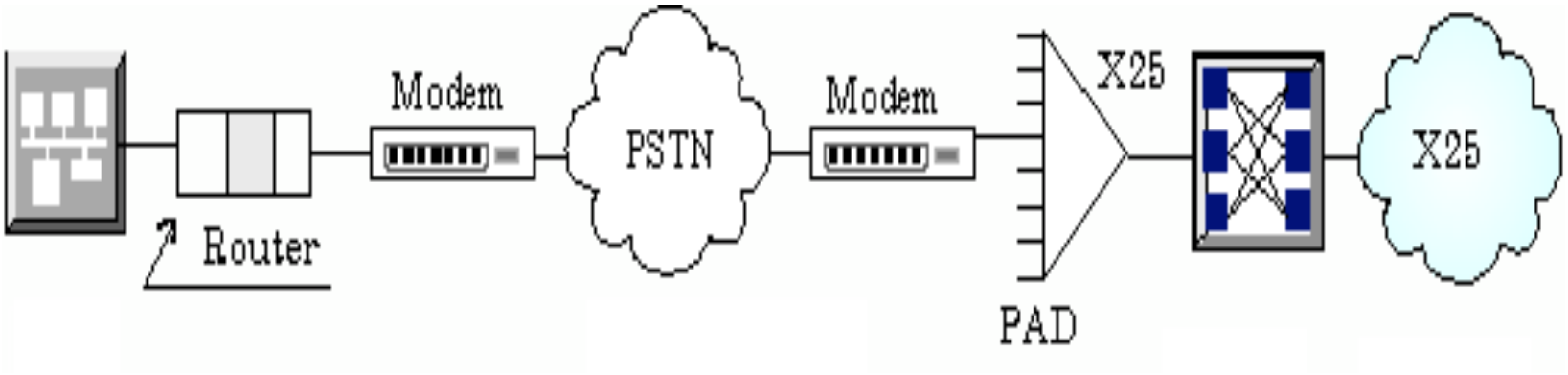
POS e ATM

Infrastruttura di rete (1/3)

- Sistema di interconnessione basato sullo standard X.25
  - In fase di transizione su IP encapsulated
- Modalità di accesso alla rete
  - Collegamento X.25 diretto
  - POTS (rete telefonica)
  - ISDN D Channel (T3POS)

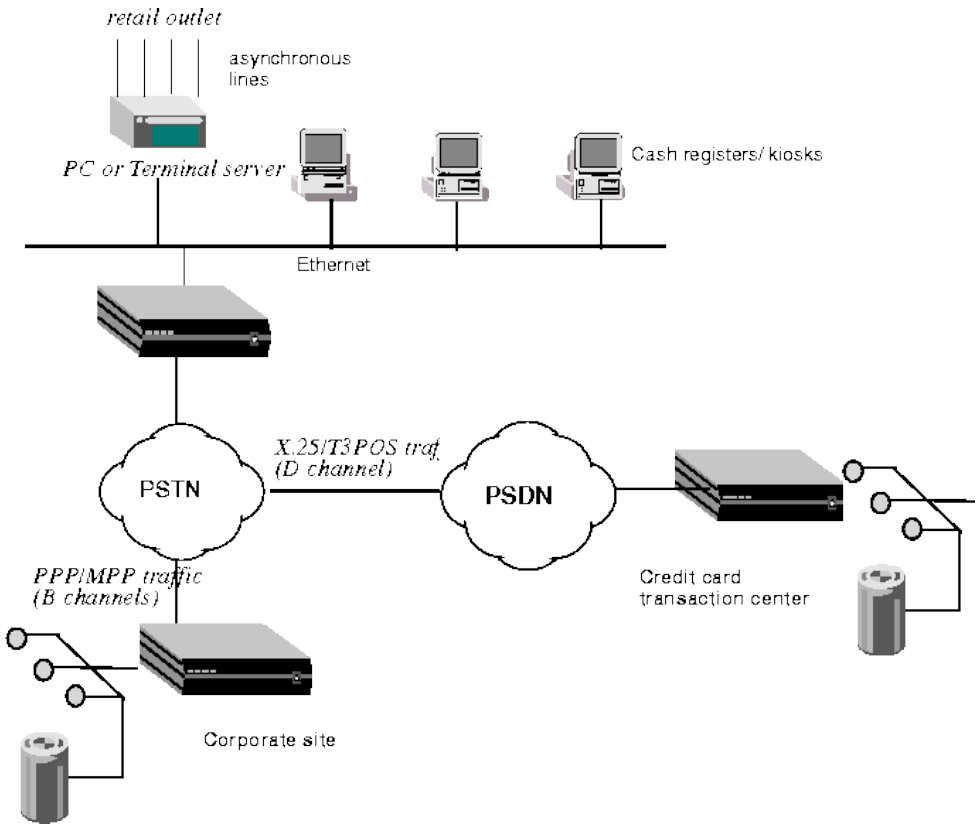
POS e ATM

Infrastruttura di rete (2/3)



POS e ATM

Infrastruttura di rete (3/3)



POS e ATM

…ma siamo sicuri?

- Integrità apparati
- Sistemi protezione PIN e transazioni
- Sistemi antifrode
- Utilizzo di chip
- Difficoltà di accesso alla rete (s.t.o.)

- Mancanza di standard “forti”
- Utilizzo di carte clonate/forgiate

On-line Payment
Elementi in gioco

- Credit Card
- Transazione
- Personal Computer
- Infrastruttura di comunicazione
- Seller
- On-line Payment Gateway
- Circuito Bancario

On-line Payment

Infrastruttura di rete

- Comunicazione tramite TCP/IP (Internet)
- Utilizzo di protocolli di cifratura/autenticazione (SSL)
- Gateway verso il Circuito Bancario
  - OTP
  - Certificati Digitali

On-line Payment

…ma siamo sicuri?

- Utilizzo di cifratura e autenticazione “forti”
  - Fra Utente e Seller
    - L’utente e’ l’anello debole della catena (ettercap)
  - Fra Seller e Circuito Bancario
    - Punto critico di passaggio di informazioni
- Memorizzazione delle informazioni della carta di credito
- Assenza di conferma istantanea della transazione
  - Necessità di verificare l’ammontare tramite estratto conto

PayPal

PayPal
Tipi di account

- Unverified
  - Richiede carta di credito
- Verified
  - Richiede possesso effettivo della carta
- Business
  - Richiede la presentazione dei dati di un conto bancario intestato

PayPal
Operazioni

- Versamento
- Giroconto
- Prelievo

PayPal
…ma siamo sicuri?

- SSL
- Verifica del proprietario della carta
- Fiducia verso PayPal

- Memorizzazione delle informazioni di carta di credito
- Riscontro effettivo del momento di prelievo

DMT/ALTA

DMT/ALTA
Struttura

- DMT: Circuito di conti bancari
- ALTA: Interfacciamento DMT con il mondo
- E-gold: Circuito per l'acquisto di Oro virtuale

DMT/ALTA

Da “fuori” a “dentro” (1/2)

- Creo un account anonimo su ALTA
- Il circuito ALTA lo associa dinamicamente ad alcuni conti DMT.
- Acquisto oro a mio nome su un account del circuito e-gold (con carta di credito)
- Informo il circuito ALTA della cifra che voglio depositare

DMT/ALTA

Da “fuori” a “dentro” (2/2)

- Il circuito ALTA genera un Claim Number univoco per la transazione
- Trasferisco dal mio account e-gold ad un account e-gold, di cui ALTA e’ intestatario, la cifra desiderata utilizzando il Claim Number come causale
- ALTA associa la transazione al mio account ALTA quando reinserisco il claim number
- ALTA effettua il prelievo e lo deposita sui conti DMT
- DMT mantiene in movimento i soldi tra vari conti.

- La stessa procedura puo’ essere effettuata al contrario

DMT/ALTA

…ma siamo sicuri?

- Sistema completamente basato su tecniche crittografiche pubbliche
- Totale anonimicita’
- Nessun gestore/operatore umano

- Molto recente
- Fiducia nel sistema

Conclusioni

- L’utente e’ l’anello debole
- In qualche modo le informazioni di verifica e quelle immesse debbono convergere (SPOF)
- Importanza della copertura assicurativa
- Nuovi standard in arrivo

Riferimenti

- www.paypal.com
- www.orlingrabbe.com/dmt_guide.htm
- www.blackmarket-press.net
- ettercap.sf.net

naga@antifork.org

nail@itapac.net

Messenger says…

Never give out your password or credit card number in an instant message conversation.