Studio, progettazione ed implementazione di applicativi mobili per pagamenti elettronici

Giuseppe Criscione

A.A. 2020/2021

Dipartimento di Matematica e Informatica
Corso di Laurea Magistrale in Informatica

In collaborazione con

intrapresa
LOADING INNOVATION

Sommario

Il lavoro di tesi è stato svolto presso **Intrapresa Srl**, azienda leader nel settore della distribuzione carburanti, con focus sui **pagamenti elettronici** utilizzati all'interno del circuito di fidelizzazione. Il lavoro ha riguardato i seguenti punti:

- Studio delle tipologie di pagamento utilizzate
- Studio Tecnologie di pagamento
- Sicurezza dei pagamenti
- Sviluppo di applicativi di pagamento
- Sviluppo sicuro di un applicativo per POS Android

Tipologie di pagamento

Ad oggi, le principali tipologie di pagamento utilizzate sono le seguenti:

- **Smartcard**
  - Banda magnetica: dati in chiaro, nessuna sicurezza
  - Chip: ISO/IEC 7810 e ISO/IEC 7816
  - NFC: pagamenti contactless
- **Mobile Wallet**
  - Google Pay: intermediario offre servizi di virtualizzazione
  - Apple Pay: emulazione delle carte
- **Mobile Web Payments**
  - PayPal: sistema di pagamento ad hoc con funzione di proxy

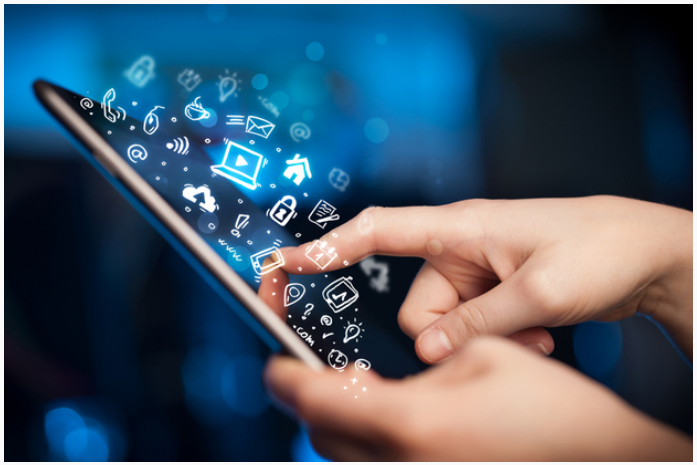
La fase di **sviluppo sicuro**, si può riassumere in tre punti fondamentali:

1. Definire gli obiettivi
2. Elaborare un Threat Modelling
3. Eseguire i test di sicurezza

Sviluppo applicativi mobili: obiettivi

L'utilizzo base dell'app comprende la rendicontazione della carte privative dell'utente. L'obiettivo è quindi aggiungere all'app la possibilità di effettuare pagamenti elettronici all'interno del circuito aziendale, ovvero aggiungere:

- Pagamenti contactless
- Ricarica del wallet tramite carta di credito o prepagata
- Effettuare rifornimento in self direttamente dall'app tramite carta privativa, di credito o prepagata



Sviluppo applicativi mobili: pagamenti contactless

Obiettivo: riuscire a comunicare con un POS per completare una transazione contacless tramite **NFC**.

- Funzionalità utilizzabile solo su sistemi **Android**
- Utilizzo di HCE (Host Card Emulation) per emulare il chip della carta basato sullo stack ISO/IEC 14443 e ISO/IEC 7816-4.
- Integrare l'utilizzo di un AID a 16 byte per la comunicazione

Sviluppo applicativi mobili: ricarica del wallet

Obiettivo: riuscire a ricaricare un wallet di carte privative attraverso una **carta di credito o prepagata**.

- È necessario un maggior controllo sul flusso della transazione
- Ente di pagamento intermedio per lo scambio della valuta
- Accredito nel conto privativo dell'utente
- Gestione della sessione della transazione
- Gestione dei dati della carta e dell'utente

Sviluppo applicativi mobili: rifornimento self

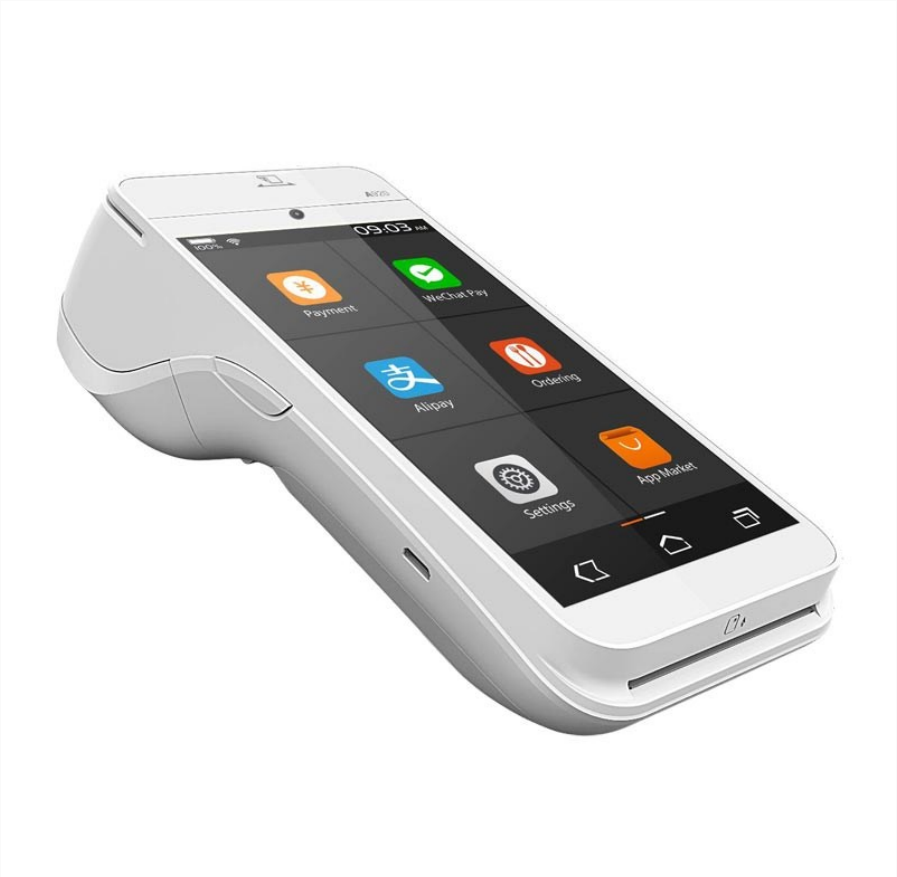
Obiettivo: effettuare il rifornimento in modalità self **direttamente dall'app**.

- Scelta dell'impianto, della carta di pagamento, dell'importo e della pompa di erogazione.
- Inserimento del PIN della carta: generazione del **PIN Block**.
- Preautorizzazione al pagamento: controllo sul PIN e sul saldo.
- Rifornimento: abilitazione della pompa di erogazione.
- Pagamento dell'importo effettivo: storno dell'importo preautorizzato e accredito dell'importo erogato.

Sviluppo applicativi mobili: applicativo POS

Obiettivo: rendere sicuro l'applicativo aziendale del **POS Android**.

- Gestire le chiavi di **cifratura** e segreti in maniera accorta.
- Utilizzo corretto delle operazioni crittografiche.
- Utilizzo della memoria sicura specifica del POS.
- Corretta esecuzione dell'app all'interno del sistema operativo.



Threat Modelling

- Rappresentazione del modello in questione da analizzare
- Identificazione delle componenti da proteggere e le relative minacce (**STRIDE**)
- Analisi del sistema dal punto di vista di un attaccante
- Identificazione di possibili misure di sicurezza

Threat Modelling

Modello	Minaccia	Proprietà	Rischio
Credenziali	S, R, EoP, T	A, I, NR, AU	Moderato
Carte di pagamento	S, T, ID, EoP	I, C, A	Alto
PIN	S, T, EoP, DoS, ID	I, C, AU, NR, D	Alto
Ricarica carta	S, T, DoS, ID	AU, NR, D	Moderato
Pagamenti contactless	S, T, R, DoS, EoP	A, I, NR, D	Alto
Pagamenti self	S, T, R, DoS, EoP	A, I, NR, D	Alto

Modello	Minaccia	Proprietà	Rischio
Firma dell'applicativo	T, DoS	A, I, C, D	Alto
Log di sistema	ID	C	Moderato
Segreti memorizzati sul codice	ID	C	Alto
Protezione codice sorgente	T, ID	I, C	Moderato

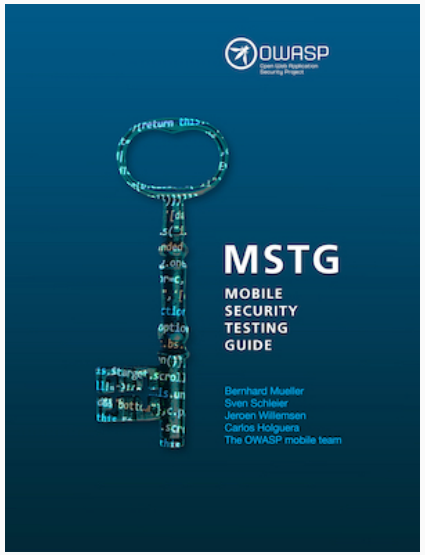
Autenticità (A), Integrità (I), Confidenzialità (C), Non-ripudio (NR), Disponibilità (D) e Autorizzazione (AU), Spoofing (S), Tampering (T), Repudiation (R), Information disclosure (ID), Denial of Service (DoS), Elevation of Privilege (EoP).

Security Testing

È necessario eseguire dei **test** per validare la sicurezza del prodotto finale o intermedio. In questo caso è stato preso come riferimento la guida MSTG redatta da OWASP.

- **Test statico**: analisi del codice, nessuna esecuzione del programma.
- **Test dinamico**: eseguito sul programma in esecuzione.

OWASP
Open Web Application Security Project



Conclusioni

Una volta elaborato un flusso di sviluppo sicuro è opportuno che venga **migliorato** ed **ampliato** nel tempo.

- Sviluppo di nuove funzionalità sempre più sicure
- Adattare il sistema agli standard di sicurezza più recenti
- Definire nuovi modelli di sicurezza.

Conclusioni

Grazie per l'attenzione! :-)