Realizzare un POS avanzato partendo dal progetto di uno smartphone

Christophe Tremlet
Security segment manager
Maxim Integrated Products – France

Come progettare a costi contenuti un terminale POS (Point-of-Sales) sofisticato, sicuro e ricco di funzionalità sfruttando i più recenti sviluppi dell'industria della telefonia cellulare

Complice anche la crescente affermazione degli smartphone, i terminali di pagamento si sono trasformati in dispositivi sofisticati, sempre più ricchi di funzionalità in grado di eseguire transazioni, gestire inventari e far girare applicazioni sia di tipo business sia orientate ai social media. Essi possono anche essere utilizzati per veicolare nuovi servizi e messaggi promozionali delle aziende produttrici e assicurano una migliore fruizione da parte dell'utente. Tra le caratteristiche più avanzate dei terminali di pagamento di fascia alta e dei dispositivi embedded si possono annoverare un touchscreen a colori e un audio di elevata qualità, oltre al supporto di sistemi operativi completi di funzionalità come la piattaforma Android.

Al pari degli smartphone, le apparecchiature per le transazioni finanziarie di tipo elettronico devono disporre di numerose opzioni di connettività (WiFi, GPRS, 3G) ed essere caratterizzate da consumi ridotti. Al crescere della complessità di queste apparecchiature sempre più "smart", corrisponde un aumento – in misura anche superiore – dei costi. Di conseguenza, lo sviluppo di dispositivi così avanzati comporta il coinvolgimento di un gran numero di risorse progettuali e il pagamento di diritti di licenza, con il rischio sempre in agguato di ritardare il time to market.

Anche se l'aumento dei costi di sviluppo è un comune denominatore per le apparecchiature elettroniche sofisticate, que-

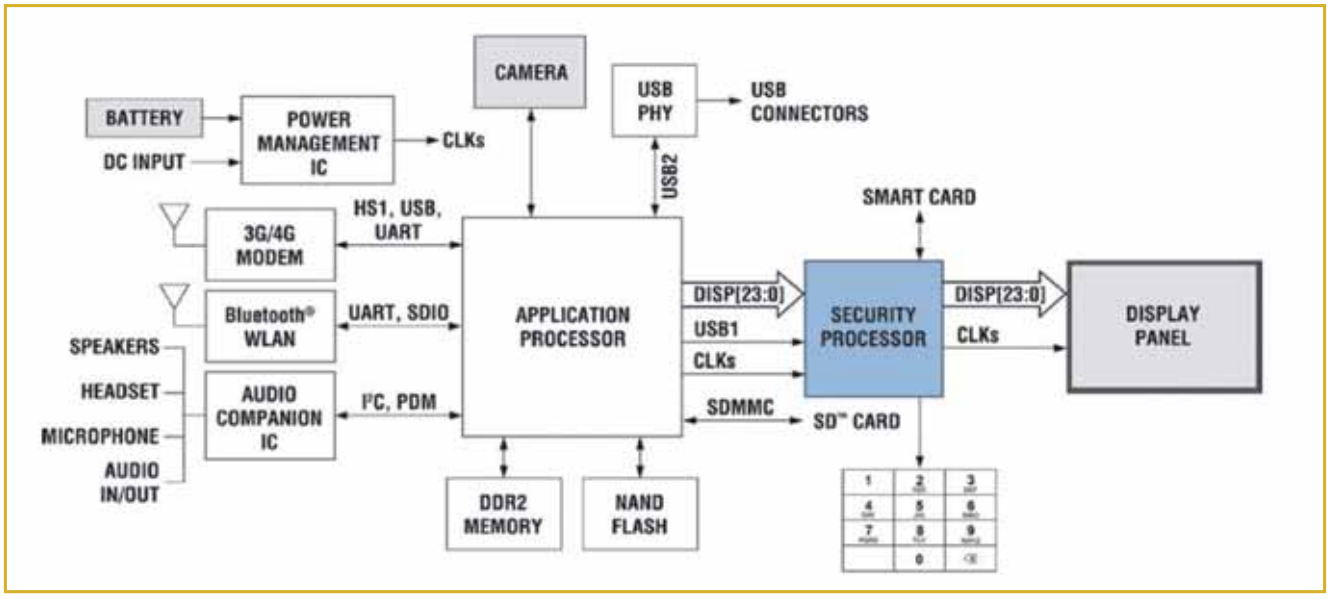

Fig. 1 – Per contrastare in maniera semplice ed economica le minacce alla sicurezza è possibile aggiungere un processore di sicurezza in grado di assumere il controllo del display

sto fenomeno assume un'importanza ancora maggiore per i terminali di pagamento. Ciò è imputabile in larga misura alla differenza dei volumi: i costi di sviluppo di uno smartphone sono ammortizzati in un intervallo di tempo ragionevole grazie al gran numero di unità vendute. Per dare un'idea della differenza, il Nilson Report ha stimato per i terminali di pagamento un volume di unità pari a 15 milioni all'anno, contro i 420 milioni di smartphone venduti nel 2011. Da queste cifre appare chiaro che l'impatto dei costi di sviluppo su ogni dispositivo di transazione finanziaria risulta molto più elevato. Tra gli altri vincoli per apparecchiature di questo tipo si possono segnalare quelli legati alla sicurezza (e alle relative certificazioni) che influenzano sia i costi sia i tempi di sviluppo. L'implementazione delle funzionalità di sicurezza in un terminale POS incide sia sulla componente hardware sia su quella software (in questo contesto il termine hardware si riferisce a tutti i componenti – fino al processore che supporta tutti i meccanismi anti-effrazione).

Ogni nuova famiglia di smartphone prevede l'uso di una nuova generazione di processori applicativi (application processor) – si pensi all'evoluzione dai processori con core ARM11 a quelli con core ARM Cortex-A15 – oppure la migrazione da un processore singolo a uno con doppio core. Oltre ai miglioramenti che riguardano il processore, si potrebbe verificare la sostituzione di un video decoder o un acceleratore grafico. Al fine di semplificare l'adozione di tali migliorie in fase progettuale, l'industria dei semiconduttori continua a sviluppare processori applicativi sempre più potenti per soddisfare le esigenze del mercato. Le dimensioni del mercato dei telefoni cellulari sono infatti tali da giustificare gli enormi investimenti richiesti per lo sviluppo di un nuovo microprocessore di fascia alta. Tali investimenti includono fra gli altri i costi della licenza del core, quelli delle maschere realizzate utilizzando i nodi tecnologici più recenti e lo sviluppo dei blocchi analogici.

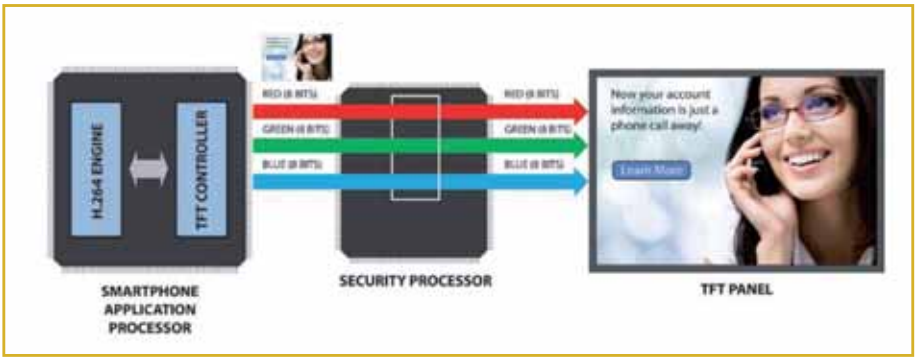

Fig. 2 – In modalità normale il processore di sicurezza agisce alla stregua di un dispositivo pass-through

La situazione attuale

Oggigiorno l'architettura prevalente utilizzata per il progetto di un terminale POS prevede un microcontrollore sicuro (secure microcontroller, ovvero un micro con caratteristiche tali da renderlo sicuro da attacchi finalizzati all'estrazione del codice in esso contenuto effettuati in maniera intrusiva o non intrusiva) su chip singolo. Tali microcontrollori rappresentano il nucleo centrale del terminale di pagamento: essi integrano il core processore, fanno girare il sistema operativo e gestiscono le funzioni di comunicazione e di visualizzazione. Essi supportano inoltre le funzioni di sicurezza più critiche, come il rilevamento di effrazioni, la memorizzazione della chiave di sicurezza con possibilità di distruzione istantanea della chiave stessa e il calcolo crittografico con le associare contromisure. Mentre i vantaggi legati all'abbinamento tra le funzioni generiche di un dispositivo embedded con quelle di sicurezza appaiano ovvii in termini di numero di componenti utilizzati (BOM) e di costi di produzione, questa soluzione potrebbe non risultare la più appropriata per soddisfare i severi requisiti di sviluppo e i vincoli dei dispositivi di fascia alta. Se per una famiglia di cellulari potrebbe aver senso sviluppare un nuovo processore a causa del numero potenzialmente molto elevato di unità vendute, le dimensioni del mercato dei terminali finanziari non sempre giustifica sviluppi di questo tipo. Senza dimenticare che la migrazione di un intero sistema operativo e di una famiglia di applicazioni su un nuovo processore è un'operazione molto complessa. Il software legato alla sicurezza non viene fornito sotto forma di componente standard liberamente disponibile sul mercato e molto spesso è strettamente connesso all'hardware. Esso inoltre deve essere completamente ricertificato, complicando ulteriormente l'operazione di migrazione.

In definitiva, la situazione per gli sviluppatori di terminali di pagamento di fascia alta risulta piuttosto complessa. Essi devono creare un progetto usando i microcontrollori sicuri esistenti (con il rischio di sviluppare un design con una tecnologia che sarà destinata inevitabilmente a diventare ben presto obsoleta) oppure finanziare lo sviluppo di un nuovo microcontrollore (sostenendo gli annessi costi della migrazione software e della certificazione). In quest'ultimo caso la sostenibilità dal punto di vista finanziario può essere dubbia quando si deve progettare un terminale di pagamento di fascia alta che includa numerose caratteristiche ad alto valore aggiunto.

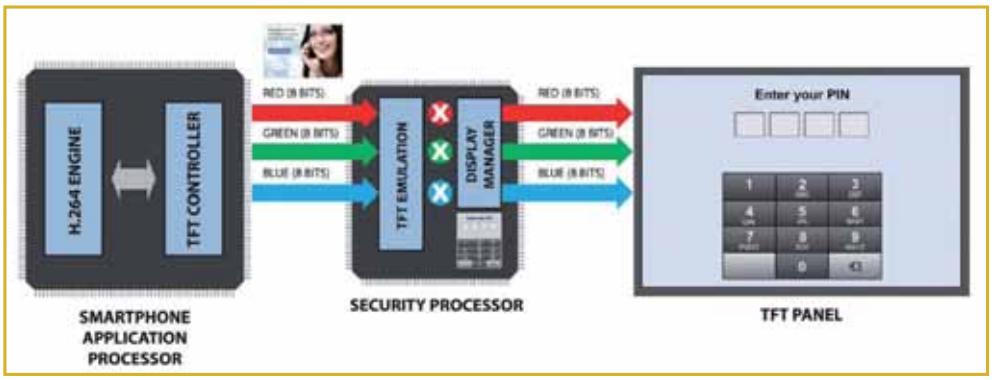

Fig. 3 – In modalità sicura il processore di sicurezza assume il controllo del pannello

Un percorso alternativo

A questo punto è utile chiedersi se esiste un modo per sviluppare un'apparecchiatura POS ricca di funzionalità a costi sostenibili. Ovvero sfruttare gli sforzi fatti dall'industria dei telefoni cellulari riutilizzando la tecnologia hardware e software sviluppata per quel particolare mercato. Fortunatamente la risposta è affermativa. Grazie alla crescita esponenziale del mercato degli smartphone, la varietà di blocchi base che possono essere utilizzati per i terminali di pagamento – sia hardware sia software – è decisamente ampia. I produttori di semiconduttori possono disporre di un'estesa gamma di microcontrollori e SoC (System-on-Chip) che consentono lo sviluppo di un insieme completo di funzionalità per un dispositivo multimediale.

Non solo i microcontrollori sono dotati di un sistema operativo come Android, ma gli sviluppatori possono anche acquistare senza problemi reference design per smartphone. Per un costruttore di terminali POS è naturale sfruttare questi reference design, che supportano tutte le funzioni generiche, e aggiungere le caratteristiche di sicurezza specifiche per i terminali finanziari. L'aggiunta di tali funzioni a un sistema esistente non è un compito banale se non viene attentamente analizzato a livello architetturale. Uno dei problemi principali per aggiungere le funzioni di sicurezza è rappresentato dal display: lo standard PCI PIN Transaction Security (PCI-PTS) richiede il completo controllo del display. In assenza di un controllo di questo tipo, la tipica minaccia alla sicurezza è un'applicazione non sicura o dolosa che richiederà il codice PIN dell'utente.

Questo malware potrebbe visualizzare un falso messaggio del tipo "digitare il vostro codice PIN" per ottenere il PIN dell'utente e inviarlo all'"aggressore" che lo userà per scopi fraudolenti. Per contrastare una minaccia di questo tipo, lo standard PCI_PTS richiede che il firmware sia in grado di impedire il verificarsi di uno scenario del tipo appena descritto. Un requisito di questo tipo non esiste per gli smartphone, ragion per cui l'implementazione di questo controllo può richiedere sostanziali modifiche del sistemi operativo e degli applicativi. Modifiche di questo tipo richiedono uno sforzo progettuale notevole riducendo in larga misura i benefici legati all'uso di un reference design "chiavi in mano".

Processore di sicurezza

Per contrastare questa minaccia, la soluzione proposta da Maxim prevede l'aggiunta di un processore di sicurezza (security processor) in grado di assumere il controllo del display (Fig. 1). Questo processore è collegato all'uscita del bus TFT del processore principale e al bus di ingresso TFT del pannello. Esso ha il completo controllo della tastiera numerica e supporta due modalità di funzionamento: sicura (trusted mode) e normale (normal mode).

Nella modalità normale (Fig. 2), il processore di sicurezza funziona come un semplice dispositivo di collegamento (pass-through). La tastiera è disabilitata e il secondo processore rilascia i dati sul bus TFT dal processore principale che fluiscono verso al pannello TFT. Anche se un'applicazione non autorizzata tenta di visualizzare un falso messaggio per la richiesta del PIN, questa non avrà effetto alcuno perché la tastiera è stata disabilitata. L'applicazione non autorizzata non riceverà quindi alcun tipo di dato dalla tastiera.

In modalità sicura il processore di sicurezza assume il controllo del bus TFT e il pannello visualizzerà solamente immagine autenticate, come la verifica della firma digitale. I dati inviati sul bus TFT dal processore principale non saranno mai visualizzati poiché il bus di ingresso del pannello TFT è fisicamente disconnesso dal bus di uscita TFT del processore principale. In questo modo la tastiera numerica è abilitata in modo che l'utente possa immettere il suo codice PIN quando richiesto (Fig. 3).

L'esistenza di queste due modalità operative rappresenta un notevole beneficio per le funzionalità dell'apparecchiatura. In modalità normale il terminale di pagamento si comporta praticamente alla stessa stregua di uno smartphone. Esso può, per esempio, visualizzare un video utilizzando il suo lettore multimediale originale senza modificare l'hardware o il software del progetto di riferimento dello smartphone. In questa modalità è possibile utilizzare qualsiasi risoluzione, profondità di colore o frequenza d'immagine (frame rate). In modalità sicura, invece, il terminale viene utilizzato per eseguire le transazioni finanziarie standard. Questa funzionalità è completamente integrata nel secondo processore e non richiede alcuna modifica al sistema operativo o alle applicazioni "ereditate" dallo smartphone. Le funzioni di sicurezza vengono aggiunte al sistema dal secondo processore.

Un approccio di questo tipo ha riflessi positivi sulla velocità di evoluzione di una famiglia di terminali POS. Lo sviluppo di una linea di terminali POS con caratteristiche multimediali avanzate richiede l'uso di un nuovo processore multimediale e la migrazione del software su questo nuovo controllore. Se l'apparecchiatura

POS è stata costruita utilizzando un singolo microcontrollore con funzioni di sicurezza integrate, il passaggio alla successiva generazione significa investire nello sviluppo di un nuovo processore e affrontare i costi di una migrazione software e della completa ricertificazione. Nel caso si utilizzi un processore secondario, lo sviluppo risulta notevolmente semplificato. In questo caso è possibile partire dal reference design di uno smartphone che integra le più recenti innovazioni multimediali e aggiungere il processore di sicurezza dotato del medesimo firmware della precedente generazione. Poiché le sicurezza non ha subito modifiche dalla generazione precedente, la certificazione risulta più semplice, rapida ed economica. Grazie a un approccio di questo tipo il prodotto finale disporrà di tutte le più recenti funzioni multimediali che l'utilizzatore si aspetta di trovare.

Una strategia di questo tipo non significa l'abbandono dell'architettura a singolo processore per le apparecchiature POS. L'approccio proposto in questo articolo assicura i migliori vantaggi – in termini di time to market e di costi di sviluppo – per la realizzazione di dispositivi di fascia alta, per i quali i costruttori di POS vogliono seguire le tendenze proprie del mercato degli smartphone, sempre più ricchi di caratteristiche e funzionalità. Per i dispositivi di fascia medio-bassa, per i quali il software è meno complesso (e il numero delle caratteristiche multimediali nettamente inferiore) o per prodotti caratterizzati da un ciclo di vita più breve, l'approccio basato su un singolo processore con funzioni di sicurezza integrate resta ancora valido.

Una vasta offerta

Maxim è un'azienda produttrice di soluzioni per l'industria dei dispositivi di pagamento elettronici riconosciuta a livello internazionale. L'ampia gamma di processori sicuri offerti dalla società consente lo sviluppo di terminali di pagamento a costi contenuti. L'uso dei circuiti integrati sicuri di Maxim permette agli OEM di ridurre il time to market, grazie sia alla disponibilità di un'ampia offerta software sia alle pre-certificazioni. Il microcontrollore sicuro MAX32590 (JIBE) basato su ARM9 integra tutti i meccanismi di sicurezza necessari per ottenere senza problemi la certificazione PCI-PTS 3.1. Per garantire una maggior sicurezza, MAX32590 include blocchi cifrati con contromisure avanzate, meccanismi di rilevamento delle manomissioni e memoria sicura con meccanismi di cancellazione (wipe) avanzati. Poiché l'occupazione di spazio della batteria di backup di MAX32590 è minima, questo processore rappresenta la soluzione ideale per il progetto di apparecchiature POS mobili e portatili. Maxim ha previsto una versione equipaggiata con l'innovativa funzione di controllo sicuro del display descritta in questo articolo. ■