Entrust consente a Xumi di garantire la sicurezza di una nuova tecnologia per i pagamenti su dispositivi mobili

LA SFIDA COMMERCIALE

La tecnologia di comunicazione in prossimità (NFC, Near-Field Communication) permette lo scambio di dati tra due dispositivi vicini e, negli ultimi anni, ha reso possibili i pagamenti in modalità contactless attraverso portafogli mobili e apposite carte.

Agevoli tanto per i clienti quanto per i commercianti, i pagamenti tramite NFC hanno tuttavia aperto la strada a nuove frodi. Secondo la presidente di Xumi Juliana Cafik, la diffusione dei portafogli mobili e dei pagamenti contactless porterà a un aumento delle truffe legate alla tecnologia NFC e, purtroppo, ogni acquisto fraudolento comporta anche la perdita della merce e costose commissioni di riaddebito per i commercianti.

Xumi è un fornitore di servizi di pagamento sicuri il cui obiettivo è bloccare le transazioni ingannevoli prima che avvengano, ovvero prevenirle invece di rilevarle a posteriori. Le soluzioni dell'azienda sfruttano vari livelli di protezione antifrode per aumentare la sicurezza per i titolari delle carte e i commercianti.

Per effettuare pagamenti mediante dispositivi mobili, gli utenti devono dotarsi di un

> **« A livello tecnico, ci siamo posti l'obiettivo di creare un ambiente sicuro sugli smartphone dei clienti, che potesse contenere una carta di credito senza richiedere l'accesso a un ambiente di esecuzione affidabile (TEE, Trusted Execution Environment) né lo sviluppo di nuovi algoritmi o metodologie crittografiche. È qui che sono entrati in gioco gli HSM nShield di Entrust. »**
>
> – Juliana Cafik, Presidente, Xumi

Xumi

portafoglio per contenere le carte di credito, mentre i commercianti devono disporre di un POS che supporti questa modalità di pagamento, oltre alle transazioni via Web e a quelle tradizionali. La tecnologia su cui si fonda il sistema deve essere coerente e, allo stesso tempo, sicura per entrambe le parti.

LA SFIDA TECNICA

"Il settore dei servizi di pagamento non è compatto," ha dichiarato Cafik. "Esiste una divisione sistemica tra i prodotti di consumo, ovvero le carte e gli account, e le applicazioni commerciali, che ricevono le transazioni da parti completamente diverse che si affidano a tecnologie del tutto differenti.

A causa di questa divergenza, non è sempre possibile creare fiducia tra il cliente e il commerciante e questo spiega le numerose frodi. L'unico modo per risolvere questo problema è sviluppare una tecnologia che gestisca la transazione complessiva garantendo alti livelli di sicurezza."

"A livello tecnico, ci siamo posti l'obiettivo di creare un ambiente sicuro sugli smartphone dei clienti, che potesse contenere una carta di credito senza richiedere l'accesso a un ambiente di esecuzione affidabile (TEE, Trusted Execution Environment) né lo sviluppo di nuovi algoritmi o metodologie crittografiche. È qui che sono entrati in gioco gli hardware security module (HSM) nShield® di Entrust," ha spiegato Cafik.

LA SOLUZIONE

Gli HSM nShield Connect di Entrust sono dispositivi hardware affidabili e a prova di manomissione che aumentano l'efficacia dell'elaborazione crittografica generando e proteggendo le chiavi usate per cifrare/decifrare i dati e creare firme e certificati digitali. Gli HSM nShield di Entrust consentono alle imprese di:

- Soddisfare e superare gli standard normativi consolidati ed emergenti relativi alla cybersicurezza
- Raggiungere livelli più elevati di sicurezza e affidabilità dei dati
- Mantenere livelli competitivi di servizio e flessibilità

"Disponiamo di diverse metodologie di protezione, tra cui la cifratura, l'autenticazione, l'offuscamento del codice, la crittografia e altre tecnologie," ha commentato Cafik. "Tuttavia, gli HSM nShield di Entrust ci hanno consentito di sviluppare un'architettura al servizio di clienti e commercianti, che introduce un nuovo standard di sicurezza per i portafogli e i POS mobili senza richiedere l'accesso al TEE degli smartphone."

"La sicurezza del sistema copre l'applicazione mobile e il lato server," ha aggiunto Cafik. "Gli HSM ci aiutano a creare strutture che possono essere utilizzate per verificare l'affidabilità da entrambe le parti, senza dipendere dai dispositivi mobili. Questo risulta particolarmente utile dal lato server, che deve soddisfare tutti i requisiti di sicurezza del Payment Card Industry Data Security Standard (PCI DSS) per la crittografia delle informazioni personali e di pagamento archiviate. Deve inoltre poter configurare le operazioni in un ambiente dalla sicurezza elevata. Gli HSM, che utilizziamo anche per rendere sicura la comunicazione tra il server e il client e per proteggere le informazioni di configurazione, sono essenziali a questo scopo."

Xumi

> **L'aiuto del team di vendita di Entrust si è rivelato inestimabile per la realizzazione di questo progetto. Tutti si sono dimostrati molto competenti e ci hanno guidati passo per passo.**
>
> – Juliana Cafik, Presidente, Xumi

Incluso nel progetto sin dalle prime fasi, l'HSM nShield Connect di Entrust scelto ha introdotto una root of trust essenziale per garantire la sicurezza dell'ambiente operativo.

I RISULTATI

Xumi si sta preparando alla fase di verifica concettuale con l'aiuto dei partner CyberSource e Global Payments. La domanda dell'azienda è già stata certificata come di livello 2 dall'Open Web Application Security Project (OWASP), il cui Application Security Verification Standard (ASVS) offre una base per testare i controlli tecnici di sicurezza delle applicazioni Web e indica agli sviluppatori un elenco di requisiti per lo sviluppo sicuro.[1]

Dopo aver completato questa fase, Xumi intende implementare altri HSM nShield di Entrust in una località di back-up per finalità di disaster recovery, failover a caldo e bilanciamento del carico. L'organizzazione continuerà a lavorare con gli esperti di Entrust per garantire la massima reattività delle transazioni.

Cafik ha osservato: "L'aiuto del team di vendita di Entrust si è rivelato inestimabile per la realizzazione di questo progetto. Tutti si sono dimostrati molto competenti e ci hanno guidati passo per passo. A posteriori mi ritengo molto soddisfatta, perché ci hanno consigliato di usare un algoritmo a curva ellittica, di cui stiamo decisamente vedendo i vantaggi.

Fin dall'inizio, il team di Entrust ci ha offerto il supporto di cui avevamo bisogno e questo è stato un enorme vantaggio per un'azienda piccola come la nostra. I nostri sviluppatori sono straordinari, ma se l'HSM avesse richiesto varie modifiche alla configurazione, il processo si sarebbe rivelato troppo impegnativo per noi.

Il personale di Entrust ha cercato di capire l'uso che avremmo fatto dell'HSM e di prevedere le sfide che avremmo dovuto superare. Non ci hanno fatto perdere tempo e di questo gliene sono molto grata."

Xumi

Obiettivi commerciali

- Sviluppo di una tecnologia di pagamento mobile che soddisfi i requisiti di sicurezza di consumatori e commercianti

Obiettivi tecnici

- Creazione di un'architettura che supporti le transazioni lato cliente e commerciante, senza accedere al TEE del dispositivo mobile
- Sicurezza delle comunicazioni client-server e delle informazioni di configurazione
- Conformità ai requisiti previsti dallo standard PCI DSS per il lato server del commerciante
- Riduzione dei tempi della verifica concettuale
- Creazione di una tecnologia sicura che stabilisca un livello di fiducia tra il dispositivo mobile di un consumatore e l'applicazione di pagamento di un commerciante

La soluzione

- HSM nShield Connect XC
- Assistenza del personale esperto di Entrust

INFORMAZIONI SU ENTRUST

Entrust permette al mondo di continuare ad avanzare in sicurezza attraverso sistemi di identificazione, pagamento e protezione dei dati ad alta affidabilità. Oggi più che mai, le persone si aspettano esperienze sicure e ottimizzate, che si tratti di attraversare le frontiere tra Stati, effettuare un acquisto, accedere ai servizi elettronici della pubblica amministrazione o collegarsi a una rete aziendale. Entrust offre un'ineguagliabile gamma di soluzioni di sicurezza digitale ed emissione di credenziali, il vero fondamento di tutte queste interazioni. Con oltre 2.500 colleghi, una rete di partner globali e clienti in più di 150 Paesi, non sorprende che le organizzazioni più fidate al mondo scelgano noi.

[1] https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

Scopri di più su
entrust.com/HSM

Per contattarci:
HSMinfo@entrust.com