Entrust, Xumi의 새로운 모바일 결제 기술 구축 및 보안 지원

비즈니스적 난관

근거리 무선통신(NFC) 기술을 사용하면 가까운 두 장치가 서로 데이터를 교환할 수 있습니다. 최근 몇 년간 NFC 기술은 모바일 지갑과 비접촉식 카드를 통한 비접촉 결제를 가능하게 했습니다.

NFC 결제는 소비자와 판매자에게 새로운 차원의 편의성을 제공하는 동시에, 새로운 사기 수단으로 활용될 수 있습니다. Xumi의 임원 Juliana Cafik에 따르면 모바일 지갑과 대는 방식의 결제 방식(tap-to-pay)이 주류가 되면서 사기 NFC 결제의 비율이 증가할 것이라고 합니다. 또, 모든 사기 결제 구매는 판매자에게 상품 분실과 값비싼 입금 취소 수수료를 의미합니다.

Xumi는 사기 결제가 일어나기 전에 미리 방지하는 사기 결제 거래 예방을 목표로 하는 보안 결제 제공업체입니다. 이 솔루션은 고유한 사기 방지 계층을 차용하여 카드 소지자와 판매자 양측의 보안을 모두 강화합니다.

> **우리의 기술적 난관은 신뢰 실행 환경(TEE, trusted execution environment)에 액세스하거나 새로운 알고리즘과 암호화 방법을 구축·개발하지 않고도 신용카드를 보관할 수 있도록 소비자의 휴대폰을 안전한 환경으로 만드는 것이었습니다. 여기가 바로 Entrust nShield HSM이 필요한 부분입니다.**
>
> – Xumi 임원, Juliana Cafik

Xumi

모바일 결제에서 소비자는 신용카드를 보관할 지갑이 필요하고 판매자는 웹 거래와 오프라인 거래뿐만 아니라 휴대기기를 위한 판매 시점(point of sale)이 필요합니다. 근본 기술은 양측 모두에게 일관성 있게 적용할 수 있어야 합니다. 또, 양측 모두에게 안전한 기술이어야 합니다.

기술적 난관

Cafik은 "결제 산업은 분열되어 있습니다. "라며 "카드나 계정 유형인 소비자 제품은 판매자 애플리케이션으로부터 체계적으로 분리되어 있습니다. 판매자 애플리케이션은 완전히 다른 기술을 사용하는 완전히 다른 관계자가 프로비저닝한 거래를 전송받습니다.

이러한 분열로 인해 미상의 두 관계자(소비자와 판매자) 간의 신뢰를 구축하는 것은 아예 불가능합니다. 그래서 사기 행위가 상당히 많은 겁니다. 이를 해결하는 유일한 방법은 거래의 양단을 안전하게 처리하는 한 가지 기술을 만드는 것입니다."라고 말했습니다.

Cafik은 이어 "우리의 기술적 난관은 신뢰 실행 환경(TEE, trusted execution environment)에 액세스하거나 새로운 알고리즘과 암호화 방법을 구축·개발하지 않고도 신용카드를 보관할 수 있도록 소비자의 휴대폰을 안전한 환경으로 만드는 것이었습니다. 여기가 바로 Entrust nShield® 하드웨어 보안 모듈(HSM)이 필요한 부분입니다." 라고 말했습니다.

솔루션

nShield Connect HSM은 데이터를 암호화·복호화하고 디지털 서명과 인증서를 생성하는 데 사용되는 키를 생성, 보호하여 암호화 프로세스를 강화하는 강력한 변조 방지 하드웨어 장치입니다. Entrust nShield HSM으로 누릴 수 있는 이점은 다음과 같습니다.

- 기존·신규 사이버 보안 관련 규제를 기준 이상 충족 가능
- 더 높은 수준의 데이터 보안 및 신뢰 확보
- 높은 수준의 서비스와 비즈니스 민첩성 유지

Cafik은 "우리는 암호화, 인증, 코드 난독화, 암호화 등의 기술을 포함한 여러 보안 방법론을 가지고 있습니다."라며, "그러나 Entrust nShield HSM을 사용하면 거래 소비자와 판매자 모두를 위한 아키텍처를 구축할 수 있어 휴대폰의 TEE에 액세스하지 않고도 모바일 지갑과 모바일 POS에 대한 새로운 보안 표준을 만들 수 있습니다."라고 설명했습니다.

이어 "시스템 보안은 모바일 앱과 서버 모두에 적용됩니다. HSM은 양측의 신뢰를 검증할 수 있으며, 소비자 휴대기기에 의존하는 것 없이 사용할 수 있는 구조를 만드는 데 도움이 됩니다. 특히 서버에 유용하죠. 우리의 주요 목표는 결제 사기를 방지하는 것입니다. 따라서, 서버 보안은 저장된 개인 정보와 결제 정보를 암호화하는 과정에서 모든 PCI DSS(Payment Card Industry Data Security Standard) 보안 요건을 충족해야 하며, 고도로 안전한 환경에서 작업을 구성할 수 있어야 합니다. 여기서 HSM이 핵심적인 역할을 담당합니다. 또한, HSM은 서버와 클라이언트 간의 통신을 보호하고 구성 정보를 보호합니다."라고 Cafik은 덧붙였습니다.

Xumi

> **Entrust 영업팀은 이 프로젝트를 구현하는 데 정말 큰 도움이 되었습니다. 풍부한 관련 지식을 바탕으로 모든 과정에서 우리를 잘 안내했습니다.**
>
> – Xumi 임원, Juliana Cafik

Cafik에 따르면 Entrust nShield Connect HSM은 처음부터 설계에 포함된 요소였으며, 신뢰점을 제공하여 전체 작업 환경을 보호하는 핵심 역할을 담당했습니다.

결과

Xumi는 파트너사인 CyberSource 및 Global Payments와 함께 자사의 모바일 결제 애플리케이션으로 상업적 개념 증명(Commercial Proof of Concept)을 준비하고 있습니다. Xumi의 애플리케이션은 이미 OWASP(Open Web Application Security Project, 개방형 웹 애플리케이션 보안 프로젝트) 레벨 2 인증을 받았습니다. OWASP ASVS(Application Security Verification Standard, 애플리케이션 보안 검증 표준) 프로젝트는 웹 애플리케이션 기술 보안 제어를 점검하는 기반이며, 개발자에게는 보안 개발에 필요한 요건을 제공합니다.[1]

Xumi는 개념 증명(PoC)을 완료한 후, 백업 사이트에 추가 Entrust nShield HSM을 배치하여 완전한 재해 복구와 Hot Failover(장애 극복 기능), 로드 밸런싱을 보장할 계획입니다. 또한, 빠른 거래가 가능하도록 Entrust 전문가와 지속적으로 협력하여 최대 수준의 응답성을 제공하고자 합니다.

Cafik은 "Entrust 영업팀은 이 프로젝트를 구현하는 데 정말 큰 도움이 되었습니다. 풍부한 관련 지식을 바탕으로 모든 과정에서 우리를 잘 안내했습니다. 그리고 돌이켜보니, 타원 곡선 알고리즘을 사용하도록 권장해준 것이 얼마나 고마운지 모르겠습니다. 권장에 따른 결과, 이로 인한 진정한 이점을 몸소 체험하고 있습니다.

처음부터 Entrust는 우리에게 필요한 것을 정확히 제공했습니다. 이는 우리와 같은 기업에 굉장한 이점입니다. 작은 기업이니까요. 우리에게는 정말 뛰어난 개발자가 몇몇 있습니다. HSM을 다른 구성으로 여러 번 변경해야 했다면 우리에게는 매우 어려운 일이었을 겁니다.

Entrust는 매우 신중한 태도로 우리가 HSM을 어떻게 이용할 것인지 이해했으며, 문제를 직면하기 전에 앞서 고려했습니다. 우리 시간을 전혀 낭비하지 않았습니다. 정말 고마운 부분이죠."라며 말을 맺었습니다.

Xumi

비즈니스적 요구

- 소비자와 판매자 모두의 보안 요건을 통합하는 모바일 결제 기술

기술적 요구

- 소비자의 휴대기기와 판매자의 결제 애플리케이션 간에 직접적인 신뢰를 가능하게 하는 보안 기술 생성

솔루션

- nShield Connect XC HSM
- Entrust 전문가의 지원

기술적 요구

- 휴대기기의 TEE 액세스 없이 거래 소비자 및 판매자 모두를 위한 아키텍처 생성
- 클라이언트-서버 통신과 구성 정보 보안
- 거래의 판매자 서버에서 PCI DSS 요건 준수
- 상업적 개념 증명에 소요되는 시간 단축

ENTRUST 소개

Entrust는 믿을 수 있는 신원, 결제 및 데이터 보호를 가능케 함으로써 안전한 세상을 유지합니다. 사람들은 국경을 넘고, 구매를 하고, 전자 정부 서비스에 접속하고 기업 네트워크에 로그인하는 것이 원활하고 안전한 경험이기를 오늘날, 그 어느 때보다도 더 요구합니다. Entrust는 이와 같은 모든 상호작용의 핵심에 있는 디지털 보안 및 자격 증명 발급 솔루션에 있어 견줄 데 없는 다양성을 자랑합니다. 2,500 명이 넘는 동료 및 글로벌 파트너로 구성된 네트워크, 그리고 150개국 이상의 고객을 보유한 당사는 세계에서 가장 신뢰 받는 기관들의 신뢰를 받고 있습니다.

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

에서 자세히 보기
entrust.com/HSM

ENTRUST

연락처:
HSMinfo@entrust.com