SISA

Customer Success Story

How SISA Helped a Leading Hospitality Platform Provider Strengthen Data Confidentiality Through Application Encryption Hardening

About The Customer

The customer is Southeast Asia's largest and fastest-growing technology-driven hospitality platform, focused on transforming the travel and accommodation landscape. Headquartered in the region, the customer specializes in converting fragmented supply inventories into standardized, branded accommodations using scalable and innovative SaaS-based solutions. With operations across major cities and tourist destinations, the platform enables users to access affordable and reliable stays while empowering hospitality partners to streamline their operations.

Business Challenge

The organization relied on client-side encryption to secure sensitive user data in its web and mobile applications. However, the encryption logic, including the AES key and IV, was hardcoded into the client-side code, making it vulnerable to reverse engineering. Attackers could extract these cryptographic elements using static and dynamic analysis tools, enabling them to decrypt user data, bypass encryption, and manipulate payloads. The absence of server-side validation further compounded the risk, allowing malicious data to be accepted without verification.

As the platform scaled across cities and partner networks, its applications became central to customer engagement, bookings, and payment flows. The customer needed independent assurance that the cryptographic controls it depended on were genuinely protecting user data - and not creating a false sense of security that an attacker could quietly defeat.

Solution Offered by SISA

SISA conducted a focused application security assessment of the customer's web and mobile applications to determine how effectively client-side encryption was protecting sensitive user data, and whether the underlying cryptographic implementation could be abused. The assessment followed a structured, phased methodology - combining AI-assisted analysis with manual, attacker-led testing - to identify, validate, and help remediate the encryption weaknesses at their root cause rather than at the surface.

SISA's 5-Phase Application Security Assessment

Phase 1

Application Discovery and Scoping

SISA began by mapping the customer's web and mobile applications, their data flows, and the exact points at which sensitive data was encrypted and decrypted on the client. This included understanding how the AES-based encryption routine was invoked, where cryptographic material resided, and which API calls carried encrypted payloads.

Phase 2

Threat Modeling and Attack Surface Mapping

The team then assessed the application from an attacker's perspective. Because encryption and decryption executed entirely on the client, SISA prioritized the risks that flow from that design decision: extraction of hardcoded keys, decryption of intercepted data, tampering with encrypted requests, and the absence of server-side validation as a broken trust boundary.

Phase 3

Security Testing and Exploitation

SISA combined static and dynamic analysis across the client-side code of both the web and mobile applications. Through static decompilation and inspection of the client bundle and mobile binaries, the team recovered the hardcoded AES key and IV embedded directly in the code. Using dynamic analysis and runtime instrumentation - including hooking of cryptographic functions and interception of application traffic - SISA observed the encryption and decryption operations in real time, decrypted sensitive user data in transit, and reconstructed the complete cryptographic scheme used by the application.

Phase 4

Validation and Impact Analysis

SISA validated the full attack path end to end. Using the recovered key and IV, the team decrypted confidential user data and then forged and modified encrypted payloads. Because the backend performed no independent validation of incoming data, these manipulated payloads were accepted and processed - confirming that the client-side encryption offered no real security guarantee and could be bypassed entirely.

Phase 5

Reporting and Remediation Guidance

SISA delivered evidence-backed findings, proof of exploitation, and a prioritized, risk-based remediation roadmap, along with a walkthrough to ensure the development team fully understood both the risk and the fix.

SISA's 6-Point Remediation Guidance

01

Shift encryption to the backend: Perform all encryption and decryption of sensitive data within a controlled server environment, rather than in code the user can inspect and manipulate.

02

Implement secure, centralized key management: Manage cryptographic keys through a dedicated Key Management System (KMS) or secrets vault, eliminating hardcoded keys and IVs from client-side code.

03

Enforce server-side validation: Refactor the application so the backend independently validates all incoming data and never trusts client-supplied or client-encrypted payloads without verification.

04

Harden the client applications: Add code obfuscation and anti-tampering controls to the web and mobile apps to raise the cost and difficulty of reverse engineering.

05

Adopt end-to-end encryption best practices: Use authenticated encryption, per-session random IVs, and proper key rotation in place of static cryptographic material.

06

Monitor for anomalous activity: Feed application and API telemetry into SIEM and detection tooling to surface repeated decryption failures, tampering attempts, and other signs of abuse.

Business Impact

The assessment gave the customer clear, evidence-based visibility into a critical flaw that had, until then, been masked by the assumption that client-side encryption was protecting user data. Left unaddressed, the weakness could have allowed attackers to reverse engineer the applications, recover the encryption keys, and decrypt or manipulate sensitive user data at scale - exposing the business to data breaches, fraud, identity theft, and regulatory non-compliance. By validating the full attack path and guiding remediation, SISA helped the customer convert a hidden, systemic risk into a hardened, defensible encryption architecture.

Key benefits included:

Eliminated a critical data-exposure path

Moving cryptographic operations server-side and removing hardcoded keys closed the route by which an attacker could decrypt or forge sensitive user data.

Restored genuine confidentiality and integrity of user data

Server-side encryption, secure key management, and server-side validation ensured that sensitive data could no longer be decrypted or tampered with simply by manipulating the client.

Strengthened regulatory alignment

The remediation brought the customer's data-protection practices closer to the expectations of standards such as PCI DSS, GDPR, and HIPAA, reducing exposure to penalties and breach-notification obligations.

Clear visibility into exploitable risk

By demonstrating the end-to-end attack path rather than reporting a theoretical flaw, SISA gave engineering leadership an unambiguous, prioritized basis for action.

A more resilient, defensible architecture

Obfuscation, anti-tampering, authenticated encryption, and SIEM-based monitoring gave the customer layered protection and ongoing detection against future reverse-engineering attempts.

Conclusion

Through this application security assessment, SISA helped the customer move beyond surface-level vulnerability identification to root-cause validation and practical, architecture-level remediation. What began as a convenient client-side encryption scheme was shown to be fundamentally bypassable; by relocating trust to a secure backend, enforcing rigorous key management and server-side validation, and adding tamper resistance and monitoring, the customer significantly strengthened the confidentiality and integrity of its users' data. As a result, the platform is now better positioned to protect sensitive information, meet its regulatory obligations, and sustain the trust of the users and hospitality partners that depend on it.