sysmosoft

Sysmosoft SENSE Addresses OWASP’s Top Mobile Risks and Vulnerabilities

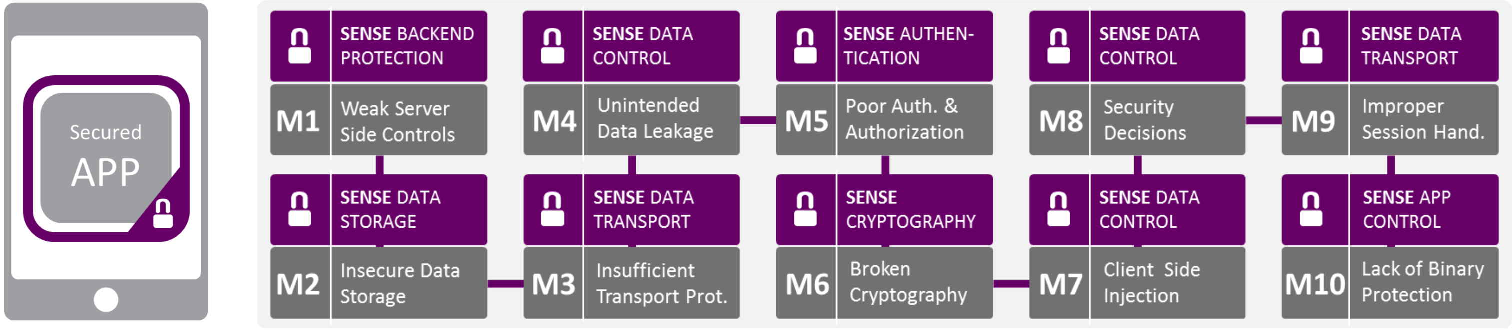
This document presents Sysmosoft SENSE’s security countermeasures against key mobile risks and vulnerabilities. SENSE enables organizations to meet the highest of security standards.

OWASP Mobile App Security Risks

The Open Web Application Security Project (OWASP) defined a list of key security risks frequently found in mobile applications and corporate back-end services. A single vulnerability in mobile Apps can lead to data loss and damage a company’s brand and reputation. Organizations looking to release business critical mobile services should implement security measures to mitigate these risks in accordance with their confidentiality requirements.

Sysmosoft SENSE Mobile App Risk Mitigation

SENSE is mobile App security solution that enables organizations to implement state-of-the-art security requirements when building and delivering business critical mobile Apps. SENSE addresses security risks without requiring complex integration or specialized knowledge and skills. Sysmosoft leverages OWASP resources, including threat modelling, code quality and security testing, to deliver advanced security countermeasures.



Secured APP

SENSE BACKEND PROTECTION
M1 Weak Server Side Controls

SENSE DATA STORAGE
M2 Insecure Data Storage

SENSE DATA TRANSPORT
M3 Insufficient Transport Prot.

SENSE DATA CONTROL
M4 Unintended Data Leakage

SENSE AUTHENTICATION
M5 Poor Auth. & Authorization

SENSE CRYPTOGRAPHY
M6 Broken Cryptography

SENSE DATA CONTROL
M7 Client Side Injection

SENSE DATA CONTROL
M8 Security Decisions

SENSE DATA TRANSPORT
M9 Improper Session Hand.

SENSE APP CONTROL
M10 Lack of Binary Protection

About OWASP

The Open Web Application Security Project (OWASP) is an open source community dedicated to helping organizations conceive, develop, acquire, operate and maintain trusted Apps.

OWASP Mobile Security Project: Top 10 Mobile Risks

The OWASP Mobile Security Project is a centralized resource intended to give developers and security teams the resources they need to build and maintain secure mobile Apps.

The goal of the project is to classify mobile security risks and provide development controls to reduce the impact or likelihood of exploitation.

For more information about OWASP mobile security project and top 10 mobile risks : https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

Vulnerability	Description	How SENSE Prevents an Exploit	Relevant SENSE Features
M1 **Weak Server Side Controls**	Mobile Apps are connected to the backend infrastructure of an organization, which is then connected to sensitive business information. Due to pressures on fast deployment time, backend services are rarely designed with security in mind. A vulnerable backend that is exposed to the internet can lead to a data breach with a material impact on the organization.	SENSE is composed of an optional proxy that can be managed and deployed within the organization's infrastructure. SENSE's proxy is a hardened single entry point for mobile requests running in front of sensitive backend application services. SENSE filters, validates, authenticates and authorizes each request at the application level. As a result, only trusted requests reach the company backend.	✓ Single entry point (HTTPS Secure cypher suites) ✓ Hardened SENSE proxy server ✓ App-Level authenticated encryption ✓ App-level authorization and authentication ✓ Centralized security management
M2 **Insecure Data Storage**	Mobile Apps can store highly confidential information including client data, sales forecasts or intellectual property at rest on the mobile device. Mobile Apps typically delegate data protection to the device and are therefore subject to device-specific vulnerabilities and weaknesses. Without additional protection measures, malwares, malicious third-party apps, hackers and other threats can exploit a device vulnerability to steal confidential or sensitive information.	SENSE automatically encrypts data stored at rest by the App plus a dedicated app-level authenticated encryption (AES-GCM). This ensures data remains protected even if the device is vulnerable or not controlled by the organization. SENSE encryption leverages specific keys to fulfil security requirements. These keys include remote keys generated and stored server-side and temporary keys used for single transaction or traditional local keys derived from user's password.	✓ App-level data and database encryption ✓ File names anonymization ✓ Encryption key management ✓ Remote server secure key store ✓ Local secure key store ✓ Data and key wipe
M3 **Insufficient Transport Layer Protection**	Mobile Apps are connected to corporate backend services to retrieve sensitive information. Without sufficient protection for data-in-transit, attackers with access to the network (public Wi-Fi) can intercept traffic and exploit vulnerabilities to steal data or user credentials exchanged between the App and the corporate server.	SENSE encrypts network traffic between the mobile App and the company's backend infrastructure. SENSE uses standard TLS protocol provided by the device associated with a dedicated app level network encryption layer. This leverages best security practices including mutual authentication (soft token), perfect-forward-secrecy (Ephemeral Diffie-Hellman Key Exchange) and Authenticated-Encryption (AES-GCM).	✓ App-level data-in-transit encryption ✓ Ephemeral key exchange ✓ Perfect forward secrecy ✓ Mutual transport layer authentication ✓ Certificate control

Vulnerability	Description	How SENSE Prevents an Exploit	Relevant SENSE Feature
M4 **Unintended Data Leakage**	Mobile devices implement data caching mechanisms to enhance the user experience. Information from the keyboard, pasteboard, browser and HTML pages are automatic cached at-rest on the device, in the cloud or within the personal computer by the operating system. Without sufficient security measures, App data is at risk within these external insecure area.	SENSE prevents mobile Apps from leaking sensitive information from unsecure device caches, including the keyboard, browser and HTML caches, as well as log files and the pasteboard. In addition to data leakage prevention capabilities, SENSE's dedicated encryption ensures data remains inaccessible in the long-term to malicious entities even if it's copied to an external unsecure source.	✓ Data leakage prevention ✓ Hardened HTML5 web browser ✓ App backgrounding detection ✓ App HTML caching prevention ✓ App logs control ✓ Data encryption using dedicated keys
M5 **Poor Authorization and Authentication**	Mobile Apps authenticate end-users prior to allowing access to local data stored or remote services provided by the organization. Authentication is the root element of security and should be handled carefully by Apps that have access to sensitive information. Without sufficient authentication processes, data can be compromised in numerous ways, such as an authentication bypass, by passcode brute-force and the elevation of privilege.	SENSE uses dedicated two-factor authentication mechanisms to ensure that only authorized users and authorized Apps can access confidential information. SENSE uses a cryptographic key protected with a cryptographic camouflage technique that verifies the identity of the App and users through password or an external hardware token against the company's authentication backend. SENSE can also authorize access based on the user's geolocation.	✓ Secure App activation with a unique key ✓ User local authentication ✓ Remote server two-factor authentication ✓ Optional remote token authentication ✓ Geo-located data access rights ✓ User access rights
M6 **Broken Cryptography**	Mobile Apps may use weak cryptography algorithms (MD5, DES, …) that incorrectly use cryptography functions API (weak random, static IV, ...) or implement a flawed process or algorithm (key generation, random numbers generation, ...) which leads to data loss.	SENSE uses a dedicated cryptography library with state-of-the-art encryption algorithms and dedicated keys to protected sensitive data without reliance on the underlying cryptography capabilities of the device. SENSE algorithms have undergone several audits by banks to ensure that they meet the highest security standards.	✓ State-of-the-art cryptography ✓ Audited security ✓ FIPS test vectors ✓ App-level cryptography library

Vulnerability	Description	How SENSE Prevents an Exploit	Relevant SENSE Feature
M7 **Client Side Injection**	Client side injection may occur when mobile Apps don't control input, which is instead provided by end-users or other sources. As a result the App or the underlying components such as databases may execute malicious code, leading to a data leak.	SENSE enables Apps to validate inputs provided by end-users and perform automatic validation of HTTP traffic to ensure remote services are not providing malicious code. SENSE attributes each user's unique keys which ensures data devices remains segregated.	✓ User input validation ✓ Data validation ✓ HTML/CSS validation ✓ Message authentication
M8 **Security Decisions via Untrusted Inputs**	Mobile Apps read and share data across different channels (inter-application services, app storage, app public folders, keychains, remote servers, cloud services, ...), which may be susceptible to surveillance or tampering. Mobile Apps that fail to perform security checks on data from an external source can undermine the entire system and result in a data leak.	SENSE ensures Apps only receive data from authorized and authenticated sources. Messages sent are authenticated using strong cryptographic algorithms (HMAC or GMAC) to avoid tampering by an attacker. Using its dedicated application level encryption layer, SENSE removes the dependency on the operating system's mechanisms that are susceptible to being monitored or tampered with.	✓ Data authentication ✓ Data source verification ✓ Message authentication ✓ Separate keyboard cache ✓ Remote services access control list
M9 **Improper Session Handling**	Once authenticated and connected to a corporate backend, mobile Apps have to be capable of handling a communication session while preventing attackers from stealing data. Improper Session Handling typically occurs when developers fail to implement best practices within the corporate backend or on mobile Apps.	SENSE session handling is part of the SENSE Secure Transport capability and leverages best practices. SENSE session is generated at the application level and uses a session identifier with strong entropy. Each session is unique and associated with unique encryption and authentication keys generated during the authenticated key exchange. Session timeouts can be defined directly within the SENSE configuration.	✓ Secure session establishment ✓ Strong unique session ID ✓ Session timeout management

Vulnerability	Description	How SENSE Prevents an Exploit	Relevant SENSE Feature
M10 Lack of Binary Protection	Mobile Apps are deployed outside of the organization in an uncontrolled environment. Attackers can easily gain access to an App and reverse engineer it, bypassing or modifying security mechanisms to execute malicious code. Mobile Apps usually fail to prevent reverse engineering and tampering, which leads to compromised information or identity theft.	SENSE implements security mechanisms that prevent attackers from tampering with Apps. SENSE performs automatic cryptography checksum of mobile Apps at runtime combined with advanced jailbreak/root detection and debugging detection (C++) to prevent the attacker from bypassing security methods. According to industry best practices, SENSE security algorithms establish keys in an unique manner for each instance of the App.	✓ App integrity control ✓ App anti-hacking detection ✓ Jailbreak detection ✓ Debugger detection controls

Planning to release new business critical mobile Apps ?

Contact us

Who we are

Sysmosoft SA is a Swiss company founded in 2010 with the conviction that mobile technologies would fundamentally change the way organization do business.

Sysmosoft's mission is to enable organizations to easily release business critical mobile Apps that have to meet strong security and compliance requirements.

Sysmosoft SENSE is an audited secure mobile technology, built by Sysmosoft, that strengthens mobile Apps with unique security capabilities without requiring specialized integration, skills or knowledge from the organization.

Sysmosoft is a proven solution with several enterprise customers in the finance and public sector that have released business critical Apps to business units for internal use and to customers in a safe and compliant manner.

Contact

Sysmosoft SA
Rue Galilée 6
1400 Yverdon-les-Bains
Phone : +41 24 524 10 36
Email : info@sysmosoft.com