SAML Security Cheat Sheet

Introduction

The OWASP SAML Security Cheat Sheet lists several recommendations related to the Web Browser SAML/SSO Profile with Redirect/POST bindings.

This document responds to those recommendations in the context of the ComponentSpace SAML products.

Validate Message Confidentiality and Integrity

HTTPS using TLS 1.2 is the recommended transport. TLS 1.2 support is provided at the operating system level.

Encrypting/decrypting SAML assertions is supported and recommended in sensitive environments or where the SAML assertions includes sensitive user information.

Validate Protocol Usage

- **AuthnRequest(ID, SP):** Generated SAML authn requests include a unique ID and an issuer field that identifies the service provider. The SAML response is checked to ensure it includes an InResponseTo field that ties it to the authn request.

- **AuthAssert(ID, C, IdP, SP):** The SAML response is checked to ensure it contains a single SAML assertion only. The SAML assertion ID is checked to prevent replay attacks. The SAML assertion issuer and SubjectConfirmationData's Recipient are checked to confirm the sender and intended recipient.

Validate Signatures

Schema Validation

SAML messages and assertions are validated against local copies of the XML schema.

Automatic downloading of schemas from third party locations is not supported.

The XML schemas are those included in the SAML specification and related specifications.

Signature Validation

KeyInfo elements are ignored. The public key/ X.509 certificate used to validate signatures is obtained directly from the partner provider and stored locally.

Signature Wrapping Attacks

The SAML products are not vulnerable to XML Signature Wrapping attacks.

Validate Protocol Processing Rules

The processing rules defined in section 3.4.1.4 of the SAML Core specification and section 4.1.4.3 of the SAML Profiles specification are implemented.

Validate Binding Implementation

The processing rules for HTTP Redirect and HTTP Post bindings defined in the SAML Binding specification are implemented.

Validate Security Countermeasures

Countermeasures are in place for the various threats identified by the SAML Security specification.

IP filtering is not included by the SAML products but may be implemented at the application level, if required.

SAML responses have configurable lifetimes defaulting to three minutes.

SAML responses are only used once.

Unsolicited Response (ie. IdP Initiated SSO) Considerations for Service Providers

The processing rules defined in section 4.1.5 of the SAML profiles specification are implemented.

Relay state is passed to the application which is responsible for ensuring it's an acceptable URL.

Checks are in place to prevent replay attacks.

Identity Provider and Service Provider Considerations

Identity Provider (IdP) Considerations

- The application is responsible for any validation of X.509 certificates for algorithm compatibility, strength of encryption, export restrictions.

- The SAML products default to "http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p" and "http://www.w3.org/2001/04/xmlenc#aes256-cbc" respectively for the key and data encryption algorithms. Other encryption algorithms are available.

- SAML response and assertions are only accepted after having been confirmed to have come from an authorized identity provider.

- Both CA issued and self-signed X.509 certificates are supported. The SAML products don't impose any restrictions.

- It's recommended that the server clock is synchronized to a standard time source. Typically, this is done at the operating system level.

- The application is responsible for defining the levels of assurance for identity verification. The SAML products don't impose any restrictions.

- The application is responsible for the user identity information included in the SAML assertion. The SAML products don't impose any restrictions.

- SAML responses and/or SAML assertions may be signed.

Service Provider (SP) Considerations

- The application is responsible for user session state. The SAML products don't impose any restrictions.
- The application is responsible for the level of granularity in setting authorization context. The SAML products don't impose any restrictions.
- The SAML products ensure either the SAML responses and/or SAML assertions are signed.
- SAML message and/or SAML assertion signatures are verified.
- Signatures are verified using the public keys/X.509 certificates of authorized IdPs only.
- X.509 certificates may be validated. The degree of validation is configurable.
- SAML assertions outside the NotBefore/NotOnorAfter period are rejected.
- SAML assertions with an unexpected recipient field are rejected.
- SAML logout is supported.
- It's recommended that SAML assertions are exchanged over HTTPS using TLS 1.2.
- The application is responsible for defining session management criteria. The SAML products don't impose any restrictions.
- The application is responsible for verifying user identities obtained from SAML assertions. The SAML products don't impose any restrictions.

Input Validation

The application is responsible for any input validation. The SAML products don't directly accept user input.

Cryptography

Strong encryption (including 256-bit AES-CBC and AES-GCM) is supported.

Insecure encryption algorithms are supported for backward compatibility with third party products, but their use is not recommended.