SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107
Accredited by NAAC-UGC with ‘A’ Grade
Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

Department of Information Technology

Topic 9 – Security Standards

Security Standards

- Security standards define the processes, procedures, and practices necessary for implementing a security program

- Security standards are based on a set of key principles intended to protect this type of trusted environment.

Security Standards

- SAML
- OAuth,
- OpenID,
- SSL/TLS)

Security Standards

Security Assertion Markup Language (SAML)
SAML is an XML-based standard for communicating

- authentication,
- authorization, and
- attribute information

Used to securely send assertions between partner organizations regarding the identity

- The Organization for the Advancement of Structured Information Standards (OASIS) is responsible for defining, enhancing, and maintaining the SAML specifications.

SAML is built on

- SOAP,
- HTTP, and
- XML

Security Standards

- SAML relies on HTTP as its communications protocol and specifies the use of SOAP (currently, version 1.1).

- Most SAML transactions are expressed in a standardized form of XML.

- SAML assertions and protocols are specified using XML schema.

- Both SAML 1.1 and SAML 2.0 use digital signatures (based on the XML Signature standard) for authentication and message integrity.

- XML encryption is supported in SAML 2.0, though SAML 1.1 does not have encryption capabilities.

- SAML protocol refers to what is transmitted, not how it is transmitted.

- SAML protocol is a simple request–response protocol. The most important type of SAML protocol request is a query.

- A service provider makes a query directly to an identity provider over a secure back channel.

Security Standards

- SAML assertions are usually transferred from identity providers to service providers
- Assertions contain statements that service providers use to make access control decisions
- Three types of statements are provided by SAML: authentication statements, attribute statements, and authorization decision statements

```
<saml:Assertion A...>
<Authentication>
...
</Authentication>
<Attribute>
...
</Attribute>
<Authorization>
...
</Authorization>
</saml:Assertion A>
```

The assertion shown above is interpreted as follows:
Assertion A, issued at time T by issuer I, regarding subject S, provided conditions C are valid.

Security Standards

Open Authentication (OAuth)

- OAuth is an open protocol, initiated by Blaine Cook and Chris Messina, to allow secure API authorization in a simple, standardized method for various types of web applications.
- OAuth is a method for publishing and interacting with protected data.
- For developers, OAuth provides users access to their data while protecting account credentials.
- OAuth allows users to grant access to their information, which is shared by the service provider and consumers without sharing all of their identity.
- With Oauth, sites use tokens coupled with shared secrets to access resources. Secrets, just like passwords, must be protected.
- It is used to establish a mechanism forexchanging a user name and password for a token with defined rights and to provide tools to protect the token.

Security Standards

Open Authentication (OAuth)

- OAuth is an open protocol, initiated by Blaine Cook and Chris Messina, to allow secure API authorization in a simple, standardized method for various types of web applications.
- OAuth is a method for publishing and interacting with protected data.
- For developers, OAuth provides users access to their data while protecting account credentials.
- OAuth allows users to grant access to their information, which is shared by the service provider and consumers without sharing all of their identity.
- With Oauth, sites use tokens coupled with shared secrets to access resources. Secrets, just like passwords, must be protected.
- It is used to establish a mechanism for exchanging a user name and password for a token with defined rights and to provide tools to protect the token.

Security Standards

OpenID

- OpenID is an open, decentralized standard for user authentication and access control that allows users to log onto many services using the same digital identity.

- It is a single-sign-on (SSO) method of access control.

- It replaces the common log-in process (i.e., a log-in name and a password) by allowing users to log in once and gain access to resources across participating systems.

- An OpenID is in the form of a unique URL and is authenticated by the entity hosting the OpenID URL.

- The OpenID protocol does not rely on a central authority to authenticate a user's identity.

Security Standards

SSL/TLS

- Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographically secure protocols designed to provide security and data integrity for communications over TCP/IP.

- TLS and SSL encrypt the segments of network connections at the transport layer.

- The TLS protocol allows client/server applications to communicate across a network in a way specifically designed to prevent eavesdropping, tampering, and message forgery.

- TLS provides endpoint authentication and data confidentiality by using cryptography.

- TLS authentication is oneway the server is authenticated, because the client already knows the server’s identity.

Security Standards

SSL/TLS

- Validation does not identify the server to the end user.

- TLS also supports a more secure bilateral connection mode whereby both ends of the connection can be assured that they are communicating with whom they believe they are connected.

- This is known as mutual authentication

- Mutual authentication requires the TLS clientside to also maintain a certificate.

TLS involves three basic phases:
1. Peer negotiation for algorithm support
2. Key exchange and authentication
3. Symmetric cipher encryption and message authentication (assured) authentication.

THANK YOU