CLOUD COMPUTING

List out and explain various Identity Protocols

Submitted By: Harikrishnan R
Roll No: 26
Submitted To: Rini Kurian

Identity and access management (IAM) protocols.

A core, foundational element to understand with identity and access management (IAM) solutions is protocols.

Identity solutions often depend on industry-standard authentication protocols. Unfortunately, different types of IT resources generally support different authentication protocols.

Organizations have a mixture of all of these types of resources, but their identity and access management solutions may only support only one or a couple of these authentication protocols. That causes IT organizations to build a collection of solutions that ultimately comprise their entire IAM infrastructure.

The best approach is to determine which authentication protocols are in use (or should be), find an identity management solution that supports those protocols, and then employ one single IAM solution that doesn't have to be modified just to reach bare minimum functionality.

An authentication protocol is a type of computer communications protocol or cryptographic protocol specifically designed for transfer of authentication data between two entities. It allows the receiving entity to authenticate the connecting entity (e.g. Client connecting to a Server) as well as authenticate itself to the connecting entity (Server to a client) by declaring the type of information needed for authentication as well as syntax.[1] It is the most important layer of protection needed for secure communication within computer networks.

Purpose

With the increasing amount of trustworthy information being accessible over the network, the need for keeping unauthorized persons from access to this data emerged. Stealing someone's identity is easy in the computing world - special verification methods had to be invented to find out whether the person/computer requesting data is really who he says he is.[2] The task of the authentication protocol is to specify the exact series of steps needed for execution of the authentication. It has to comply with the main protocol principles:

A Protocol has to involve two or more parties and everyone involved in the protocol must know the protocol in advance.

All the included parties have to follow the protocol.

- A protocol has to be unambiguous - each step must be defined precisely.
- A protocol must be complete - must include a specified action for every possible situation.

Types of Protocols are:

1. Authentication protocols developed for PPP Point-to-Point Protocol
   Protocols are used mainly by Point-to-Point Protocol (PPP) servers to validate the identity of remote clients before granting them access to server data. Most of them use a password as the cornerstone

of the authentication. In most cases, the password has to be shared between the communicating entities in advance.

2. AAA architecture protocols (Authentication, Authorization, Accounting)
   Complex protocols used in larger networks for verifying the user (Authentication), controlling access to server data (Authorization) and monitoring network resources and information needed for billing of services (Accounting).

**Various AAA protocols are:

a. Native Authentication

Okay, so native authentication isn't exactly a protocol. In fact, it's just the opposite.

We include it on this list to emphasize the point that most devices have their own authentication mechanisms. While some devices can access LDAP, for example, the challenges to connect those devices to LDAP are significant.

Specifically, Windows® and macOS devices are challenging to manage with third party protocols. As a result, while there may not be a specific protocol, the APIs to create and manage users on Windows, Mac, and Linux® devices are critical for any identity management solution.

b. LDAP

One of the oldest and most durable authentication protocols, LDAP has been an industry standard since the mid-1990s. Lightweight Directory Access Protocol is often used for connecting to Linux devices, NAS devices / file servers, and more technical applications, as in DevOps environments. Many on-premises applications and storage devices still authenticate to the LDAP protocol.

LDAP is flexible and customizable, which is powerful, but it is notoriously difficult to configure and administer. In recent years, LDAP-as-a-Service solutions emerged to streamline LDAP's capabilities for organizations.

Use LDAP for: Linux devices, NAS devices/file servers, technical applications, on-perm applications.

c. Kerberos

Invented at MIT, Kerberos is used extensively under the hood by Microsoft as the authentication protocol for Windows and Windows-related systems.

The primary benefit in Windows networks is the ability to automatically sign-in users to any resources connected to the domain. With the steady move to SaaS-based applications, Kerberos has become a less important authentication protocol, but it is still used widely by Microsoft for their on-perm domain controller. Also, it's important to note that, with the changing IT landscape, many organizations have shifted away from an on-perm domain to the domain less enterprise architecture, relegating Kerberos to be somewhat less relevant than it was a decade or so ago.

Use Kerberos for: Windows systems, on-prem Microsoft applications / server infrastructure

d. RADIUS

Remote Authentication Dial-In User Service (RADIUS) is an authentication protocol primarily used by networking solutions such as wireless networks, VPNs, and network infrastructure equipment. RADIUS servers generally connect back to a central directory service which contains user credentials. RADIUS was primarily used by ISPs and the like early on, but has since been repurposed to control Wi-Fi networks and VPNs.

As with LDAP, there are options for companies that would rather not deal with their own RADIUS servers. RADIUS-as-a-Service (RaaS) provides you with pre-built, pre-configured, scalable, redundant, and fully managed and maintained RADIUS servers.

Use RADIUS for: wireless networks, VPNs, network infrastructure equipment.

e. SAML

Security Assertion Mark-up Language (SAML) is the authentication protocol most often associated with single sign-on solutions for web applications. The open standard is employed widely by service providers (web application providers) and identity providers (web application SSO solutions).

SAML implementations are defined by an identity provider and a service provider. A service provider is, for example, a web application that a user wants to access. The service provider will request authentication from an identity provider, which is ultimately backed by a directory service. Historically, identity providers were merely proxies for the core directory service, but with platforms such as Directory-as-a-Service, those functions (IDP & SSO) are merging.

SAML has made great inroads into the web application sector, but is generally not relevant for devices and generally not used by internal applications due to the overhead to adopt it.

Use SAML for: web applications.

f. OpenID

Another authentication mechanism for web applications, OpenID has gained some adoption due to support from significant consumer facing web applications such as Google® and Yahoo! OpenID works similar to SAML but is less complex to implement. Using OpenID, a third party web application could allow users to log in to their services via a Google, Microsoft, Facebook, Twitter, or Yahoo ID, for example.

This authentication mechanism is used for consumer facing web applications, although it is starting to gain some traction in business scenarios due to the popularity of G Suite™ (formerly Google Apps for Work).

Use OpenID for: web applications.

g. OAuth

A similar protocol to OpenID, OAuth is used by major consumer Internet sites such as Google, Facebook, and Twitter to federate their identities to third party sites.

Use OAuth for: web applications.

h. TACACS

Adopted extensively in the network infrastructure market, TACACS is a relatively simple authentication protocol. TACACS was first developed in the mid-1980s to manage authentication for the U.S. Department of Defence unclassified network.

The need behind this protocol was to allow users to jump between machines or network infrastructure without having to re-login.

Use TACACS for: network infrastructure.

List of various other authentication protocols

- AKA
- CAVE-based authentication
- CRAM-MD5
- Digest
- Host Identity Protocol (HIP)
- LAN Manager
- NTLM, also known as NT LAN Manager
- OpenID protocol
- Password-authenticated key agreement protocols
- Protocol for Carrying Authentication for Network Access (PANA)
- Secure Remote Password protocol (SRP)
- RFID-Authentication Protocols
- Woo Lam 92 (protocol)
- SAML