rfc4513

Mécanismes de sécurité et méthodes d'authentification

LDAP offre les mécanismes de sécurité suivants :

- Authentification simple (Bind) fournis des mécanisme nom/mot de passe, et SASL.
- Des mécanismes pour supporter des contrôles d'accès spécifiques au vendeur
- Un service d'intégrité des données via TLS ou des mécanismes SASL
- Un service de confidentialité des données via TLS ou des mécanismes SASL
- Limitation de l'utilisation des ressources serveurs au moyen de limites administratives
- Authentification serveur via TLS ou des mécanismes SASL

Il est désirable de permettre aux clients de s'authentifier en utilisant divers mécanismes où les identités sont représentées sous forme de DN (RFC4512), chaîne (RFC4514), ou un nom d'utilisateur simple (RFC4013). Un serveur LDAP doit supporter le mécanisme d'authentification anonyme (Bind). Les implémentations LDAP qui supportent un mécanisme d'authentification autre que l'authentification anonyme (Bind) doivent supporter le mécanisme d'authentification nom/mot de passe Bind et doivent être capable de protéger ces accréditifs en utilisant TLS

Opération StartTLS

Le but d'utiliser TLS avec LDAP est de s'assurer de la confidentialité et de l'intégrité des données, et optionnellement fournir l'authentification. Les services d'authentification de TLS sont disponibles dans LDAP uniquement en combinaison avec la méthode d'authentification SASL externe.

StartTLS Request Sequencing

Un client peut envoyer la requête étendue StartTLS n'importe quand après avoir établis une session LDAP, excepté :

- Quand TLS est actuellement établie dans la session
- Quand une négociation multi-niveau SASL est en cours
- Quand il y'a des réponse en attente pour des requêtes précédemment fournies dans la session

Une violation de ces points résultent en code de retour **operationsError**

Certificat Client

Si des requêtes ou des demandes LDAP qu'un client émet en fournissant un certificat durant la négociation TLS et que ce certificat n'est pas utilisable ou ne peut être validé, le serveur peut utiliser une stratégie de sécurité local pour déterminer si la négociation réussie ou non.

Vérification de l'identité du serveur

Pour prévenir d'une attaque MITM, le client doit vérifier l'identité du serveur. L'identité du serveur est appelé l'identité de référence. Le client détermine le type de l'identité de référence (ex : nom DNS ou Address IP) et effectue une comparaison entre l'identité de référence et chaque **subjectAltName**. Différents subjectAltName sont matchés de différentes manière.

Le client peut mapper l'identité de référence à un type différent avant d'effectuer une comparaison, mais devrait le mapper uniquement en types pour lesquels le mappage est soit inhérent à la sécurité (ex : extraire le nom DNS de l'URI), soit pour effectuer un mappage sécurisé (ex : DNSSEC)

L'identité du serveur peut également être vérifié en comparant son cn dans le RDN du subjectName, bien que ce soit déprécié.

Comparaison des noms DNS

Si l'identité de référence est un nom de domaine internationalisé, il doit être convertit en ACE (ASCII Compatible Encoding) (RFC3490) avant de le comparer au SAN, en type dNSName. Le caractère '*' est autorisé dans les valeurs SAN de type dNSName.

Comparaison des adresses IP

Quand l'identité de référence est une adresse IP, l'identité doit être convertie en représentation "network byte order" (RFC791, RFC2460) La chaîne d'octets est comparée avec le SAN de type iPAddress.

Comparaison des autres types subjectName

L'implémentation des clients peut supporter une comparaison avec d'autres types de valeurs dans le SAN.

Discovery of Resultant Security Level

Une fois TLS établis dans une session LDAP, les 2 parties sont libre de continuer ou non, basé sur une stratégie local et sur le niveau de sécurité atteint. Les implémentations peuvent réévaluer le niveau de sécurité à tout moment, et si le niveau est inadéquat, devraient supprimer la couche TLS.

Refresh of Server Capabilities Information

Une fois TLS établis dans une session LDAP, le client devrait supprimer ou rafraîchir toutes les informations sur le serveur obtenu avant l'initialisation de TLS. C'est une protection aux attaques MITM.

Suite de chiffrement TLS

De nombreux problèmes devraient être considérés en sélectionnant la suite de chiffrement TLS :

- la capacité de la suite de chiffrement à fournir une protection de confidentialité des mots de passe et autre.
- la considération de la valeur du mot de passe et/ou données versus le niveau de confidentialité fournies par lasuite de chiffrement.
- Les vulnérabilités de la suite de chiffrement aux attaque MITM. Cette suite ne devrait pas être utilisé pour protéger les mots de passe et autres données sensibles.
- Après une négociation TLS, les 2 parties devraient vérifier que les services de sécurité fournis par la suite de chiffrement négociée sont adéquat pour la session LDAP. Si ce n'est pas le cas, TLS devrait être terminé.

Etat d'Authorisation

Toute session LDAP a un état d'autorisation. cet état comprend de nombreux facteurs tels que l'authentification établie, comment elle a été établie, et quels services de sécurité sont en place. Certains facteurs peuvent être déterminés et/ou affectés par des évènements de protocole.

une fois la session LDAP établie, la session a une identité d'autorisation anonyme. dès qu'une session BindRequest est reçue, le serveur place la session dans un état d'autorisation anonyme. Si la requête est réussie, la session est placée dans l'état authentification requise avec son état d'autorisation associée.

Bind Operation

Cette opération permet d'échanger des informations d'authentification entre le client et le serveur pour établir un nouvel état d'autorisation. Si l'identité d'autorisation est spécifiée, le serveur doit vérifier que l'identité d'authentification de client est permises pour permettre l'identité d'autorisation. Le serveur doit rejeter l'opération Bind avec un code invalidCredentials si le client n'est pas autorisé.

Simple Authentication Method

L'authentification simple fournis 3 mécanismes d'authentification :

- un mécanisme d'authentification anonyme
- un mécanisme d'authentification non-authentifié
- un mécanisme d'authentification DN/mot de passe

Anonymous Authentication Mechanism of Simple Bind

Un client LDAP peut utiliser le mécanisme d'authentification anonyme de la méthode simple Bind pour établir une autorisation anonyme en envoyant un Bind Request avec un nom vide et en spécifiant l'authentification simple contenant un mot de passe vide.

Unauthenticated Authentication Mechanism of Simple Bind

Un client LDAP peut utiliser le mécanisme d'authentification non-authentifié de la méthode simple Bind pour établir une autorisation anonyme en envoyant un Bind Request avec un nom (DN) et en spécifiant l'authentification simple contenant un mot de passe vide.

Name/Password Authentication Mechanism of Simple Bind

Un client LDAP peut utiliser le mécanisme d'authentification nom/mot de passe de la méthode simple Bind pour établir une autorisation anonyme en envoyant un Bind Request avec un nom (DN) et en spécifiant l'authentification simple contenant un mot de passe non vide.

Méthode d'authentification SASL

LDAP permet d'utiliser les mécanismes SASL. Vu que LDAP fournis nativement les méthodes d'authentification anonyme et nom/mot de passe, les mécanismes similaire SASL ne sont pas utilisés avec LDAP.

Initialisation de l'authentification SASL et échange du protocole

Le mécanisme SASL est initié via un message BindRequest avec les paramètres suivants :

- la version est **3**
- AuthenticationChoice est **sasl**
- l'élément mécanisme de la séquence **SaslCredentials** contient la valeur du mécanisme SASL voulu
- Les crédentials optionnels de la séquence **SaslCredentials** peuvent être utilisés pour fournir une réponse client initiale pour les mécanismes qui stipulent que le client envoie les données en premier.

un challenge est indiqué par le serveur qui envoie un message **BindResponse** avec un **resultCode** de **saslBindProgress**.

Au niveau du message LDAP, ces challenges et réponses sont des tokens binaires opaque de longueur arbitraire. les serveurs LDAP utilisent le champ **serverSaslCreds** dans un message **BindResponse** pour transmettre chaque challenge. Les clients LDAP utilisent le champ credentials dans la séquence **SaslCredentials** d'un message **BindRequest** pour transmettre chaque réponse.

Les clients envoyant un message **BindRequest** avec le choix **sasl** devraient envoyer une valeurs vide dans le champs nom, et les serveurs recevant un tel message devraient ignorer la valeur du champ nom.

Un client peut annuler une négociation SASL en envoyant un message **BindRequest** avec une valeur différente dans le champ **mecanism** de **SaslCredentials** ou avec **AuthenticationChoice** autre que **sasl**.

Le serveur indique la fin d'un échange SASL en répondant avec un **BindResponse** avec une valeur resultCode qui n'est pas **saslBindProgress**.

Le champ **serverSaslCreds** dans le **BindResponse** peut être utilisé pour inclure un challenge optionnel avec une notification **success** pour les mécanismes qui spécifient que le serveur envoie des données additionnelles avec l'indication de réussite.

Champs optionnels

LDAP fournis un champ optionnel pour une réponse initial dans un échange SASL et un champ optionnel pour les données additionnelles indiquant la sortie de l'échange. Vu que le contenu de ces champs dépend du mécanisme utilisé, SASL nécessite que le protocole détail comment un champ vide est distingué d'un champ absent. Une réponse vide est distinguée par la présence de **SaslCredentials.credentials** OCTET STRING (de longueur 0) dans le PDU. Si le client ne fournis pas de données additionnelles, ce champs doit être omis.

Octet où La couche de sécurité négociée prend effet

les couches SASL prennent effet suivant la transmission par le serveur et la réception par le client d'un BindResponse final dans l'échange avec un resultCode à Success. La couche reste effective jusqu'à ce qu'une nouvelle couche soit installée

Détermination des mécanismes SASL supportés

Les clients peuvent déterminer les mécanismes SASL supportés par le serveur en lisant l'attribut **supportedSASLMecanisms** depuis le Root DSE. Le serveur devrait autoriser tous les clients à lire cet attribut.

Règles pour utiliser les couches SASL

Une fois une couche SASL installée, le client devrait supprimer ou rafraîchir les informations sur le serveur obtenus avant la négociation SASL.

Identité d'autorisation SASL

Certains mécanismes SASL permettent aux clients de demander une identité d'autorisation pour la session LDAP. La décision de permettre ou non à l'identité d'authentification courante d'avoir accès à l'identité d'authorisation demandée est une décision locale. l'identité d'autorisation est une chaîne UTF8 sous la forme :

```
authzId = dnAuthzId / uAuthzId
 ; distinguished-name-based authz id
dnAuthzId = "dn :" distinguishedName
 ; unspecified authorization id, UTF-8 encoded
uAuthzId = "u :" userid
userid = *UTF8 ; syntax unspecified
```

Mécanismes d'authentification SASL EXTERNAL

Un client peut utiliser le mécanisme SASL EXTERNAL pour demander au serveur LDAP d'authentifier et établir une identité d'autorisation en utilisant des crédentials de sécurité échangés par une couche de sécurité tel que par l'authentification TLS.

Implicit Assertion

Une identité d'autorisation implicite est effectuée en invoquant une requête Bind SASL utilisant le mécanisme EXTERNAL qui n'inclus pas le champ optionnel crédentials. Le serveur va dériver l'identité d'autorisation du client de l'identité d'authentification fournies par la couche de sécurité en accord avec la stratégie locale.

Explicit Assertion

Une identité d'autorisation explicite est effectuée en invoquant une requête Bind SASL utilisant le mécanisme EXTERNAL qui inclus le champ credentials. La valeur de ce champs est l'identité d'autorisation.

Considérations de sécurité général

LDAP lui-même ne fournis aucune sécurité ou protection pour l'accès à l'annuaire par des moyens autres que le protocole LDAP. Les données sensibles peuvent être transportés dans presque tous les messages DAP, et leur divulgation peuvent-être soumis aux lois et autres réglementations dans de nombreux pays.

Une session dans laquelle le client n'a pas établit des services de protection et d'intégrité des données est sujet à des attaques MITM.

L'expérience montre que les clients peuvent mal utiliser le mécanisme d'authentification non-authentifié. Par exemple, un client peut prendre la décision de demander accès à des informations une fois une requête Bind complétée. Le serveur LDAP peut induire le client en erreurs, le laissant penser qu'il a été authentifié avec succès.

LDAP autorise des attributs de mot de passe multi-valués. Dans les systèmes où les entrées doivent avoir un seul mot de passe, les contrôles administratifs doivent être renforcés.