Network Working Group
<draft-ietf-cat-kerb-dh-key-exchange-00.txt>
Internet-Draft

M. Horowitz
Stonecast, Inc.

February, 1999

Diffie-Hellman Key Exchange for Kerberos V5

Status of this Memo

Abstract

The Kerberos protocol [RFC1510] currently establishes session keys by the assertion of one party (usually the KDC). This document describes a method for using the Diffie-Hellman algorithm to establish the shared secret between a Kerberos client and application service. For the purposes of this document, the Ticket Granting Service is considered an application service.

Overview

Two new pre-authentication types are defined which are used to establish a shared secret between Kerberos peers using ephemeral-ephemeral Diffie-Hellman key exchange.

Once the shared secret is established, it is used in place of the key returned in the EncKDCRepPart.

Protocol

The first message, PA-DH-REQ, is sent from the client to the server.

```
PA-DH-REQ ::= SEQUENCE {
        clientAuth              [0] ClientAuthenticator,
        clientAuthChecksum      [1] Checksum
                                -- computed over clientAuth,
                                -- Checksum key is the client
                                -- long-term secret key for an AS-REQ,
                                -- or the Ticket key for TGS-REQ.
}

ClientAuthenticator ::= SEQUENCE {
        clientPublicValue       [0] OriginatorPublicKey,
        kdcRealm                [1] Realm,
        ctime                   [2] KerberosTime,
        cusec                   [3] INTEGER
}
```

The ClientAuthenticator has two purposes. The first is to carry the client's DH (Diffie-Hellman) public value. The second is to provide enough information to avoid replay to another realm (kdcRealm) or later replay (ctime, cusec) should an attacker derive the private value from the DH public value. The checksum prevents modification and demonstrates the identity of the client to the KDC.

The second message, PA-DH-REP, is sent from the server to the client.

```
PA-DH-REP ::= SEQUENCE {
        serverAuth              [0] OriginatorPublicKey,
}
```

The server message is just the server's DH public value. It is not checksummed. In the case of an AS exchange, the client has no way to verify the KDC is legitimate. In the case of a TGS exchange, the EncTGSRepPart is encrypted in a key which validates the identity of the KDC.

The OriginatorPublicKey is defined in [CMS].

Once the DH key exchange is complete, the resulting secret must be converted to a symmetric key for use by the two peers. This is done via a simple modification to key derivation [HorowitzKD]:

```
Key = DK(k-fold(DH shared secret), Well-Known Constant)
```

Security Considerations

This document defines a new form of cryptography key exchange in Kerberos V5.

Using Diffie-Hellman for key exchange provides for stronger shared secrets with perfect forward secrecy. If the keys used to authenticate the exchange are compromised (such as a password or service key), past kerberos exchanges are not compromised, because only the public values are revealed. Even future exchanges are

somewhat protected, as the attacker would need to engage in an active attack rather than a passive attack to exploit the compromised key.

Acknowledgements

I would like to thank Sam Hartman for his contributions to this document.

References

[CMS] Housely, R., "Cryptographic Message Syntax", draft-ietf-smime-cms-10.txt, December 1998.

[HorowitzKD] Horowitz, M., "Key Derivation for Authentication, Integrity, and Privacy", Informational RFC submission pending.

[RFC1510] Kohl, J. and Neuman, C., "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993.

Author's Address

Marc Horowitz
Stonecast, Inc.
108 Stow Road
Harvard, MA 01451

Phone: +1 978 456 9103
Email: marc@stonecast.net