OSF DCE SIG
Request For Comments: 26.0
J. Pato (GZA)
June 1993

USING PRE-AUTHENTICATION TO AVOID PASSWORD GUESSING ATTACKS

1. INTRODUCTION

Users select poor passwords.

The strength of a security system is measured by the strength of its weakest link. Frequently, the weakest link is the password selected by a user. Password quality filters help impose restrictions on the type of password a user selects — but ultimately a key derived from a password that can be remembered and typed by a human is weaker than a truly random key. Attackers frequently take advantage of this property to break into systems ([Gram 84], [Seel 89], [Spaf 89]). Consequently, we must develop systems that make it harder for an attacker to leverage the weakness of password derived keys.

2. CURRENT PROTOCOL EXPOSURES

The Kerberos V5 protocols [Kohl 92] are subject to password guessing attacks in two ways:

(a) Attacks on a ticket issued for a given server principal.

(b) Attacks on a principal's ticket granting ticket.

These attacks share a common method — the attacker obtains data from the KDC encrypted using the victim's key. The data returned from the KDC contains verifiable plaintext — an attacker will be able to determine if they have guessed the proper key. The format of the data does not lend itself to an attacker with a pre-computed dictionary in the way a UNIX `/etc/passwd` file is vulnerable, but this simply increases the amount of time necessary to mount an attack. The attacker can simply make a network request to obtain the data and then proceed to attack it on a high speed processor.

In general the first attack is not as troubling as the second. In the DCE, servers and human users generally do not share a principal. Consequently, servers need not maintain keys that are derived from passwords. Server keys are typically generated from the full 56-bit DES key space and are much harder to attack than a key derived from a password. Human principals can be protected from an attack on their password-derived key by allowing them to act only as a client and not a server. The DCE registry database maintains administrative information about principals that determines which may act as clients, which as servers and which may be both.

2.1. Protecting Client Principals

The simplest mechanism for protecting client principals is to provide each principal with a device that stores a true 56-bit random DES key. The user's password then unlocks the device — but is not used in any network protocols. This insulates the password derived key from network attacks. This approach, however, relies on the widespread availability of the appropriate devices.

In the absence of hardware support, we must enhance the basic authentication protocol to avoid issuing a TGT encrypted using the user's key unless the KDC has been presented with proof that the caller knows the user's key. With this change, the KDC will not issue the data to an attacker — and it can notice persistent failures to establish a given principal's identity, recognize this as an attack, and take appropriate protective action.

3. USING PRE-AUTHENTICATION

The Kerberos V5 protocol allows the initial authentication request to carry optional pre-authentication data (*padata*). Currently the specification of the protocol does not define specific uses of this field, but the recent MIT Beta 2 implementation of the protocol has implemented a basic prototype facility. The MIT prototype takes the current time of day and encrypts it using the client principal's key. This data is sent to the KDC in the padata field to allow the KDC to determine that the request was timely and that the requester had access to the client's key. If the buffer decrypts correctly the KDC processes the request normally.

The following is the redefinition in ASN.1 of the prototype pre-authentication data:

```
PADATA-ENC-TIMESTAMPS ::= EncryptedData
        -- encrypted using the key of the client principal

PADATA-ENC-USERINFO ::= SEQUENCE {
        pvno     [0] INTEGER,
        cur_time [1] KerberosTime,
        nonce    [2] INTEGER
}
```

This approach has many of the benefits needed to avoid password guessing attacks. It is, however, still vulnerable to attackers who can listen to network messages. This weakness is due to using the client's password to encrypt verifiable plaintext [Loma 89]. An attacker can sniff the appropriate requests and replies on the network, and then attack them offline.

3.1. Third Party Pre-Authentication Sponsor

In the DCE, we have the opportunity to use a stronger approach and avoid sending any data over the network that is encrypted using the user's key. In the DCE, each machine has a corresponding authentication principal and the machine knows the key shared with the KDC. This allows us to use a key known to the local machine and the KDC to encrypt data rather than a key derived from the user's password.

The `PADATA-ENC-THIRD-PARTY` pre-authentication type provides a mechanism for the KDC to verify that the client knows a principal's key without exposing that key to network eavesdroppers. The padata contains three components: a ticket granting ticket (TGT) for the third party principal; a random key encrypted using the session key of the TGT; and a buffer encrypted using the client principal's key then encrypted under the preceding random key. Specifically:

```
PADATA-ENC-THIRD-PARTY ::= SEQUENCE {
        ticket       [0] Ticket,
        enc-subkey   [1] EncryptedData,
                -- encrypted using the ticket session key
        enc-userinfo [2] EncryptedData
                -- encrypted using the subkey
}

PADATA-ENC-THIRD-PARTY-SUBKEY ::= EncryptionKey

PADATA-ENC-THIRD-PARTY-ENC-USERINFO ::= EncryptedData
        -- encrypted using the key of the client principal

PADATA-ENC-THIRD-PARTY-USERINFO ::= PADATA-ENC-USERINFO
```

When a client principal is about to initiate a KRB_AS_REQ (initial authentication exchange with the KDC) it obtains the TGT for the third party sponsor, a usable version of the random subkey and a version of the same key encrypted under the session key in the third party's TGT. The ticket identifies the third party sponsor for the authentication exchange and establishes a shared key between the KDC and the third party sponsor. Note that the third party sponsor must obtain a TGT to the cell of the client principal, since the ticket passed in this message must be understood by the authentication server of the client's home cell.

The client encrypts the current time using the key derived from its password. The full encrypted data block is then encrypted with the random subkey.

3.2. Handling Pre-Authentication at the KDC

The principal database is extended with a per-principal attribute that determines if that principal must use pre-authentication and if so, which forms of preauthentication are permitted. When this attribute is set the principal is protected from initial authentication password guessing attacks. The KDC will not generate a KRB_AS_REP message for a principal that requires pre-authentication if the KRB_AS_REQ message did not properly use pre-authentication, instead it will issue a KRB_ERROR message with status KDC_PREAUTH_FAILED.

When PADATA-ENC-TIMESTAMPS is used, the KDC simply verifies that the client knew the correct password, and then yields a normal KRB_AS_REP message. Upon receipt of a KRB_AS_REQ bearing the PADATA-ENC-THIRD-PARTY padata type, the KDC decrypts the various buffers and also verifies that the client knew the correct password. The encrypted portion of the KRB_AS_REP message, however, is not encrypted using the client's key; the random subkey from the padata is used instead.

4. DETECTING AND THWARTING PASSWORD GUESSING ATTEMPTS

When a principal requires pre-authentication, it is possible for the KDC to detect failed initial authentication attempts. This allows the system to take protective action when an attack is detected. Policy attributes control the frequency of and place limits on attempts at initial authentication. When the policy-driven thresholds are exceeded, the KDC will mark the principal as invalid for initial authentication and alert administrators.

The DCE (1.0.2 and later) supports weak replication of the KDC database — so the limits on attempts cannot be hard. The limits are proportional to the number of replicas in the cell. When a replica detects that an attack has exceeded the limits at that replica, it will send an update to the master to disable that principal's access. Cell policy may also be configured to have each slave replica inform the master after a given number of failed attempts that is smaller than the disabling threshold. This increases the amount of traffic from a slave to the master, but allows the master to detect intrusion attempts that attempt to circumvent the limits by trying multiple replicas. When the master accumulates failed login attempts from multiple slaves that exceed the limits for a principal, it will automatically disable access for that principal without waiting for a given replica to exceed the threshold.

4.1. Preventing Denial of Service Attacks

The account lockout mechanism described above suffers from the vulnerability to denial of service attacks. An attacker who wishes to prevent a system administrator, or any other legitimate user, from accessing the distributed system need only simulate a password guessing attack to prevent the legitimate user from having access to her account.

The probability of denying access to a legitimate user can be lessened by adding a time period for the account lockout. Rather than letting the password guessing attempt lockout the account until a manual administrative action is taken, the account is locked out for a configurable period of time. This period establishes the rate at which an attacker can attempt to guess the given user's password. The configurable period of time can be set to an infinite value if manual administrative action is the desired policy.

5. ACKNOWLEDGEMENTS

Ted T'so (MIT) provided the prototype pre-authentication facility. Charlie Kaufman (DEC) and Bill Sommerfeld (HP) provided comments and suggestions on the third party sponsor pre-authentication facility. Some aspects of this design were influenced by contributors to the Kerberos mailing list during the June 1990 discussion on initial authentication.

DCE-RFC 26.0 was developed and written while the author was at Hewlett-Packard Company.

REFERENCES

[Gram 84] F. T. Grampp and R. M. Morris, ''UNIX Operating System Security'', AT&T Bell Laboratories Tech J. 63, 8, part 2, October 1984.

[Kohl 92] John Kohl and B. Clifford Neuman, ''The Kerberos Network Authentication Service'', INTERNET-DRAFT RFC, revision 5.1, 1 September 1992

[Loma 89] T. Mark A. Lomas, Li Gong, Jerome H. Saltzer and Roger M. Needham, ''Reducing Risks from Poorly Chosen Keys'', in Proceedings of the Twelfth ACM Symposium on Operating Systems Principles, December, 1989.

[Seel 89] Donn Seeley, ‘‘Password Cracking: A Game of Wits’’, Communications of the ACM 32, 6, June 1989.

[Spaf 89] Eugene H. Spafford, ‘‘Crisis and Aftermath’’, Communications of the ACM 32, 6, June 1989.

AUTHOR’S ADDRESS

Joseph N. Pato
Geer-Zolot Associates
1 Main Street
Cambridge, MA 02142
USA

Internet email: pato@gza.com
Telephone: +1-617-374-3700