This memo assigns client authentication error codes for those situations where a client may take specific corrective action in the face of a failed authentication attempt. Some of these codes are used by one strategy to transition users away from unencrypted clear text passwords.

A number of important security considerations related to authentication errors are also discussed.

This memo assigns SMTP error codes [SMTP], ESMTP error codes [ESMTP-ERR], IMAP response codes [IMAP4], POP3 [POP3] extension codes [POPEXT], and ACAP [ACAP] response codes.
1. Conventions Used in this Memo

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as defined in "Key words for use in RFCs to Indicate Requirement Levels" [KEYWORDS].

1.1. Terminology Used in the Memo

Authentication Credentials
   The information the client sends to the server to prove its identity to the server.

Authentication Verifier
   A piece of per-user data stored on a server which is used to verify if an authentication exchange for a given user includes valid authentication credentials.

Passphrase
   The term "passphrase" is used rather than "password" to discourage the use of simple single-word passphrases.

2. Concealing Users on the System

Before discussing specific error codes, it is important to note that an active attacker who is aware of the userids of people on the system is more dangerous than an active attacker with no information. This concern is pervasive when discussing authentication error codes, because it is very easy to reveal the existence of a user with an incautious authentication error system.

However, there may be cases where it is more important to give the client good information so it can take corrective action, than it is to conceal users. For example, help desk costs necessary for users who see a generic "Authentication Failed" error at one site might outweigh the risk of revealing system userid to an active attacker.

Every server which provides client authentication SHOULD have a configuration setting where the validity of a user is not revealed by a failed authentication attempt. In particular, the non-existance of a user is treated identically to a bad passphrase, an authentication mechanism deemed too weak, or a missing authentication verifier, both in the text of the protocol and in the speed of the server response.
3. An Authentication Transition System

While there is a strong desire to stop sending unencrypted clear text passphrases, system administrators of existing systems often are unable to do so unless it is nearly painless for the users. A number of Internet protocols (e.g., HTTP, POP, ACAP, IMAP, SNMP, PPP) now have standards track challenge-response authentication mechanisms based on cryptographic hash functions. However, the authentication verifier for these mechanisms is either the user’s passphrase itself or something derived from it in a special way.

Unfortunately, most sites with existing users have authentication verifiers that are an incompatible one-way function of the user’s passphrase. Thus a new mechanism normally cannot be deployed without forcing users to set new passphrases on the system. So even if a user were to set his POP client to use APOP [POP3], the authentication would fail until the appropriate server verifier was initialized.

A site which is more concerned with ending the use of unencrypted clear text passphrases than with revealing users to an active attacker can enable authentication transitioning. When a client attempts to use APOP, but the verifier is not initialized, then the server returns a response code indicating that a "transition is needed." The client then attempts authentication with a clear text passphrase one last time (with user confirmation) to force a transition. After this, both the client and the server can flag the user as transitioned and cease using unencrypted clear text passphrases.

Note that a man-in-the-middle attacker could cause a client authentication to fail with this specific error code in an attempt to trick the client into using an unencrypted clear text passphrase. A client can prevent this attack by negotiating a full-strength encryption layer prior to using a clear text passphrase for the transition, or mitigate the attack either by getting explicit user permission for the transition or by saving a flag after a successful strong authentication and refusing to transition again.

4. Authentication Response Codes

This section identifies a number of authentication success and error conditions where a client MAY take a specific action. For each condition, a response code suitable for ACAP, IMAP or POP is defined, a regular SMTP 3-digit error code, an enhanced SMTP error code [ESMTP-CODES], and in some cases an FTP response codes from...
Successful Authentication

ACAP, IMAP, POP: Generic "OK" response suffices
SMTP: 234 [SMTP-AUTH]
Enhanced SMTP: 2.7.0
FTP: multiple, see [FTP] and [FTP-SEC] for details

This indicates that the security exchange was successful.

Security Considerations: May not indicate client or server is authenticated.

Successful Authentication with Data

ACAP: SASL base64data [ACAP]
IMAP, POP: N/A
SMTP: N/A
Enhanced SMTP: N/A
FTP: 235 [ADAT=base64data] [FTP-SEC]

This is used when the server has successfully authenticated the client, but includes optional data in the response which the client may use to mutually authenticate the server. Protocols without such a response have an extra round-trip when the server provides mutual authentication data as described in SASL [SASL].

Security Considerations: Integrity protection is not possible if this information ignored by the client.

Temporary Authentication Failure

ACAP, IMAP, POP: TRYLATER [ACAP]
SMTP: 454 [SMTP-AUTH]
Enhanced SMTP: 4.7.0
FTP: 431 [FTP-SEC]

This occurs when there is a temporary failure during authentication. It indicates some resource necessary to authenticate is unavailable at the present time.

Security Considerations: May reveal information about users on
a system with multiple authentication sources where an earlier one is local and a later one is remote.

Invalid Authentication Mechanism

ACAP, IMAP, POP: The generic BAD or -ERR response suffices
SMTP: 504 [SMTP, SMTP-AUTH]
Enhanced SMTP: 5.5.4 [ESMTP-CODES]
FTP: 504 [FTP, FTP-SEC]

This error code occurs when the client attempts to use an authentication mechanism which the server does not implement.

Security Considerations: An active attacker could issue this error code to attempt to get the client to try a weaker mechanism and reveal more information. Clients SHOULD be configurable to fail or get user permission if the only remaining mechanisms are weak.

Authentication Failed (Bad user name or passphrase)

ACAP, IMAP, POP: The generic NO or -ERR response suffices
SMTP: 535 [SMTP-AUTH]
Enhanced SMTP: 5.7.8
FTP: 530 [FTP]

This occurs when an invalid user name is used, or the passphrase or other authentication credentials are incorrect. It is also the preferred error code for any non-syntax failures which do not have a specific error code here. It is quite reasonable for a server to return only success error codes, or this error code.

Security Considerations: It is important not to distinguish between "unknown user" and "bad passphrase" to conceal users. It is important to supply a consistent delay when this error code occurs to prevent fast password searches. A server MAY unilaterally close the connection after a specific number of failed authentication attempts to make password searches even harder.

Authenticate Exchange Cancelled

ACAP, IMAP, POP: The generic BAD or -ERR response suffices
SMTP: 501 [SMTP-AUTH]
Enhanced SMTP: 5.7.0 [ESMTP-CODES]
FTP: not defined
This occurs when the client cancels a multiple-round-trip authenticate exchange in the middle. SASL profiles are required to document how the client cancels the exchange.

Security Considerations: none

Authentication Mechanism Too Weak

ACAP, IMAP, POP: AUTH-TOO-WEAK
SMTP: 522
Enhanced SMTP: 5.7.9
FTP: 534

Some currently deployed clients are statically configured to use only clear text passphrases by default, but can be configured to support a stronger mechanism. This error code provides a way to tell those clients that they are no longer permitted to use a weak mechanism, such as clear text passphrases, and must try something stronger. It may be particularly useful during a transition period where a weaker mechanism is available to un-transitioned users and a stronger mechanism is required for transitioned users.

Security Considerations: Reveals information about the users on the system, but provides ability to force clients to upgrade their authentication.

Encryption Needed

ACAP, IMAP, POP: ENCRYPT-NEEDED
SMTP: 523
Enhanced SMTP: 5.7.10
FTP: not defined

This indicates that external strong privacy layer is needed in order to use the requested authentication mechanism. This is primarily intended for use with clear text authentication mechanisms. A client which receives this may activate a security layer such as TLS prior to authenticating, or attempt to use a stronger mechanism. Note that code this does reveal the existance of users on the system to an active attacker but that is mitigated by the ability to force users to activate a privacy layer.

Security Considerations: If this is applied regardless of the user name supplied, this can improve site security. If this is applied on a per-user basis, it can reveal information about users on the system.
Expired Passphrase

ACAP, IMAP, POP: EXPIRED-PASS
SMTP: 524
Enhanced SMTP: 5.7.11
FTP: not defined

This indicates the user’s passphrase or passphrase has expired and needs to be changed. Many sites have a policy which forbids a passphrase or passphrase from being used too long. These sites will set a time period after which passphrases must be changed. Some sites also pre-expire passphrases set by a system administrator, such that a user must change their passphrase prior to using their account. A client which receives this error code can treat it as a user request to change her passphrase.

Security Considerations: The server should verify that the correct old authentication credentials were provided prior to issuing this error, otherwise it would reveal information about users on the system.

Transition Needed

ACAP, IMAP, POP: TRANSITION-NEEDED [ACAP]
SMTP: 422 [SMTP-AUTH]
Enhanced SMTP: 4.7.12
FTP: not defined

This occurs after a client attempts to authenticate using a mechanism other than clear text. It indicates that the server has an entry for the specified user in a legacy authentication database but does not yet have an authentication verifier necessary to offer the requested mechanism. A client which receives this error code may do a one-time login using a clear text login after asking the user for permission to activate the transition.

Security Considerations: If clear text passwords are used to transition, a strong privacy layer SHOULD be used. This error reveals the existence of users to active attackers, but it also provides an effective method to transition away from using clear text passphrases without forcing users to change their passphrases.
User Account Disabled

ACAP, IMAP, POP: DISABLED
SMTP: 525
Enhanced SMTP: 5.7.13
FTP: not defined

Sometimes a system administrator will have to disable a user’s account (e.g., due to lack of payment, abuse, evidence of a break-in attempt, etc). This error code occurs after a successful authentication to a disabled account. This informs the client that the failure is permanent until the user contacts their system administrator to get the account re-enabled. It differs from a generic authentication failure where the client’s best option is to present the passphrase entry dialog in case the user simply mistyped their passphrase.

Security Considerations: Same as for EXPIRED-PASS above.

5. Gradual Transition on PLAIN Example

Here is a sample transition exchange between an IMAP client and server. In this example, "C:" and "S:" indicate lines sent by the client and server respectively. If such lines are wrapped without a new "C:" or "S:" label, then the wrapping is for editorial clarity and is not part of the command.

Note that this example uses the IMAP profile [IMAP4] of SASL [SASL]. The base64 encoding of challenges and responses, as well as the "+ " preceding the responses are part of the IMAP4 profile, not part of SASL itself. Newer profiles of SASL will include the initial client PLAIN message with the AUTHENTICATE command itself so the extra round trip below (the server response with an empty "+ ") can be eliminated.

In this example, the user’s authentication identifier is "tim", his authorization identifier is the same, and his passphrase is "tanstaafstanstaaf".

S: * OK IMAP4 server ready
C: A001 CAPABILITY
S: * CAPABILITY IMAP4 IMAP4rev1 AUTH=CRAM-MD5 AUTH=PLAIN
S: A001 OK done
C: A002 AUTHENTICATE CRAM-MD5
S: + FDE40TYuNjkh3MTw0T6yQHv3c3RvZmZpY2UucmVzdG9uLm1jaS5sZ5uZXQ+
C: dGltIGI5MTNhNjAyYzd1ZGE3YTQ5NWI0ZTZlNzMzNGQzODkw
S: A002 NO [TRANSITION-NEEDED] You can’t login securely until you’ve changed your passphrase on the server
<client gets permission from user to transition>
C: A003 AUTHENTICATE PLAIN
S: +
C: AHRpbQB0YW5zdGFhZ2nRhbwrNOYWFm
S: A003 OK You can now login securely in the future.
C: A004 SELECT INBOX
...

6. Security Considerations

Security considerations are discussed throughout this document, and in sections 2-4 in some detail. This memo focuses on two major security concerns: network transmission of unencrypted clear text passphrases, and revealing the existence of users on the system to an attacker. It suggests one way to remedy the former at the short-term expense of the latter weakness.

7. References


Acknowledgements

The following people provided helpful feedback on this document:

Ned Freed, Steve Hole, John Myers, Larry Osterman

Author’s Address

Chris Newman
Innosoft International, Inc.
1050 Lakes Drive
West Covina, CA 91790 USA

Email: chris.newman@innosoft.com