Network Working Group
Internet Draft: ROAMING-ELGAMAL
Document: draft-overell-roaming-elgamal-sasl-00.txt February 1998
Expires: August 1998

P. Overell
Demon Internet Ltd

ROAMING-ELGAMAL SASL Authentication Mechanism

Status of this Memo

Abstract

ROAMING-ELGAMAL is an SASL [SASL] authentication mechanism in which ElGamal [ELG] public key cryptography is used to encrypt the persona and password thus giving a high degree of security.

Although specifically designed for the Simple Roaming Authentication Protocol [SRAP], ROAMING-ELGAMAL is intended to be a registered SASL mechanism and so could be adapted to other protocols. The mechanism has been designed to resist attack from interception, man in the middle, and replay. The security of the mechanism rests with the protection of the private key.

1. Conventions Used in this Document

In SASL terminology "server" means the authenticator and "client" means the authenticatee. Data from the server to the client is a "challenge", data from the client to the server is a "response".

All syntax is specified using ABNF [ABNF] and its core definitions.

2. ROAMING-ELGAMAL Mechanism

The SASL authentication type associated with ROAMING-ELGAMAL is "ROAMING-ELGAMAL".

This memo is only concerned with authentication, however, a security layer could be easily added either by continuing to use ElGamal encryption for the remainder of the conversation; or by using a symmetric cipher with a session key derived from the calculated value of y^k, a value known to both parties only after authentication is complete.

2.1 Initial Server Challenge

The data encoded in the initial challenge is a persona, a fingerprint and a cookie.

The persona indicates which persona/password pair the server is seeking authentication for. If no persona is specified (zero size) then the client may choose either to return any of its persona/passwords or fail the command. If the persona is specified but not recognized then the client SHOULD fail the command. An implementation MAY choose the persona to be the same as a "username" or "user id" but this memo does not require this interpretation.

The fingerprint indicates which public key the client should use to encrypt its response. The fingerprint MAY be the MD5 or SHA-1 of the public key as per PGP, but this memo does not require this interpretation.

The cookie is a presumptively arbitrary string of random octets. The cookie should be unique and unpredictable, preferably a cryptographically strong random number. Its purpose is to defeat replay attack.

This memo does not define the length or content of the persona, fingerprint or cookie. To permit any octet to be used each element is preceded by its size in octets expressed as a number in text enclosed in braces. The encoding used is defined by the host protocol.

Syntax

```
unencoded-challenge = size persona size fingerprint size cookie

persona = *OCTET
```

```
      fingerprint = *OCTET
```

cookie = *OCTET

size = "{" 1*DIGIT "}"

Example (fictitious)

{4}paul{32}AB246508F5217B54C77D3400239BCA45{16}9723763476348973

2.2 Client's Response

If the client wishes to proceed then it responds with an encoded string of the ElGamal encrypted string of the PKCS#1 [PKCS#1] packed string consisting of the client's persona, password and the server's cookie. The server's public key is used for the encryption. This memo does not describe how the client may obtain the server's public key. The encoding used is defined by the host protocol

This memo places no restriction whatsoever on the content or length of persona, password or cookie. In the unpacked-response each element is preceded by its size in octets expressed as a number in text enclosed in braces.

Syntax

persona = *OCTET

password = *OCTET

cookie = *OCTET

size = "{" 1*DIGIT "}"

unpacked-response = size persona size password size cookie

packed-response = %x00 %x02 8*padding %x00 unpacked-response

padding = %x01-FF

Example (fictitious)

{4}paul{8}sausages{20}b_basdlwyweyfbc73m8f

2.2.1 Packing and Encryption

Let L be the length in octets of the ElGamal encryption modulus.

If the length of the unpacked-response is greater than L - 11 octets then the unpacked-response is split into sections, each of which

must be less than or equal to L - 11 octets long.

Each unpacked-response-section is then packed according to [PKCS#1] by preceding the unpacked-response-section with octet 0, octet 2, a padding string, and an octet 0. The padding string consists of at least eight non-zero random octets. The total length of the packed form is the same as the length of the ElGamal encryption modulus.

To encrypt a packed-response-section

Given the client's public key (p, g, y) where p is the prime modulus and y = g^x mod p where x is the private key.

M is the packed-response-section considered to be an integer with the first octet being the most significant.

Pick a random number k

a = g^k mod p

b = y^k M mod p

The encrypted-response-section is ab. These two numbers are expressed as string consisting of two multiprecision fields as defined in [PGPFormat].

Definition. A multiprecision field is the concatenation of two fields:

(a) a whole number field of length 2, with value B;
(b) a whole number field, with value V.

Field (b) is of length [(B+7)/8], i.e., the greatest integer which is no larger than (B+7)/8. The value of the multiprecision field is defined to be V. V must be between 2^{B-1} and 2^B - 1 inclusive. In other words B must be exactly the number of significant bits in V.

The encrypted-response is formed by concatenating all of the encrypted-response-sections.

The encrypted-response is then encoded according to the host protocol.

2.3 Authentication

The server then decodes, decrypts and unpacks the string and then verifies the persona, password and cookie. If correct the client is deemed to be authenticated.

ElGamal decryption is given by

M = b/a^x mod p

3. References

[ABNF] RFC2234, "Augmented BNF for syntax specifications: ABNF", D. Crocker and P. Overell, November 1997.

[ELG] "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms". T. ElGamal, IEEE Transactions on Information Theory, v. IT-31, n. 4, 1985, pp. 469-472.

[PGPForm] RFC1991, "PGP Message Exchange Formats". D. Atkins et al. August 1996.

[PKCS#1] RSA Data Security, Inc. Public-Key Cryptography Standards (PKCS). PKCS #1, "RSA Encryption Standard". An RSA Laboratories Technical Note, version 1.5, revised November 1, 1993.

[SASL] RFC2222, "Simple Authentication and Security Layer (SASL)". J. Myers, Netscape Communications, October 1997.

[SRAP] Work in progress, "Simple Roaming Authentication Protocol", P. Overell, Demon Internet Ltd. February 1998

4. Security Considerations

The use of ElGamal public key encryption together with a cryptographically strong cookie should make this mechanism resistant to interception, man in the middle and replay attacks.

5. Author's Address

P. Overell
Demon Internet Ltd
Dorking Business Park
Dorking
Surrey
RH4 1HN
UK

mailto:paulo@turnpike.com