Network Working Group
Internet-Draft
Expires: August 25, 2003

J. Laganier
ENS Lyon / Sun Microsystems, Inc.
G. Montenegro
Sun Microsystems, Inc.

February 24, 2003

Using IKE with IPv6 Cryptographically Generated Address
draft-laganier-ike-ipv6-cga-00

Status of this Memo

Copyright Notice

Abstract

This document describes IKE peer authentication via IPv6 Cryptographically Generated Addresses. These have been proposed to solve several security issues in the absence of any trusted infrastructure.

Table of Contents

1. Introduction and Problem Statement

This document describes how to use IKE with IPv6 Cryptographically Generated Address (CGA). This technique only requires slight modifications and can be used by one or both peers.

One use of CGA is address proof-of-ownership, but it can also be used with authorization certificates (e.g. SPKI, Keynote2) to enable a flexible authorization framework. CGA's have been proposed to solve several security issues in the absence of any trusted infrastructure, for example, securing Binding Updates in Mobile IPv6, securing Neighbor Discovery for IPv6, and securing Group Membership in Multicast and Anycast communications.

2. Related work

The lack of a global, Internet-wide, trusted infrastructure is at the heart of these issues. This precludes a straightforward application of IPsec between any two previously unknown nodes. The impossibility of always having the choice of obtaining a security association by leveraging a centralized infrastructure has led to cryptographic techniques commonly known as CGA or SUCV. CGA usage has lacked generality as it has been applied either within specific frameworks like Mobile IP ([4], [5]) or using its own custom protocol, Statistically Unique and Cryptographically Verifiable protocol (sucvP) [4]. Lately, a proposal using Just Fast Keying (JFK) has been put forth ([6]). Nevertheless, we believe that a full-blown key exchange protocol is redundant. Moreover, because the design, implementation and debugging of a new security protocol is especially costly and error-prone, we think that it is not worth "reinventing the wheel". From the point of view of implementation effort, the fact that this approach only requires the addition of stand-alone CGA validation routines into existing IKE daemons (e.g. racoon, isakmpd, pluto, etc) is another considerable advantage.

Accordingly, this note presents an overview of how to use the Internet Key Exchange protocol [1] while one or both peers authenticate themselves via CGA proof-of-ownership. This document details the slight modifications needed. Additionally, it aims at capturing the current thinking about how to achieve proof-of-ownership in IKE via CGA in a standard manner, thus preventing subsequent conflicting definitions.

3. Node Configuration and Requirements

Each node that want to prove address ownership via CGA generates a public-private key pair, PK and SK, respectively. The nodes then use P to obtain and configure a CGA as specified in [4]:

```
CGA = NetworkPrefix | SHA1_64 ( PK )
```

Those nodes that want to prove that they own their CGA should use it as their so-called IKE "peer" address while sending IKE packets.

4. ISAKMP Payload use

A peer wanting to prove CGA ownership while exchanging keys with IKE has to use ISAKMP payloads in a specific manner. Following subsections describes the requirements on those of the ISAKMP payloads that need it while doing an IKE phase 1 exchange with CGA proof-of-ownership.

4.1 Identification Payload

The Identification (ID) Payload of IKE contains the name of the entity to be authenticated with the Authentication (AUTH) Payload. When using CGA, the name of the node is its CGA. Though CGA are IPv6 Addresses as well, a peer embedding its CGA within the ID payload under the type ID_IPV6_ADDR would not trigger any verification of the PK-CGA binding on the other side. Hence, we believe that a new ID type is needed to explicitly state the cryptographic nature of a CGA and require verification of the binding. Thus, a peer wanting to prove CGA ownership MUST use an ID payload of type ID_IPV6_CGADDR containing its CGA. The value of type ID_IPV6_CGADDR is initially assigned out of the range 249-255 reserved for "private use amongst cooperating systems", as per [2]. If justified, a subsequent, more official assignment will imply IANA involvement.

4.2 Certificate Payload

The Certificate (CERT) Payload provide a means to transport certificates within IKE packets. When performing CGA ownership exchange, Certificates should be used to transmit to the correspondent the public key used to generate the CGA. Though several types of certificates are specified in [1], we only use those that contains a public key, namely PKCS7_WRAPP_X509_CERT, PGP_CERT, DNS_SIGNED_KEY, X509_CERT_SIGNATURE and SPKI_CERT. A peer wanting to prove CGA ownership MUST use a CERT payload that contains the public key used when generating its CGA.

4.3 Certificate Request Payload

The Certificate Request (CERTREQ) Payload is used by a peer to request preferred certificates to its correspondent. A preference is the type of certificate requested as well as an acceptable certificate authority for this type. A peer can include multiples preferences using several CERTREQ payload. For CGA, certificates used would usually be self-signed, though this does not preclude one to generate its CGA using the public key embedded in a CA-signed certificate.

4.4 Authentication Payload

The Authentication (AUTH) Payload contains data used to authenticate the entity named in the ID payload, i.e. the CGA owner. Since CGA are generated using public key cryptography, the AUTH payload have to contain a digital signature of the message computed using the public key contained in the CERT payload. Currently specified digital signature algorithms includes RSA and DSA, but this scheme could be used with any public key cryptographic algorithm. A peer wanting to prove CGA ownership MUST use an AUTH payload that contains the digital signature computed using the private key associated with its CGA.

5. Authentication of the IKE Security Association

[1] does not mandate that two peers exchanging keys use the same means of authenticating themselves. Available means of authentication are Digital Signatures, Public Key Encryption and Pre-shared Secret. It is explicitly stated that end-points are not required to use the same means of authenticating themselves. One could use pre-shared secret, while the other could use a digital signature. This note does not conflict with that, allowing one or both entities to prove CGA ownership, thus allowing one to possibly use another means of authenticating itself.

On nodes that want to verify address ownership, IKE implementation should be modified to handle the case of CGA verification which is very similar to already implemented self-signed certificates one. Apart from verifying the self-signed certificate, the implementation MUST verify that the public key contained in the certificate generate the address used in the identity payload as detailed above.

6. Conclusion

This note presents an overview of how IKE and CGA can be combined to achieve CGA proof-of-ownership authentication. The CGA technique is sufficiently well understood and can use widely deployed and implemented mechanisms. This proposal works in the absence of any previously established direct or indirect (via a broker, AAA roaming operator or trusted third party) security relationship. Because of this, these methods are a very practical and deployable means of using IPsec between previously unknown peers.

7. Security Considerations

This document discusses possible use of IKE as a means to prove CGA ownership and exchange keys to bootstrap IPsec SAs. Because IKE has already been specified and this technique only slightly modify it, we believe that this should not raise others security concerns that those incurred by CGA proof-of-ownership. Though the cryptographic algorithm used are the same, CGA proof-of-ownership is very different in nature to authentication. One must be especially careful when establishing the security policy, as this technique allows nodes that use their own IPv6 CGA to be successfully authenticated as their "owner". This is similar in essence to IKE used with self-signed certificates, with the additional consideration that CGA binds the address to the public key. A CGA may be considered as a verifiable self-generated address.

8. Open Issues

This document introduce a new ID payload type, ID_IPV6_CGADDR. However, it is not yet clear what is the most appropriate means of requiring peers to verify the PK-CGA binding. Other means are possible.

9. Intellectual Property Rights Considerations

The IETF takes no position regarding the validity or scope of intellectual property or other rights that might be claimed pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list of claimed rights.

Normative References

[1] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[2] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[3] Maughan, D., Schneider, M., Schertler, M. and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

Informative References

[4] Montenegro, G. and C. Castelluccia, "Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses.", NDSS 2002, February 2002.

[5] Roe, M., Aura, T., O'Shea, G. and J. Arkko, "Authentication of Mobile IPv6 Binding Updates and Acknowledgments", draft-roe-mobileip-updateauth-02 (work in progress), February 2002.

[6] Castelluccia, C. and G. Montenegro, "IPv6 Opportunistic Encryption", INRIA Research Report RR-4568, October 2002.

[7] Castelluccia, C. and G. Montenegro, "Securing Group Management in IPv6 with Cryptographically Generated Addresses", draft-irtf-gsec-sgmv6-00 (work in progress), April 2002.

Authors' Addresses

Julien Laganier
ENS Lyon / Sun Microsystems, Inc.
180, avenue de l'Europe
38334 Saint Ismier CEDEX
France

EMail: julien.laganier@sun.com

Gabriel Montenegro
Sun Microsystems, Inc.
180, avenue de l'Europe
38334 Saint Ismier CEDEX
France

EMail: gab@sun.com

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.