Network Working Group

Scott Bradner
Harvard University
Allison Mankin
USC/ISI
Jeffrey I. Schiller
Massachusetts Institute of Technology
Feb, 2001

A Framework for Purpose Built Keys (PBK)

<draft-bradner-pbk-frame-00.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Copyright Notice

Copyright (C) The Internet Society (2001). All Rights Reserved.

Abstract

This memo defines a framework for the consideration of a particular class of the need to authenticate the source of a network communication. The class consists of those cases where the actual identity of the source is not important but the knowledge that the source is the same one as started the communication and the assurance that the source cannot be spoofed are important. This memo defines the use of specially generated public/private key pairs, known as

Purpose Built Keys (PBKs), to provide this knowledge and assurance.

1.0 Introduction

There are many cases in Internet protocols where cryptographic mechanisms can add significant security improvement. However most such mechanisms rely on associating keys to entities, ultimately requiring an enterprise wide or potentially globally deployed Public Key Infrastructure (PKI).

In the absence of security mechanisms, many protocols are continuously vulnerable to attack.

However there are many circumstances where we can improve overall security by narrowing the window of vulnerability, so that if we assume that some operation is performed securely, we can secure all future transactions.

There are also cases where the actual identity of the initiator of a network communication is not an important piece of information, yet it is important to know that successive packets are from that same source. One example of this is in mobile IPv6. Mobile IPv6 contains a rebinding option that enables a mobile node to tell the other end of a communication that the IP address for the mobile node has changed. It is clearly important to know that any such rebinding request actually came from the correct mobile node even if the identity of the user of that mobile node does not need to be known.

Note that it is not that the identity of the user here is unimportant to the network (the node user may well authenticate to a AAA server at the start of network activity), but rather that it is unimportant to accomplish that level of authentication for the purpose of rebinding. Another example of this class of authentication would be continuing a connection through local renumbering of its site.

This memo describes the use of a temporary public/private key pair which is generated by a host for each case where the consistency of authentication needs to be assured. For example, a new key pair would be generated before each mobile IP session and discarded when the session was complete.

This use of these host-generated temporary keys is confined to the

parties in a communication and does not require that the keys be registered with or known by any third party. Thus this mechanism does not require that any support infrastructure exist outside of the protocol support in the corresponding hosts and can be deployed incrementally as host support becomes available. It also scales well

since the operations are confined to the end systems involved in the communication.

By not using registered keys, this mechanism preserves user anonymity as long as the identity of the users are not obtained by some other process during the communication.

This mechanism does not require the use of a reliable protocol and it is a mechanism that fits under transports or under applications, and differs from IPSec in that it is applied on demand by an application or transport.

When this mechanism is used with applications it can be used in ways similar to the use of web cookies but the use is under the control of the node that initiates the connection rather than under the control of the server. This mechanism gives the user control over the scope of the use of a particular identity.

2.0 Conceptual Overview

Following is a conceptual step-by-step description of the PBK process when operating below the transport layer.

First some definitions:
initiating node: the node initiating the conversation
receiving node: the node at the other end of the conversation

Before a initiating node initiates a connection during which it will need to prove that it is the same node that started the connection it creates a public/private key pair for use during the connection. This is known as a purpose-built key (PBK) pair.

The initiating node then creates an Endpoint ID (EID) by performing a cryptographic hash of the public part of the PBK. This EID will be used as an identity token for the node.

The initiating node then initiates the connection. The EID is sent along with the initial packets in the connection. In IPv6 this could be done in an end-to-end option header, in IPv4 as a header option. (These option ideas are for transport level use of the PBK - if the PBK was used from within HTTP or another application, its position would not be have to be in the IP header). The EID does not need to appear in all of the packets; it just has to be reliably conveyed to the receiving node.

The receiving node stores the EID and the source IP address in the received packet in a table.

At some time in the connection before the proof of identity is needed, the initiating node sends its public key to the receiving node. This again could be done in IP-level options or in an application-level exchange. The receiving node verifies that the received public key hashes to the previously provided EID.

When the initiating node wants to perform some operation, such as a mobile IPv6 address rebinding, it sends the operation request along with the EID. The message is signed using the private part of the PBK. If replay protection is necessary, a nonce value (a monotonically increasing value) or timestamp may be included with the operation request.

When the receiving node gets such an operation request, it fetches the previously sent public key from session state. This key is then used to verify the digital signature on the operation request. If the protocol calls for a nonce value, it verifies that the nonce value is larger then any previously received nonce. The protocol may use a timestamp, in which case the receiving node determines if the timestamp is timely for the operation request.

The PBKs would normally be discarded at the end of the communication but in those cases where a continuity of identity is needed over multiple sessions the PBKs could be retained until the requirement was over.

3.0 Notes on the design

The hash of the public key is used as the EID so that the

relationship between an offered EID and public key can be established. If a receiving node is in possession of the private key and the hash of the corresponding public key matches an offered EID, it can be sure that it has the correct EID for that public key.

Retransmission algorithms, where they are needed, must be conformant with RFC 2914 [RFC2914].

In the cases where commands could be issued by both ends of a communication, as would be the case in mobile IPv6 if both ends were mobile, separate PBKs would be created by each end and the mechanism would be run independently by each end.

3.0 Security Considerations

This whole document is about how to perform authenticated operations in an environment where there is no security infrastructure and one where network addresses might change during the communication.

In the absence of infrastructure, it is not always possible to authenticate one party to another. In the absence of any cryptographic security mechanism, internet transactions are continuously at risk of compromise. With PBKs it is possible to leverage an initial "leap of faith" so that presuming an initial transaction has not been tampered with (say the exchange of EID's at the beginning of an association between two parties), future transactions can be secured.

6.0 Author's Addresses

Scott Bradner
Harvard University
Cambridge MA 02138

Phone +1 617 495 3864
email sob@harvard.edu

Allison Mankin
University of Southern California, Information Sciences Institute
4350 N. Fairfax Drive, Suite 620

Arlington, VA 22203
Phone: +1 703 812 3706
email: mankin@isi.edu

Jeffrey I. Schiller
Massachusetts Institute of Technology
MIT Room W92-190
77 Massachusetts Avenue
Cambridge, MA 02139-4307
Phone: +1 617 253 0161
email: jis@mit.edu

Appendix A - Mobile IPv6 Example

Let's start by discussing briefly how Mobile IPv6 works. Note: This is not intended to be a comprehensive description of the protocol, and important details are left out for brevity. Full information can be obtained from [MobileIPv6].

In a Mobile IPv6 world, a node may move from location to location. As it does, the best IP address to reach it may change, as IP addresses are integral to the operation of routing. As a node changes its topological location on the Internet, it needs to be reached at a different IP address.

Yet, TCP and other transport protocols expect an IP address to remain stable for the duration of a session. Mobile IP deals with this by

having a router close to a node's "home" address be in a position to intercept and forward any traffic for the mobile node to the IP address that it is currently reachable at. A mobile node's normal IP address is called its "home" address and the IP address where it is currently reachable is its "in care of" address.

When a mobile IP node sends a packet, it labels its return address with that of its normal home address (via the Home Address Option), knowing that the home router, called the "home agent" will forward packets to it at its current "in care of" address. However this results in a routing triangle with the home agent as the third vertex. This is obviously inefficient from a router perspective, and if the difference, topologically, between a node's home address and current care of address is large, it can be very inefficient.

To deal with this, mobile IPv6 introduces the notion of a "Binding Update" (BU) message. This message informs the mobile node's correspondent that it is now really located at a different IP address, the "in care of" address, and that packets destined for it should be instead routed to the care of address. This eliminates the triangle, resulting in efficient routing.

However it introduces a security problem. An attacker can source a bogus BU message to cause a sender to route traffic for a particular recipient via the attacker's infrastructure. This can be used for denial of service (the attacker discards packets). Or it can be used to eavesdrop on traffic (the attacker peruses the packets and then forwards them on to their intended recipient).

This attack can be thwarted by using PBK. Specifically when a session is initiated, the mobile node provides its EID in the first several packets of the session. This can be done via an IPv6 option header. This EID is noted and stored by the mobile node's correspondent. Now

when the mobile node moves, it can provide its public key and send a BU signed with the corresponding private key. Note: Doing this will require changes to the BU message as currently defined in [MobileIPv6].

The correspondent can verify that the EID and public key go together by hashing the public key and verifying that the resultant hash matches the EID. It can then verify the signature on the BU using the

public key.

Once a destination learns a mobile node's (or any node for that matter) EID, it is impossible for a third party attacker to forge signed messages. If correspondents refused unsigned BUs, then it is not possible to divert traffic.

References

[RFC2914] Floyd, S., "Congestion Control Principles", RFC 2914, September 2000.

[MobileIPv6] Johson, David B., and Charles Perkins, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-13.txt, November 2000.

Moskowitz, R., "Host Identity Payload Architecture", "Host Identity Payload Protocol", http://homebase.htt-consult.com/~hip, 2001.

Full Copyright statement

Copyright (C) The Internet Society (2001). All Rights Reserved. This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on An "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.