Internet Draft
Intended status: Experimental
Expires: 15 February 2009

D. Groth
ITUA Inc.

15 August 2008

OpenPGP Attribute Extension
draft-groth-openpgp-attribute-extension-00.txt

Status of this Memo

Abstract

A RFC was accepted extending TLS usage to include OpenPGP keys (RFC 5081) as an alternative or in addition to X.509 certificates, however the author did not really standardise the way the information in OpenPGP keys was to be presented and this could be detrimental or fragment efforts to utilise OpenPGP keys in this manner.

The author didn't touch on the issue generating confidence scores beyond potential use of Certificate Authorities.

Table of Contents

1. Introduction

This document outlines ways User Attribute fields can be used, suitable for any OpenPGP keys being used in for a server purpose and the information would also be in a suitable format that computers can easily parse.

An understanding of OpenPGP (RFC 4880) is assumed by this document. Unless otherwise specified, the character set for text is the UTF-8 (RFC 3629) encoding of Unicode (ISO 10646).

2. From the Client Perspective

2.1. 6 degrees of separation in a practical sense

The PGP web of trust is in part based on the six degrees of separation principle: anecdotally, everyone in the world knows everyone else through at most six other people. Henk P. Penning has a website up that explores this very issue with OpenPGP keys, http://pgp.cs.uu.nl/plot/ and according to his calculations most keys have an average of just under six degrees of separation.

For the purpose of generating a tangible confidence rating that a host controls a particular host key we will be using arbitrary numbers. Default values of 100 points for keys marked 'I trust ultimately', 50 points for keys marked 'I trust fully', 30 points

for keys marked as 'I trust marginally', 0 points for keys marked 'I don't know' and -1 point for any keys marked 'I do not trust' are good base values although any arbitrary number should work, but may vary based on individual circumstances.

For anyone we don't know directly, we need to calculate trust paths between keys by decaying points from the second relationship outwards. Again these are arbitrary values and they can be customised based on individual needs. The general case will use a base of 75% for ultimately trusted introduction, 50% for full trusted introduction, 25% trust for marginal introduction, -1 for untrustworthy and 0 for don't know.

You follow trust paths between the local key ring and the key of the server you are intending to request information from, branching out until you get a points value of 0 or less, or find a direct path to the host key. In either case you no longer follow that branch any further.

For the system to be confident about an OpenPGP key you set the minimum points required, again this can be any arbitrary number such as 100.

2.2. Refining Confidence Scores

The system must have the ability for more finely grained control over individual scores. The default method in OpenPGP is too coarse, and doesn't easily allow you to distinguish between the capabilities of different individuals. For example you trust Bob's judgement when verifying other people holding the right keys more than most. You add an exception for Bob so that anything he trusts will be assigned 75 points instead of 50.

Alice on the other hand is gullible. While you trust Alice, you don't trust the verifications she makes. An exception is made for Alice so that anything Alice trusts will only be assigned 10 points.

In this hypothetical example, even with both Alice and Bob trusting a key your system still wouldn't hit the 100 points needed, so you obviously need to get out and make more friends.

2.3. Out of band fingerprint verification

Just as people already hold key signing parties to verify each others OpenPGP user ids, variations on this would start to appear depending on the level each party needs or wants to secure their resources. It is a reasonable assumption that not all services need strong protection, and it is up to both the administrators and those making requests or connections to those services to have the right

level of confidence that the server or service being communicated with is really who it claims to be.

For example a bank would be at more at risk and hence worth protecting more than a personal blog that gets 100 visitors a month. Banks already have a relationship with their customers and it would be easy for them to provide the fingerprint of their key(s) on business cards and other stationary items.

This process is commonly used to verify personal keys but there is no reason this concept couldn't be extended so people could also sign host keys or the main organisations key which in turn is used to sign host keys.

The worst level of confidence when connecting to another host would be no different than using self signed X.509 certificates.

2.4. Commercial Services

It is possible to leverage existing OpenPGP web of trust meta information to draw similar conclusions about the confidence that the server being sent packets is the owner of the OpenPGP key used to encrypt the request, in a similar manner people make judgements on the confidence about the server they are connecting to with their web browser owns the private key matching the X.509 certificate issued by a commercial Certificate Authority.

While the focus of this draft is on individuals making their own choices, there is nothing preventing commercial entities from offering signing services against host keys. The standard practise is for OpenPGP User ID(s) to be signed by multiple entities, and this practise could be utilised by multiple commercial entities, which would potentially increase the confidence in the key being owned by the host you send packets to.

2.5. Retrieving Meta Information

To be able to calculate confidence scores the full host keys will need to be retrieved from PGP key servers, this can be a timely process and will need to be periodically re-run to ensure signatures are still valid.

2.6. Verification of dnsNames

Before accepting such a User Attribute during use, it is a policy decision of the client to decide which sections of the Subject Alternative Name to consult (e.g. when connecting to https://example.com, a web browser may receive an OpenPGP certificate with a Subject Alternative Name UAT with two parts:

DNS:example.com and DNS:example.net; for the browser, the second part of the UAT is irrelevant).

3. Structure of Host Information in OpenPGP Keys

3.1. New User Attribute Type -- subjectAltNames

OpenPGP has for the longest time been mostly used for text based communication and file encryption, so the User ID section of keys contain a name, an email address and possibly a comment.

For computer based systems to be able to easily parse the information present, this draft assigns a new User Attribute Packet type as defined in RFC 4880, to be used for Subject Alternative Names.

This section defers options to RFC 3280, section 4.2.1.7. However this section heavily references certificate authorities and for the purposes of OpenPGP this is interchangeable with any certifying agent.

3.2. Host Names

At least one user attribute type must always exist and contain a valid dnsName for any server based keys.

The client will compare the host name it connects to with all dnsName fields present in the server key. This field can contain a fully qualified host name or a host name with a wild card character. Only one wild card character is allowed to exist per dnsName, so *.example.com is valid and would match hostname.example.com and www.example.com but would not match this.hostname.example.com.

Multiple wild card characters per host name are expressly not allowed, *.*.example.com for example should be handled by both server software and client software as an invalid key, and no software should allow the creation of such dnsNames.

4. IANA Considerations

IANA needs to assign an user attribute type as set out in this draft.

5. Conclusions

Even though this draft is specifically about using OpenPGP keys for server purposes, there is nothing special about the methods used or the way the structure of the information in OpenPGP keys is presented that would prevent such keys from being utilised for other purposes.

6. Informative References

[RFC3280] Housley, et al., " Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", Network Working Group, RFC 3280, April 2002.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[RFC4880] Callas, et. al., "OpenPGP Message Format", Network Working Group, RFC 4880, November 2007.

[RFC5081] Mavrogiannopoulos, N., "Using OpenPGP Keys for Transport Layer Security (TLS) Authentication", Network Working Group, RFC 5081, November 2007.

Acknowledgements

All the people have given valuable input, listed in no particular order:

Philipp Guehring, Daniel Kahn Gillmor, Sam Johnston and Denise Khoo.

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

Author's Addresses

Duane Groth
Internet Telephony Users Association Inc.
P.O. Box 75
Banksia NSW 2216
Australia

Email: support@e164.org

Disclaimer of Validity

Copyright Statement

Intellectual Property Statements