Network Working Group
Internet-Draft
Expires: June 21, 2008

Pars Mutaf
Institut National des
Telecommunications
December 19, 2007

Verbal Key Exchange
draft-mutaf-dke-02.txt

Status of this Memo

This Internet-Draft will expire on June 21, 2008.

Copyright Notice

Abstract

This document describes a verbal key exchange protocol in which a short fingerprint is used to represent a "one-time" public key fingerprint. The one-time public key is immediately used for key exchange, before an attacker has time to find a public/private key pair that gives the same fingerprint and mount a Man-in-the-Middle attack. The protocol, however, requires that both users be present for fingerprint verification, making it suitable for mobile users only.

Table of Contents

1. Introduction 3
2. Protocol description 3
3. Security considerations 4
4. Related work 5
5. IANA considerations 6
6. Acknowledgements 6
7. Conclusion 6
8. Informative References 6
Author's Address 7
Intellectual Property and Copyright Statements 8

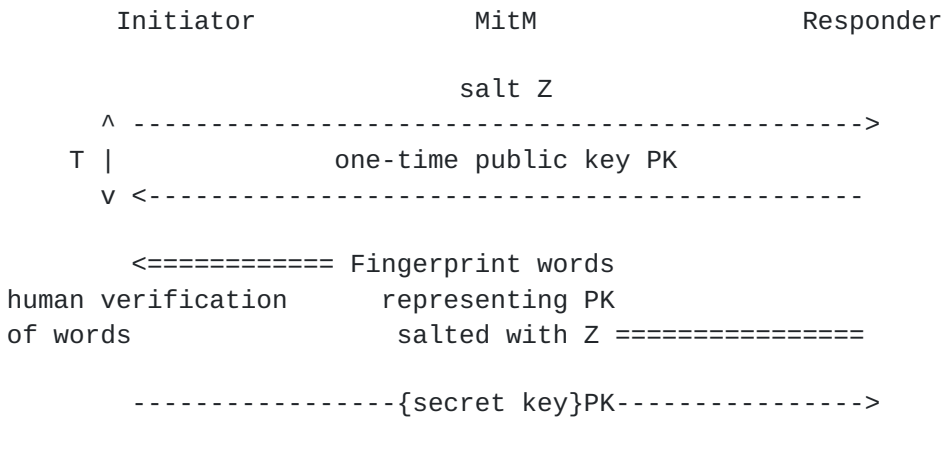
1. Introduction

Public key authentication is a difficult problem since a Public Key Infrastructure (PKI) is generally required. The problem is less challenging when two mobile users wishing to establish a security association are both present, i.e. when they meet each other. The users can verify a shared public key by comparing its "fingerprint". However, up to 160 bits long fingerprints are generally recommended today. Such a fingerprint looks like "E582 94F2 E9A2 2748 6E8B 061B 31CC 528F D7FA 8919" which is difficult to read and type by users. Simply displaying the fingerprint and assuming that the user will check it visually is not acceptable. The users must be forced to really check the fingerprint, and therefore the operation must be user-friendly.

This document describes how an easy to exchange small fingerprint can be used to authenticate a "one-time" public key. The one-time public key is immediately used for key exchange, before an attacker has time to find a public/private key pair that gives the same fingerprint and mount a Man-in-the-Middle attack.

2. Protocol description

The proposed protocol is briefly described below:



where

PK: A one-time RSA public key

==: The responder user tells the words representing the fingerprint to the initiator user through oral communication.

MitM: Man in the Middle

Figure 1

The fingerprint is represented using words from a dictionary. It is assumed that both hosts have the same dictionary containing N words. Or, the responder may return a dictionary to the initiator (TBD). Using a dictionary has two benefits. First, well-known words from a dictionary are easier to spell and understand than a 40-bit hexadecimal sequence like "E58294F2E9". Secondly, using a large dictionary containing N words, one can represent a larger number of bits per word. Each word in the dictionary will contribute log2(N) bits of entropy. If the dictionary contains N=1024 words, 4 words such as

tokyo
pizza
madonna
mercedes

can represent a 4*10=40 bits long fingerprint. The initiator user should be asked to type the same words to ensure that the verification takes place. The initiator, having the same dictionary, can reduce the verification effort using automated word completion.

3. Security considerations

The fingerprint is used to authenticate a "one-time" public key. MitM has to find a PK' giving the same fingerprint as PK, and return it to the initiator before the legitimate PK. 2^40, for example, is large enough to assume that the attacker cannot reasonably succeed. Since RSA key generation is a slow operation, an attacker may anticipate by generating and storing 2^40 public keys for all possible fingerprints. In this case, the random salt Z will force the attacker to do 2^40 fingerprint computations from the salt and the pre-computed RSA public keys. To defeat a powerful attacker having 2^40 pre-computed public keys, the fingerprint computation should preferably be a difficult task.

The fingerprint size can be increased either by increasing the number of words in the dictionary (N), or the number of read/typed words (S) by the users. The entropy per word increases logarithmically with N. Doubling the dictionary size will add only 1 bit of entropy per word. The fingerprint size increases linearly with S at the cost of reading/typing more words and hence increasing the key exchange time. Since most of the human effort will be made by the verifier typing the words read by the responder, an implementation should consider user friendly techniques e.g. word completion. Using GUI word completion making use of a keyboard and pointer, words can be entered very easily in a way that is probably acceptable to the user.

A too large dictionary will increase the word completion complexity. The initiator user will either need to type more letters to reduce the size of a list of words, or scroll over a large list for searching a word in a list. This will increase the key agreement time perceived by the responder user and the effort made by the initiator user. On the other hand, a very small dictionary will increase the number of words needed to represent a fingerprint, hence also increase the user effort.

4. Related work

In [SAS], Serge Vaudenay brings an alternative solution in which a 15-bit authentication string e.g. a 5-digit PIN code or a short hexadecimal sequence of 4 characters from {0123456789abcdef} is enough for authentication. The SAS scheme does not require public key operations for authentication and its security is orthogonal to the computational power of the man-in-the-middle. It also allows for mutual authentication and does not require a dictionary. In [MAS], the number of moves for this solution is reduced to three. [SEEING2] gives a brief description of the protocol.

Other solutions have been proposed in the literature, exploiting the presence of both users (i.e. user contact) for authentication. For example, in "Seeing is Believing", cell phones equipped with a camera, authenticate each other using a two-dimensional barcode representation of a public key. The public key is verified by taking its photo displayed on the peer device's screen [SEEING] [SEEING2].

"Loud & Clear" is another solution based on a text-to-speech engine to read an auditorially-robust, grammatically-correct sentence derived from the fingerprint of a device's public key. The text representing the fingerprint is heard from both devices equipped with speakers, and compared by the user(s). Or, alternatively, the fingerprint is heard from one device, displayed by the second device, and compared [LOUD].

"Pretty Good Privacy" uses a dictionary of words for reliable public key fingerprint transmission over a potentially noisy voice channel, in a clear unambiguous way. This is apparently inspired from the NATO phonetic alphabet used by pilots [PGPWORDLIST]. "Diceware" also uses a dictionary of 6^5=7,776 unique words that are easy to spell and remember for creating passphrases, passwords, and other cryptographic variables. Each word adds log2(7,776)=12.9 bits of entropy to the passphrase [DICEWARE].

5. IANA considerations

TBD.

6. Acknowledgements

Erik Rescorla suggested using a salt and made me aware of attacks using pre-computed RSA keys.

Michael Richardson and Nicolas Williams suggested a name like Verbal Key Exchange. Michael Richardson suggested that in IKEv2 one can authenticate the Diffie-Hellman exponent directly.

7. Conclusion

This document described a verbal key exchange protocol.

8. Informative References

[DICEWARE] The Diceware Passphrase Home Page, "http://world.std.com/~reinhold/diceware.html/".

[LOUD] Goodrich, M., Sirivianos, M., Solis, J., Tsudik, G., and E. Uzun, "Loud And Clear: Human Verifiable Authentication Based on Audio", IEEE ICDCS 2006.

[MAS] Laur, S., Asokan, N., and K. Nyberg, "Efficient mutual data authentication using manually authenticated strings", Cryptology ePrint Archive, Report 2005/424, 2006.

[PGPWORDLIST] PGP word list, "http://en.wikipedia.org/wiki/PGP_word_list".

[SAS] Vaudenay, S., "Secure Communications over Insecure Channels Based on Short Authenticated Strings", Advances in Cryptology, CRYPTO 2005.

[SEEING] McCune, J., Perrig, A., and M. Reiter, "Seeing is Believing", Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA. May 2005.

[SEEING2] Saxena, N., Ekberg, J., Kostiainen, K., and N. Asokan,

"Secure Device Pairing based on a Visual Channel",
Proceedings of the IEEE Symposium on Security and Privacy,
Oakland, CA. May 2006.

Author's Address

Pars Mutaf
Institut National des Telecommunications

Email: pars.mutaf@gmail.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).