Proposal for P1363 Study Group on
Password-Based Authenticated-Key-Exchange Methods

Bellare, Jablon, Krawczyk, MacKenzie, Rogaway, Swaminathan & Wu
February 27, 2000

ABSTRACT

We suggest standardizing methods for password-based authenticated key exchange. The scope of this effort is focused on methods where the client uses only a password; No supplementary keys or certificates are required. We believe this to be an important problem for cryptographic practice, and judge the area to be about ready for a standard.

The scope of this effort may include methods with different forms and trust models, with varying degrees of functionality. The standard will be written in a manner that describes the security goals for these methods, and presents the essential structure of these methods with respect to these goals. The standard should specify requirements for underlying primitive operations used by these methods to facilitate the use of replaceable or upgradable components where necessary and practical.

BACKGROUND OF PASSWORD-BASED AKE

Consider the scenario in which there are two entities -- a client and a server -- where the client holds a password and the server holds a function of this password. The parties would like to engage in a conversation at the end of which each holds a session key, which is known to nobody but the two of them. There is present an active adversary whose capabilities include enumerating, off-line, the words in a dictionary, this dictionary being rather likely to include the password. In a protocol we deem "good" the adversary's chance to defeat our goals will depend on how much she interacts with protocol participants -- it won't significantly depend on her expenditure of computation.

This lovely problem, password-based authenticated key exchange (AKE), was described in two papers of Bellovin and Merritt [BM92, BM93]. These authors brought forth the problem and gave the first proposed solutions.

There have been a number of subsequent suggestions for password-based AKE protocols, including the work of Steiner, Tsudik and Waidner [STW95], Jablon [Ja96,Ja97], Lucks [Lu97], Wu [Wu98], Roe, Christianson and Wheeler [RCW98], MacKenzie and Swaminathan [MS99], and Boyko, MacKenzie and Patel [BMP00]. Several of these references have taken steps to formally analyze the security of these methods.

Further work of importance includes Gong, Lomas, Needham, and Saltzer [GLNS93], who were also involved early in this topic, and recently Shoup [Sh99] and Halevi and Krawczyk [HK99]. The latter reference presents a proof that some kind of public-key cryptography is required to prevent dictionary attack in a password-based method. However, these references focus predominantly on a richer trust model, with more requirements for the client, such as the ability to store or verify the validity of a server's public key. While these added requirements are needed to meet their security goals, we instead focus on password-based methods that achieve as many of these goals as possible using only the password.

We feel that the area of password-based AKE is getting ripe for standardization. People are beginning to use and deploy these methods, and need guidance in doing so. Standards efforts in password-based AKE would help both commercial and non-commercial developers of password-based systems, many of whom do not currently know how to design strong password systems properly. Visible, widely-diseminated standards will reduce the number of weak ad-hoc systems that often result from such lack of knowledge.

Researchers also tend to keep an eye out on the world of standards to motivate their work, and a standardization effort will further fuel academic interest in this domain. Solid theoretical work is just now emerging and is likely to continue for quite a while longer.

The purpose of this effort is to define standards for the cryptographic aspects of password-based AKE, and ultimately to encourage wider standardization and use of these systems.

PROBLEM DESCRIPTION

Part of the job of the study group will be to provide solid definitions. To get things started, we provide some straw-man definitions here.

We use the term "password" to refer to any possibly low-entropy authentication key. Such keys are often derived from a secret that a person remembers, whether in the form of a PIN code, password, or passphrase. An essential goal of these methods is to help prevent brute-force attack when the password space is small, or of indeterminate size, and thus potentially small.

Password-based AKE protocols commonly have two stages: a key agreement phase, and a key confirmation phase. Key agreement is a mutual act that ends with both parties sharing a common session key, but not necessarily knowing that they share it. Key confirmation refers to steps that both parties take to verify that they share the common key. Key confirmation may be from client-to-server, server-to-client, or mutual. The scope may include protocols that don't explicitly include full mutual key confirmation. This may be desired and appropriate when the method is used in the scope of a larger system that provides the necessary confirmation. The standard must provide guidance in this regard.

The scope may also include protocols that assume either an asymmetric trust (AT) model or a symmetric trust (ST) model. In the AT model the client has a password and the server has only a particular one-way function of this password. In the ST model the client and the server both have the same data, which itself may be derived from a one-way function of the password. The significant benefit of the AT model is that a thief who steals the server's verification information must still perform a successful dictionary attack in order to masquerade as the client.

These methods may incorporate underlying cryptographic primitive functions, such as exponentiation in large finite groups, symmetric encryption functions, and one-way hash functions. The standard may identify crucial security requirements for these primitives, so as to accommodate a range of implementations. As an example of this style of modular construction, Diffie-Hellman key exchange is often defined in an abstract manner to encompass the use of a variety of finite groups.

Primary goals of the standard are to provide client-to-server authentication while providing security against dictionary attack on the password.

A more complete statement of goals is listed below. We also recognize that one of the jobs of this standards effort is to insure that these goals are clearly presented.

The focus will be on two-party password-only protocols. We will not preclude further follow-on work, but such work should not interfere with the rapid completion of a standard for the commonly used two-party model.

The standard will also encourage simplicity and efficiency in protocol selection, when all other factors are equal.

The art of crafting rigorous definitions and proofs in this domain is subtle and complex. However, even in the absence of proofs, there are obvious benefits of these methods over earlier password-only methods, and there are obvious benefits for having a formal understanding of one goals. The study group will endeavor to provide clear descriptions, and while provable security is desired, it is not a requirement for this standard.

PRELIMINARY STATEMENT OF GOALS

The standard will be a high-level one that does not emphasize specific stored or transmitted data formats. We anticipate that subsequent work will map these standard methods into specific protocols and data formats.

One job of this effort will be to provide clear descriptions and clear cryptographic requirements for these methods. To get started, we initially and informally list the following goals:

1. Security is provided against an active adversary who can direct multiple sessions between the client and server, and add, delete, or modify messages.

2. The active adversary won't be able to obtain information about the password more effectively than by direct on-line guessing -- interactively trying the most likely passwords, in order (security against offline dictionary attacks).

3. Learning already distributed session keys won't help the adversary (security against "Denning-Sacco attack").

4. If the adversary learns the client's password or the server's long-term password-verifier, still the adversary won't be able to ascertain anything about previously distributed session keys ("forward secrecy").

5. A passive adversary (eavesdropper), even after learning the password, won't be able to ascertain anything about session keys.

6. If the adversary learns the password for a specific server, the adversary will still have to perform a dictionary attack in order to impersonate the client to the server, or to impersonate another server to the client (Only applies in the asymmetric trust model).

We recognize that the omission of goal 6 may be desirable in some cases to achieve an increase in efficiency for methods in a symmetric trust model.

LIMITATIONS

We'd like to be clear about the following limitations on these methods:

1. Direct on-line guessing is always possible. We presume the server will take any necessary measures to limit direct guessing to minimize this threat. Such measures are beyond the scope of these cryptographic protocols.

2. If the server is compromised and a hashed-password verifier is revealed to an attacker, dictionary attack is unavoidable. The cost of the attack will be directly proportional to the entropy of the password, and the cost of computing the hash function.

EVALUATING PROPOSALS

For the purpose of illustration, and initial focus for the group, several methods have already been presented to the P1363 group for study. These and subsequent methods will be reviewed as appropriate, and a set of methods will be defined to achieve our goals using a variety of forms and a variety of underlying cryptographic primitives. Other criteria for protocol selection may come from the broader P1363 effort.

Much of the work in this area springs from ideas of Bellovin and Merritt [BM92,BM93]. In addition to the specific suggestions made to the P1363 group, the body of other follow-on work includes protocol suggestions by [STW95, Ja96, Ja97, Lu97, MS99, Wu98, RCW98, BESW00, and BMP00].

In choosing a password-based AKE protocol, the following characteristics are desirable. This list is not exhaustive and neither rigidly proscriptive.

1. The protocol may use an asymmetric trust model, where the client key is different from the server key, with the former being hard to compute from the latter.

2. The protocol may use a symmetric trust model where the client key is the same as, or computationally equivalent to, the server key.

3. The protocol should support a variety of underlying groups, when possible, such as subgroups of Z_p^* and various elliptic curve groups.

4. The protocol should be simple -- as simple as possible.

5. The protocol should provide some form of time-limited sensitivity to stolen long-term secrets (e.g. "forward secrecy").

6. The protocol may support a variety of "flow architectures" (that is, who speaks to whom when).

7. The protocol should be efficient in several measures: number of flows, length of these flows, computational cost at the server, computational cost at the client.

8. It is desirable that a protocol be supported by proofs. Without verifiable proofs, the usual peer review process will be used.

It is recognized that tradeoffs may exist in trying to achieve multiple desired characteristics. The standard should be sufficiently flexible to accommodate a range of anticipated uses for these methods.

WHY STANDARDIZE PASSWORD-BASED AKE PROTOCOLS?

What makes password-based authentication of so much interest is that it affords very strong guarantees using a very simple trust model based on a weak authenticator. This trust model is in fact the predominant trust model used in person-to-computer authentication. It is thus significant that good security properties may be achieved using nothing but a tiny password. In particular, these methods use no sort of public-key infrastructure. There are no certificates involved, and no certification authorities.

In light of this, some may fear that password-based AKE is incompatible with public-key infrastructure. Quite the opposite is true. Password-based protocols provide extra assurance when, for example, a certificate is forged or goes unverified by the client. If the client and server carry out a password-based AKE encrypted under the server's public-key, then client does not relinquish his password even if the server's certificate should turn out to be invalid, or if the client neglected to check it.

Besides the growing amount of academic work in this area, current interest in commercial and non-commercial applications is growing. One of the authors of this paper is associated with a company that focuses specifically on password-based AKE technology, and which maintains educational pages for this field at its web site.

The standard will be designed to provide a wider understanding of these problems and solutions, to encourage a variety of applications. Prominent evolving standards like TLS, Kerberos, HTTP, SSH, and IPSec, may be motivated to take advantage of password-based AKE methods.

REFERENCES

[BPR00] M. Bellare, D. Pointcheval and P. Rogaway.
Authenticated Key Exchange Secure Against Dictionary Attack.
To appear in Eurocrypt 2000.

[BM92] S. Bellovin and M. Merritt.
Encrypted Key Exchange: Password-Based Protocols Secure against Dictionary Attacks.
Proceedings of the Symposium on Security and Privacy, pages 72-84, IEEE, 1992.

[BM93] S. Bellovin and M. Merritt.
Augmented Encrypted Key Exchange: A Password-Based Protocol Secure against Dictionary Attacks and Password File Compromise.
Proceedings of the 1st Annual Conference on Computer and Communications Security, ACM, 1993.

[BMP00] V. Boyko, P. MacKenzie and S. Patel.
Provably Secure Password Authenticated Key Exchange Using Diffie-Hellman.
To appear in Eurocrypt 2000.

[BESW00] P. Buhler, T. Eirich, M. Steiner, M. Waidner.
Secure Password-Based Cipher Suite for TLS.
Proceedings of Network and Distributed Systems Security Symposium
February 2000.

[GLNS93] L. Gong, M. Lomas, R. Needham, and J. Saltzer.
Protecting Poorly Chosen Secrets from Guessing Attacks.
IEEE Journal on Selected Areas in Communications, 11(5):648-656, June 1993.

[HK99] S. Halevi and H. Krawczyk.
Public-Key Cryptography and Password Protocols.
February 1999. Earlier version in *Proceedings of the 5th CCS*.
ACM Press, New York, 1998.

[Ja96] D. Jablon.
Strong Password-Only Authenticated Key Exchange.
ACM Computer Communications Review, October 1996.
Available from http://www.integritysciences.com/links.html#jab96

[Ja97] D. Jablon.
Extended Password Key Exchange Protocols Immune to Dictionary Attacks.
Proceedings.of WET-ICE '97, pages 248-255. IEEE Computer Society, June 1997. Available from http://www.integritysciences.com/links.html#jab97

[Lu97] S. Lucks.
Open Key Exchange: How to Defeat Dictionary Attacks Without Encrypting Public Keys.
Proc. of the Security Protocols Workshop, LNCS 1361, Springer-Verlag, Berlin, 1997.

[MS99] P. MacKenzie and R. Swaminathan.
Secure Authentication with a Short Secret.
Manuscript. November 2, 1999.
Earlier version as Secure Network Authentication with Password Identification, Submission to IEEE P1363a. August 1999.
Available from http://grouper.ieee.org/groups/1363/addendum.html

[RCW98] M. Roe, B. Christianson and D.Wheeler.
Secure Sessions from Weak Secrets.
Technical report from University of Cambridge and University of Hertfordshire, 1998. Submitted to *Operating Systems Review.*

[Sh99] V. Shoup.
On Formal Models for Secure Key Exchange (version 4)
Manuscript, November 15, 1999. Proceedings version in *ACM Computer and Communications Security*, 1999.

[STW95] M. Steiner, G. Tsudik and M. Waidner.
Refinement and Extension of Encrypted Key Exchange.
Operating Systems Review, vol. 29, Iss. 3, pp. 22-30 July 1995.

[Wu98] T. Wu.
The Secure Remote Password Protocol.
Proceedings of the Internet Society Symposium on Network and Distributed System Security, pages 97--111, 1998.

AUTHORS

Mihir Bellare
Dept. of Computer Science & Engineering
University of California at San Diego
9500 Gilman Drive, La Jolla, CA 92093, USA
E-Mail: mihir@cs.ucsd.edu
URL: http://www-cse.ucsd.edu/users/mihir

David Jablon
Integrity Sciences, Inc.
+1 508 898 9024
E-mail: dpj@world.std.com
URL: http://www.IntegritySciences.com

Hugo Krawczyk
Dept of Electical Engineering
Technion -- Israeli Institute of Technology
Haifa 32000
Israel
E-mail: hugo@ee.technion.ac.il

Philip MacKenzie
Bell Laboratories, Room 2A-368
Lucent Technologies
600 Mountain Ave
Murray Hill, NJ 07974
E-mail: philmac@lucent.com
URL: http://www.bell-labs.com/user/philmac

Phillip Rogaway
Dept. of Computer Science, Engineering II Bldg.
University of California at Davis
Davis, CA 95616, USA
E-mail: rogaway@cs.ucdavis.edu
URL: http://www.cs.ucdavis.edu/~rogaway

Ram Swaminathan
Bell Laboratories, Room 2A-352
Lucent Technologies
600 Mountain Ave
Murray Hill, NJ 07974
E-mail: swaram@lucent.com
URL: http://www.bell-labs.com/user/swaram

Tom Wu
Arcot Systems, Inc.
E-mail: tom@arcot.com
(650) 565-7007