Management, Enterprise and Benchmarking in the 21st Century
Budapest, 2017

Password Based Cryptography

Nertila Hoxha

Óbuda University, Donát Bánki Faculty of Mechanical and Engineering, Hungary

nertila.hoxha@fti.edu.al

Abstract: A password is not just a word or string of characters but is the most important factor used for user authentication to prove identity or access approval to gain access to a resource, which is to be kept secret from those not allowed access. As passwords are often chosen without paying much attention special care is required in the process of protection from attacks. A lot of systems attempt to derive a cryptographic key directly from a password and this is to dangerous for the security of users accounts. Password based cryptography is usually defined as some form of guarantee against brute force attacks.
Nowadays exist many approaches about password based cryptography and a lot of researchers have given their contribution in this field. My aim is to analyze these approaches and to find the best techniques used for this kind of cryptography. We will see that some techniques should be improved and some other are relatively expensive.

Keywords: password based cryptography, public key cryptography, encryption schemes, protocols

1 Introduction

In security protocols sometimes password and other weak secretes serve as cryptographic keys. Early research on the design and analysis of protocols based on weak secrets are focused on techniques for defending against guessing attacks . These techniques basically aim to ensure that plaintexts encrypted under passwords do not contain redundancy that can later be used to verify a password guess. [1] While this is a helpful guideline, its informal application need not guarantee security. As experience demonstrates conjecturing the security of a protocol, or arguing it only heuristically, is not sufficient. There are two approach for analyzing security protocols.
The first approach is a formal methods or a symbolic approach. This approach adopts an theoretical view of executions. Messages are designed as elements of a term algebra constructed with symbolic operations that represent various cryptographic primitives. Parties operate on terms using a limited number of inference rules, sometimes generically known as the Dolev-Yao rules. The rules reflect a common understanding of the security of cryptographic primitives. For

example, they say that the message encrypted in a ciphertext can be recovered only if the appropriate decryption key is known. Quite often, proofs that rely on these rules can be mechanized. Work done on symbolic models for password-based protocol has concentrated on extending the Dolev-Yao rules to guessing attacks.
The second approach is the computational approach. It uses a concrete (bit level) representation, for protocol executions. The attacker is modeled as a powerful, arbitrary probabilistic polynomial-time Turing machine. Although proofs with this approach tend to be lengthy, difficult, and tedious, it is generally accepted that it provides strong guarantees. For the case of password-based protocols, work with the computational approach seems to have focused almost exclusively on the important use of passwords for authenticated key exchange. This work includes designing models and giving provably secure developments. Unusually, the security of password based encryption as a primitive has not been addressed.
In this paper I want to do the analyze of protocols based on passwords using the cryptographic primitives such as symmetric encryption, asymmetric encryption, and encryption that uses passwords as keys. The first primitive is symbolic and it is based on an extension of the classical Dolev-Yao inference rules to include password-based encryption. The second primitive is computational and it is based on concrete implementations of the encryption operations. In security protocols, password-based encryption commonly servers for attaining authenticity instead than secrecy properties, although the use of the term “encryption”.

2 Related Work

Regarding password based cryptography field there are many approaches and techniques developed by researchers both in practice and theory. As you can see above are mention some related work in this area.

A general approach to password based cryptography is given by Morris and Thompson. A method for protecting password tables is to combine a password with a salt to produce a key. The password derived a set of keys and the salt can be viewed as an index into this set and is not necessary to kept secret. [2]

Another approach is to construct key derivation techniques including [2] iteration count in the key derivation technique of to indicate how many times to iterate some underlying function by witch keys are derived. In a password based key derivation function the base key is a password and the other parameters are a salt value or an iteration count.

Password based message authentication is another method of cryptography. MAC confirm that the message send by sender has not been change during the way from sender to receiver. This method provides one key for the server and one for the client and both of them are known only from that specific server and that specific client.

Hash-based message authentication code (HMAC) maintains one private key for the server and one for the client and this private key that known only to that specific server and that specific client. A unique HMAC is created by the client side, per demand to the server by hashing the request data with the private keys and posting it as part of a request. HMAC is more secure than Message Authentication Code (MAC) because the key and the message are hashed in independent steps. [3]

For generating a key from a password from hashing tables the technic of password based key derivation use a simple protocol for deriving a key from a password via hashing tables ,implements a pseudorandom function, such as hash-based message authentication code (HMAC), to the input password ahead with a salt value and to do the process a lot of times to create a *derived key*, which can then be used as a cryptographic key in consequent operations. The supplemental computational work creates password cracking much more difficult, and is known as key stretching. The number of iteration when the standard was written in the year 2000 was minimum 1000 ,and the parameter is destined to be increased over time as CPU speeds raise. In 2005 a Kerberos standard suggested 4096 iterations, [4]Apple iOS 3 used 2000, iOS 4 used 10000, [5] while in 2011 LastPass used 5000 iterations for JavaScript clients and 100000 iterations for server-side hashing. [6]Adding a salt to the password decreases the ability to use pre calculated hashes (rainbow tables) for intruders, and means that multiple passwords have to be proved one by one, not all at once. The standard suggests a salt length of at least 64 bits.

Password based Encryption method is based on the use of password derived keys for symmetric encryption scheme. This method provides a secure channel for password derived keys and also offers a good authentication. Password based encryption can be used as a protocol. [7] For a strong authentication various cryptographic protocols depend on passwords chosen by users. The users chose short and easily memorable passwords and in these cases the protocols are vulnerable to a dictionary attack because the space of passwords is small enough to be identified by an attacker. It is more effective then to create password-based protocols that prevent off-line dictionary attacks. [8] Was Gong et al. [9] the first that has study the password-based protocol problem. He used public-key encryption to watch across off-line password-guessing intrusions. Another important work[9] , which became the basis for many subsequent works is it of Bellovin and Merritt named Encrypted Key Exchange (EKE). SPEKE [10] and SRP [11] [12]are two protocols included in this work, but also exist a lot of papers who stady these protocols [13] [14] [15]. The model for the password-based protocol problem presented by Bellare et al. [16] represent a model for the password-based protocol problem and demand that their model is rich enough to deal with password guessing, breaking secrets, server compromise, and loss of session keys. Then based in many works the ideal-cipher model (random oracles) and the two-flow protocol at the core of EKE are secure. In their proposal to the IEEE P1363 Bellare and Rogaway [17] presented many instantiations (AuthA) of the ideal-cipher . A simplified version of

AuthA is suggested by Bresson et al. [18] named One-Encryption-Key-Exchange (OEKE), and demonstrate that OEKE attain good security against dictionary intrusions in both the random oracle and ideal-cipher models under the computational Diffie–Hellman. Is Bellare that presented the ideal-cipher model. In this model $|G| = |C|$, and selecting a random function h from Ω amounts to giving the protocol (and the attacker) a perfect way to encipher strings in G: namely, for $K \in \{0, 1\}*$, we set $EK : G \rightarrow C$ to be a random bijective function, and we let $DK : \{0, 1\}* \rightarrow G$ defined by $DK(y)$ be the value x such that $EK(x) = y$, if $y \in C$, and undefined otherwise.

3 Password-based encryption protocols

Password-based encryption protocols are designed to be secure even when the secret key or password shared between two users is drawn from a small set of values. [19] Some of these protocols are subject of guessing attacks and in these attacks may succeed that the adversary can reveal the password shared between two users during a online conversation.

A theory developed and applied to provides security is the theory of multi-instace (mi) that offers the first proof-based support for the classical practice of salting in password-based cryptography. [20] Multi-instance security used only for a single instance aim to ensure security but represents a second line of defense . Mi-security as password based encryption is based on the PKC#5 [21] and encrypts a message M with a password pwd by choosing a random x bit salt sa, by extracting a key $L \leftarrow KD(pw||sa)$ and turning back $S' \leftarrow S||sa$ where $S \leftarrow\$ E(L,M)$. E is a symmetric encryption scheme, (KDF) is the key-derivation function, and KD: $\{0, 1\}* \rightarrow \{0, 1\}n$ is the s-overlap iteration KD = Hs of a cryptographic hash function H: $\{0, 1\}* \rightarrow \{0, 1\}n$. [9]

The most of passwords chosen by people are often very week, However, passwords are often poorly chosen, dropping within a set D called a “dictionary” that is small enough to drain. The target password pwd can be recover by a brute-force attack (breaking the security of the encryption) using sN hashes where $N = |D|$ is the size of the dictionary. Increasing s increments this achievement, describing the role of this iteration count, but s cannot be made too large without skeptically impacting the performance of password based encryption.[9]

Different from the previous work Mi-security offers many application in the real world and is not a theoretically method. The explanation of mi-security provided for key derivation function is a simulation-based one motivated by indifferent frameworks [22] [23]. Exist two type of attackers, that in the real word and that in an ideal counterpart but in both, target passwords $pwd1, \ldots, pwdm$ and salts $sa1, \ldots, sam$ are randomly selected. In the real world, the attacker gets input ($pwd1$, $sa1$,KD($pw1||sa1$)), . . . , ($pwdm$, sam,KD($pwdm||sa1$)) and also gets an oracle for the RO hash function H used by KD [9]. In the ideal counterpart, the input is ($pwd1$,

*sa*1,*L*1), . . . , (*pwdm, sam*,*Lm*) where the keys*L*1, . . . ,*Lm* are casually chosen, and the oracle is a simulator. The simulator used in this case can take a **Test** oracle that will steal a guess for a password and notify the simulator where it matches one of the target passwords. Necessarily, we need that when the number of queries creating by the attacker to the simulator is *y* and the number of queries creating by the simulator to its **Test** oracle is *y/s*. This constraint is critical to our proof of security amplification and a source of challenges in the proof.[9] Let turn to our main application, that of password based encryption as explain in PCSC#5 [10] where a conventional mode of operation CBC mode is combine with a password-based key derivation function (KDF).
Officially , a (*k, x, c*)-KDF is a deterministic map KD: *{*0, 1*}∗* × *{*0, 1*}x* →*{*0, 1*},k* t make use is a basic ideal primitive, *s* is the iteration count, which gives the multiplicative increment in work that should slow down brute force attacks.PKCS#5 describes two KDFs [10]. Based in this two models we can create a function Encode (*pwd, sa*) that explain how to encode its inputs onto *{*0, 1*}∗* with easly calculable inverse Decode(*W*).

3.1 Password - based encryption schemes

A password based encryption scheme is a symmetric encryption scheme where the keys are passwords and key generation is a password sampling algorithm. [9]Let KD be a (*k, x, s*)-KDF and let SE = (*K, E,D*) be an encryption scheme with *K* outputting consistently choose *k*-bit keys. Then we describe the password based encryption scheme *SE*[KD, SE] = (*P, E,D*) as pursue. Encryption *E*(*pwd,M*) is done via *sa*←$ *{*0, 1*}x* ; *K* ←KD(*pwd, sa*) ; *S* ←$ *E*(*K,M*), returning (*sa*,) as the ciphertext. Decryption recompense the key *K* by repeating the key derivation function and then put *D*. If the key derivation function is KD1 and the encryption scheme is CBC mode, then one acquire the first password based encryption scheme from PKCS#5 [10].

4 Security of Password Based Encryption

Another important element for password based encryption is the security and after analyzing the protocols and schemes we can analyze the security of password based encryption as used in PKCS#5. To measures the security of Mi -security we use the following theorem.
Theorem 1 Let $m \geq 1$, let *SE*[KD, SE] = (*P, E,D*) be the encryption scheme built from an (*k, x, s*)- KDF KD and an encryption scheme SE = (*K, E,D*) with *k*-bit keys.[9]
This theorem to measure the security uses the multi-user left-or-right security approach from ,when given access to multiple left-or-right oracles each using the same bit *b*.

Let be A an attacker A that can make $\rho 14$ queries to **Enc**$(i, \cdot, \cdot)$ for each $i \in \{1, \ldots, m\}$ and creating at most $qc < m$ corruption queries, S a c-amplifying simulator. Then we have one message sampler M and attackers D, C, and B . To test the security and to find qc corruption queries : C creates a single query **Enc**$(i, \cdot, \cdot)$ for each $1 \leq i \leq \rho$.
Also , C's executing time equals $tA+q \cdot tS$ plus a small, absolute constant, and where tA is the executing time of A, and tS is the time needed by S to answer a query. Decisively , $\gamma(M,m\rho) \leq m2\rho 2/2s$. In conclusion the theorem have a capacity to hold even when SE is only one-time secure ,which involves that the tests covers tools such as WinZip [24].

Conclusion

In this paper we presented several approach about password based cryptography and the results of our analysis show that each method has its weaknesses. Is very important to be careful when designing or implementing password-based protocols and if we want to have security we should choose a strong password. A strong password and an good method of cryptography are the best technique for more security. For a cryptosystem, the objective is to find a virtual private key from a set of weak passwords held in deferent points, and this key should be strong and resistant to intrusions as any regular key. After the key can be used in a distributed manner without ever demanding its actual reestablishment. I proposed that such functionalities in the cryptography model should justifying all the design choices along the way of implementing them.

References

[1] Martin Abadi Bogdan Warinschi, "Password-Based Encryption Analyzed,".

[2] B. Kaliski, "Password-Based Cryptography Specification," 2000.

[3] Techtarget Network. [Online]. http://searchsecurity.techtarget.com/definition/Hash-based-Message-Authentication-Code-HMAC

[4] Kenneth Rae, "Advanced Encryption Standard (AES) Encryption for Kerberos 5,".

[5] Advanced Password Cracking – Insight (ElcomSoft). Smartphone Forensics: Cracking BlackBerry Backup Passwords .

[6] LastPass Security. [Online]. https://blog.lastpass.com/2011/05/lastpass-security-notification.html/

[7] Grégory Demay, Peter Gaži, Ueli Maurer, Björn Tackmann, "Per-Session Security, Password-Based Cryptography Revisited," , 2016, p. 32.

[8] D. Pointcheval, P. Rogaway M. Bellare. (2000) Authenticated key exchange secure against dictionary attacks, Lecture Notes.

[9] L. Gong, M. Lomas, R. Needham, J. Saltzer, "Protecting poorly chosen secrets from guessing attacks," , 1993, p. 8.

[10] D. Jablon. Strong password-only authentication key exchange.

[11] T.Wu, "The secure remote password protocol," in 1998 Internet Society Symp. on Network and Distributed Systems Security, San Diego, p. 4.

[12] T.Wu. SRP6: Improvements and refinements to the secure remote password protocol.

[13] P. Buhler, T. Eirich, M. Steiner, M. Waidner, "Secure password-based cipher suite for TLS," in *Network and Distributed Systems Security*, 2000.

[14] S. Halevi, H. Krawczyk. Public-key cryptography and password protocols, ACM Trans. Inform. System Security.

[15] S. Lucks, "Open key exchange: how to defeat dictionary attacks without encrypting public keys," in *Security Protocols Workshop*.

[16] D. Pointcheval, P. Rogaway M. Bellare. (2000) Authenticated key exchange secure against dictionary attacks Lecture Notes.

[17] M. Bellare, P. Rogaway. The AuthA protocol for password-based authenticated key exchange.

[18] E. Bresson, O. Chevassut, D. Pointcheval, "Security proofs for an efficient password-based key exchange," in *10th ACM Conf. on Computer and Communications Security*, 2003, p. 9.

[19] Michel Abdalla, Pierre-Alain Fouque, David Pointcheval, "Password-Based Authenticated Key Exchange," in *International Workshop on Theory and Practice in Public Key Cryptography*

[20] Mihir Bellare Thomas Ristenpart Stefano Tessaro, "Multi-Instance Security and its Application to Password-Based Cryptography," in *CRYPTO 2012*, 2013, p. 30.

[21] "PKCS #5: Password-based cryptography standard (rfc 2898)," in *RSA Data Security, Inc.*, 2000.

[22] J.-S. Coron, Y. Dodis, C. Malinaud, P. Puniya, "How to construct a hash function," in *Advances in Cryptology*, editor In V. Shoup, Ed., 2010.

[23] U. M. Maurer, R. Renner, C. Holenstein, "Indifferentiability, impossibility results on reductions, and," in *1st Theory of Cryptography*, 2004, p. 18.

[24] T. Kohno, "Attacking and repairing the winZip encryption scheme," in *11th Conference on Computer and Communications Security*, 2004, p. 9.

[25] B. Kaliski, "Password-Based Cryptography Specification," 2000.

[26] "Multi-Instance Security and its Application to Password-Based Cryptography," , 201, p. 30.

[27] M. Bellare, A. Boldyreva, and S. Micali, , Advances in Cryptology , Ed., 2000.

[28] Zhu Zhao, Zhongqi Dong,YonggeWang, "Security analysis of a password-based authentication protocol proposed to IEEE 1363," , 2005, p. 8.

[29] S. Bellovin, M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks," in *1992 IEEE Computer Society Conf. on Research in Security and Privacy*, p. 8.