Cryptanalysis of the Secure Sessions from Weak Secrets Protocols

Jolyon Clulow

Computer Laboratory, University of Cambridge
JJ Thompson Av., CB3 0FD, UK (Email: jolyon.clulow@cl.cam.ac.uk)

(Received June 24, 2005; revised and accepted July 25, 2005)

Abstract

The Short Secret Sharing Protocols (S3P), proposed by Roe *et al* in 1998 [13] and revised in 2003 [14], is a family of protocols that bootstrap secure session keys from weak secrets such as passwords. In this letter, we describe an attack against the RSA variants of the S3P protocols. The attacker can successfully masquerade as one of the participants, establish a new session, and gain knowledge of the session key. We present possible modifications to the protocol to prevent such an attack.

Keywords: Cryptanalysis, password, security protocol

1 Introduction

One of the most significant and practical challenges in computer security is enabling human users to securely access their authorised computer systems and data remotely. In the absence of secure local storage and secure password generators, the possible solutions to this challenge are limited by the innate inability of humans to remember cryptographically strong secrets. Password based systems are the typical examples of a weak secret being used to establish authentication and secrecy properties. They are weak in the sense that passwords are chosen from a searchable set. Significant effort [1, 2, 3, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15] has been invested researching this problem; seeking secure and efficient ways to transform the weak initial password into strong cryptographic security properties. Boyd and Mathuria provide a useful survey in [4].

This research analyses the protocols proposed by Roe *et al.* in [13] and revised in [14] that bootstrap secure session keys from weak secrets. The three protocols are based on RSA, Diffie-Hellman and El-Gamal respectively, and are known as S3P. The authors of S3P claimed that, apart from being simpler and quicker than their predecessor protocols in the literature, they have slightly stronger security properties. In this work, we describe an attack against the RSA variants of the S3P protocols. The attacker can successfully masquerade as one of the participants, establish a new session, and gain knowledge of the session key. We present possible modifications to the protocol to prevent such an attack.

2 Review of the RSA Variant of the Secure Sessions from Weak Secrets Protocol

We first review the original description of the RSA variant of S3P as presented in [13] and shown in Figure 1.

$$
\begin{array}{lll}
1. & A \longrightarrow B: & N \\
2. & B \longrightarrow A: & z^{e(k)} \bmod N \\
3. & A \longrightarrow B: & n_a \\
4. & B \longrightarrow A: & n_b
\end{array}
$$

Figure 1: The original RSA variant of S3P

Alice generates an RSA modulus $N = pq$ with primes p, q chosen so that $(p-1)/2$, $(q-1)/2$ each contain a large prime factor. The modulus N is transmitted to Bob as the first message in the protocol. We assume that there is a publicly known function e that converts a password k into a large prime number $e(k)$ suitable for use as an RSA exponent. We define the plaintext $z = c|s|n_a|n_b$ where s is the session key, c is a strong random number called a confounder, and n_a, n_b are random nonces. Bob randomly generates z and then encrypts it using $e(k)$ as the public exponent and submits it to Alice. Alice, with knowledge of p, q and k, calculates $e(k)$ and the corresponding private exponent $d(k)$ such that $e(k) \cdot d(k) = 1 \bmod \phi(N)$. Alice can then recover the plaintext value of z and proves this to Bob by returning the nonce n_a. Bob confirms the value of n_a and proves to Alice that it was he who generated z by returning the value n_b. Alice and Bob accept s as the session key for further communication. It is vital that there be no redundancy in the plaintext $z = c|s|n_a|n_b$ that is encrypted; an attacker could use this information to search for k.

A revised version of the protocol designed to protect against a Bleichenbacher type attack is described in [5, 14] and differs in only the second message communicated (see Figure 2).

1. $A \longrightarrow B :$ N
2. $B \longrightarrow A :$ $z^{e(k)} + 2^{e(k)} \bmod N$
3. $A \longrightarrow B :$ n_a
4. $B \longrightarrow A :$ n_b

Figure 2: The revised RSA variant of S3P

3 Cryptanalysis of the RSA Variant of the Secure Session from Weak Secrets Protocol

The attack on the RSA variant of S3P is shown in Figure 3. An attacker, Eve, masquerades as Bob. Alice sends Eve the RSA modulus $N = pq$ for which Alice knows the primes p, q. Eve replies with the value $N - 1$. As before, Alice calculates the private exponent $d(k)$ which she uses to decrypt the message as $(N - 1)^{d(k)} = N - 1 \bmod N$ and obtains the value $N - 1$ which she interprets as $N - 1 = c|s|n_a|n_b$. She sends n_a to Eve. Eve knows that Alice has recovered the value $z = N - 1$ and so knows and can respond with the value n_b that Alice expects. The protocol has completed without any parties registering an error. Note that Eve could also have chosen 1 instead of $N - 1$.

1. $A \longrightarrow E :$ N
2. $E \longrightarrow A :$ $N - 1$
3. $A \longrightarrow E :$ n_a
4. $E \longrightarrow A :$ n_b

Figure 3: The attack on the RSA variant of S3P

Alice incorrectly believes the following: she has verified that she is communicating with Bob; Bob has identified himself by proving he has knowledge of k; finally, she has securely established a strong session key s with Bob. We note that this attack does not compromise the initial weak secret k but leads to establishment of a known session key.

This attack succeeds for two reasons. Firstly, the requirement that z contain no redundancy makes it impossible to check for forged values of $z^{e(k)}$. Further, it is not true that RSA encryption $E(z) = z^{e(k)}$ for a given exponent $e(k)$ is a one-way function. Notably, for the values 0, 1 and $N - 1$ of $E(z)$, the corresponding input can be calculated. A sanity check could be applied to test for the input values 0, 1 and $N - 1$ reduced modulo N.

An equivalent attack prevails against the following modified version of the protocol [5, 14] shown in Figure 4. This time Eve sends the value zero 0 to Alice who calculates $z = (0 - 2^{e(k)})^{d(k)} = N - 2$. Eve thus knows the value of n_b and the new session key s. In addition, Eve has succeeded in convincing Alice that she has established a secure session with Bob. Again, the attack does not extend to compromising the initial weak secret k.

1. $A \longrightarrow B :$ N
2. $B \longrightarrow A :$ $z^{e(k)} + h(k, i) \bmod N$
3. $A \longrightarrow B :$ n_a
4. $B \longrightarrow A :$ n_b

Figure 4: The modified RSA variant of S3P

4 Possible Solutions

We define a pseudo random function $h(k, i)$ that outputs $\lceil \log_2 N \rceil$ bits such that i is the minimum natural number for which $h(k, i) < N$. Using this function, we modify the protocol to ensure one-wayness.

5 Conclusion

In this letter, we have shown that both the original and revised versions of the RSA variant of the proposed S3P protocol suite are vulnerable to an impersonator attack. The attacker can successfully masquerade as one of the participants, establish a new session and gain knowledge of the session key. We present possible modifications to the protocol that prevent such an attack

References

[1] R. Anderson, M. Lomas, "Fortifying Key negotiation Schemes with Poorly Chosen Passwords", *Electronics Letters,* vol. 30, no. 13, pp. 1040–1041, 1994.

[2] S. Bellovin, M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks", in *IEEE Symposium on Research in Security and Privacy,* pp. 72–84, 1992.

[3] S. Bellovin, M. Merritt, "Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and passwordfile compromise", in *ACM Conference on Computer and Communications Security,* pp. 244–250, 1993.

[4] C. Boyd, A Mathuria, *Protocols for Key Establishment and Authentication*, Springer-Verlag, 2003.

[5] B. Christianson, *Personal Communication*, 29 June 2004.

[6] L. Gong, "Optimal authentication protocols resistant to password guessing attacks", in *Proceedings of 8th IEEE Computer Security Foundations Workshop*, pp. 24–29, 1995.

[7] L. Gong, M. Lomas, R. Needham, J. Salzer, "Protecting poorly chosen secrets from guessing attacks", *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 5, pp. 648–656, 1993.

[8] Y. Hwang, D. Yum, and P. Lee, "EPA: an efficient password-based protocol for authenticated key exchange", in *ACISP*, LNCS 2727, pp. 452–463, Springer-Verlag, 2003.

[9] IEEE P1363.2, *Password-Based Public-Key Cryptography,* http://grouper.ieee.org/groups/1363/ passwdPK/index.html

[10] D. Jablon, "Strong password-only authenticated key exchange", *ACM Computer Communications Review*, vol. 26, pp. 5–26, May 1996.

[11] D. Jablon, "Extended password key exchange protocols", in *WETICE Workshop on Enterprise Security*, pp. 248–255, 1997.

[12] T. Kwon, "Authentication and key agreement via memorable password", in *ISOC Network and Distributed System Security Symposium*, pp. 73–85, 2001.

[13] M. Roe, B. Christianson, D. Wheeler, *Secure Sessions from Weak Secret*, Technical Report UCAM-CL-TR-445, Computer Laboratory, University of Cambridge, 1998.

[14] M. Roe, B. Christianson, D. Wheeler, "Secure Sessions from Weak Secret", in *Security Protocols Workshop 2003*, LNCS 3364, Springer-Verlag, 2005.

[15] T. Wu, "Secure remote password protocol", in *ISOC Network and Distributed System Security Symposium*, pp. 97–111, 1998.

Jolyon Clulow Jolyon Clulow is reading for a Ph.D. in the security group at the Computer Laboratory, University of Cambridge. His research interests include security APIs, secure coprocessors, financial security and cryptography.