An Image Based Authentication System- Using Needham Schroeder Protocol

Raman Kumar[1], Asmita Puri [2],Vivek Gautam [3] and Saumya Singla[4]

[1,2,3,4] Department of Computer Science and Engineering,
[1,2,3,4] D A V Institute of Engineering and Technology, Jalandhar, Punjab, India.

Summary
With the upcoming technologies available for hacking text based passwords, there is a need to provide users with a secure environment that protect their resources against unauthorized access by enforcing control mechanisms. To counteract the increasing threat, Image Based Authentication (IBA) has been introduced. Apart from being more secure than usual text based passwords, IBA has proved to be an asset as it is user friendly. IBA generally encapsulates the Needham Schroeder Protocol (NSP) and provides client a completely unique and secured authentication tool to work on. This paper however proposes a hypothesis regarding the use of Needham Schroeder Protocol and is a comprehensive study on the subject of using images as the password set. This forms the basis for a secure communication between the communicating entities. The assortment of image set as client's password set aims at thwarting reply attacks. The paper also evaluates the performance of this method in terms of its efficiency and time taken. Password authentication protocols are important mean of user authentication on network. Several password authentication protocols have been introduced each claiming to withstand to the several attacks, including replay, password file compromise, denial of service, etc. Then, we present an improvement to the Needham-Schroeder Protocol, in order to remove two possible attacks. Therefore, the proposed scheme is secure and efficient against notorious conspiracy attacks.

Key words:
Image Based Authentication (IBA), Needham Schroeder Protocol (NSP), Protocol, Attacks, Shoulder Attack, Tempest Attack, Brute Force Attack, Replay Attack and Other Attacks.

1. Introduction

Authentication plays an important role in protecting resources against unauthorized use. Since the advent of the computers, man has been looking for various possible means to make communication among entities secure via various authentication processes which range from simple password based authentication system to costly and computation intensive biometric authentication systems. Passwords have proved to be very handy. They are not just some key but also serve several purposes. They authenticate us to a machine to prove our identity a secret key that only we should know. The username is used to identify us and the password validates us. But with time the various weaknesses associated with a password have come to surface. It is always possible for people other than the authenticated user to posses its knowledge at the same time. Password thefts can and do happen on a regular basis, so there is a need to protect them. Rather than using some random set of alphabets and special characters as the passwords we need something new and something unconventional to ensure safety. At the same time we need to make sure that it is easy to be remembered by you as well as difficult enough to be hacked by someone else. This is where the Image Based Authentication system comes into picture. It is based on a well understood truism that the human brain is more adept at recalling a previously seen image than a previously seen text. In a recent study conducted at the University of California at Berkeley, image-based authentication (IBA) systems have been found more user friendly than the usual text based systems. Besides being user friendly we need to strengthen the security during authentication also.

2. Needham Schroeder Protocol

The term Needham Schroeder protocol can refer to one of two communication protocols intended for use over an insecure network, both proposed by Roger Needham and Michael Schroeder [1]. Needham Schroeder Protocol is one of the earliest computer network authentication protocol designed for use on insecure networks (e.g. internet). It allows individuals communicating over a network to prove their identity to each other while also preventing eavesdropping. These are:

1. The *Needham Schroeder Symmetric Key Protocol* is based on a symmetric encryption algorithm. It forms the basis for the Kerberos protocol. This protocol aims to establish a session key between two parties on a network, typically to protect further communication.

Manuscript received November 5, 2010
Manuscript revised November 20, 2010

2. The *Needham Schroeder Public-Key Protocol*, based on public-key cryptography. This is intended to provide mutual authentication between two parties communicating on a network, but in its proposed form it is insecure.

A. The symmetric protocol

Here, Alice (A) initiates the communication to Bob (B). Also,

- S is a server trusted by both parties.
- K_{AS} is a symmetric key known only to A and S.
- K_{BS} is a symmetric key known only to B and S.
- N_A and N_B are nonce.

The protocol can be specified as follows in security protocol notation:

$A \rightarrow S: A, B, N_A$

Alice sends a message to the server identifying herself and Bob, telling the server she wants to communicate with Bob.

$S \rightarrow A:\{ N_A, K_{AB},B,\{K_{AB},A\}_{KBS}\}_{KAS}$

The server generates K_{AB} and sends back to Alice a copy encrypted under K_{BS} for Alice to forward to Bob and also a copy for Alice. Since Alice may be requesting keys for several different people, the nonce assures Alice that the message is fresh and that the server is replying to that particular message and the inclusion of Bob's name tells Alice who she is to share this key with.

$A \rightarrow B:\{K_{AB}, A\}_{KBS}$

Alice forwards the key to Bob who can decrypt it with the key he shares with the server, thus authenticating the data.

$B \rightarrow A: \{N_B\}_{KAB}$

Bob sends Alice a nonce encrypted under K_{AB} to show that he has the key.

$A \rightarrow B: \{N_B-1\}_{KAB}$

Alice performs a simple operation on the nonce, re-encrypts it and sends it back verifying that she is still alive and that she holds the key.

The protocol is vulnerable to a replay attack. If an attacker records one run of this protocol, then subsequently learns the value K_{AB} used, she can then replay the message $\{K_{AB},A\}_{KBS}$ to Bob, who will accept it, being unable to tell that the key is not fresh. This flaw is fixed in the Kerberos protocol by the inclusion of a timestamp.

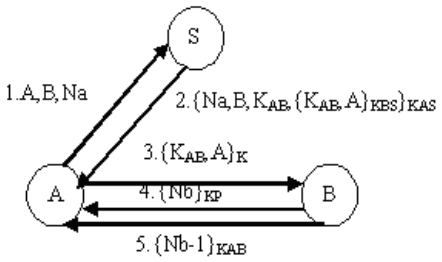

Figure – 1 The symmetric key protocol

A. The public-key protocol

This assumes the use of a public-key encryption algorithm. Here, Alice (A) and Bob (B) use a trusted server (S) to distribute public keys on request. These keys are:

- K_{PA} and K_{SA}, respectively public and private halves of an encryption key-pair belonging to A
- K_{PB} and K_{SB}, similar belonging to B
- K_{PS} and K_{SS}, similar belonging to S. (Note this has the property that K_{SS} is used to *encrypt* and K_{PS} to *decrypt*).

The protocol runs as follows:

$A \rightarrow S: A, B$

A requests B's public keys from S

$S \rightarrow A: \{K_{PB}, B\}_{KSS}$

S responds. B's identity is placed alongside K_{PB} for confirmation.

$A \rightarrow B: \{N_A, A\}_{KPB}$

A invents N_A and sends it to B.

$B \rightarrow S: B, A$

B requests A's public keys.

$S \rightarrow B: \{K_{PA}, A\}_{KSS}$

Server responds.

$B \rightarrow A: \{N_A, N_B\}_{KPA}$

B invents N_B, and sends it to A along with N_A to prove ability to decrypt with K_{SB}.

$A \rightarrow B: \{N_B\}_{KPB}$

A confirms N_B to B, to prove ability to decrypt with K_{SA}

At the end of the protocol, A and B know each other's identities, and know both N_A and N_B. These nonces are not known to eavesdroppers.

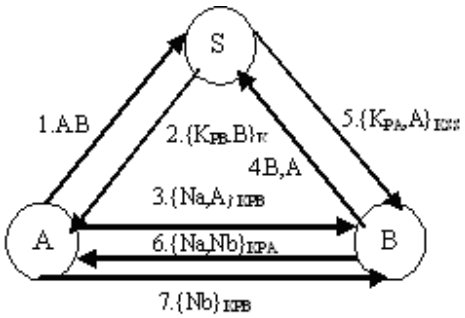

Figure – 2 The public key protocol

3. Attacks on the protocol

This section discusses the security performance of the Needham Schroeder Protocol system. This also includes the various preventive measures that have been used to protect the system against these attacks and to show how image based methods are way better than the conventional text based passwords.

3.1 Shoulder Attack

As we know the image set used for password authentication consists of images that are unique and abstract, not easily describable and differ widely in their color schemes and structures. This helps counter the shoulder attack. Also this system facilitates that the image selected is not highlighted, and so the attacker has absolutely no clue as to what image 800x600 pixels, so the entire image grid does not fit in the screen and all the images cannot be seen all at once.

3.2 Tempest Attack

This IBA system ensures that the image that the user selects is not displayed on the screen but stored in the background. This is done to make sure that the attacker gets absolutely no idea about the color coding. Because electromagnetic emanations from a moNSPor can be read by sensitive receiver kept at a certain distance from it. This aids the attacker to extract the color information from the images. Even if the attacker manages to extract information of the displayed image grid, he would still have to figure out the password from the grid which in itself is a tedious task. Also for further security, another feature has been introduced wherein the image so selected by the user to be viewed appears black and white as well as blurred so as to send out no signal that can be detected by the eavesdropper.

3.3 Brute Force Attack

To crack a password, an attacker has to sit and try all the combinations possible. This is not possible in the IBA systems. Reason being the calculations involved are too large to be sorted out. And the time restriction makes ensures the safety.

3.4 Replay Attack

If an attacker uses an older compromised value for K_{AB}, he can then replay the message $\{K_{AB},B\}_{KBS}$ to B, who will accept it, being unable to tell that the key is not fresh. The replay attack is combat by using a little modification based on the Needham Schroeder Protocol. This is done by the introduction of a new nonce N_B' in the starting itself. Before contacting the server A sets up connection with B sending its ID,A. B then replies with the nonce N_B' encrypted under K_{AB}. This nonce ensures that the session is fresh. Note that N_B' is a different nonce from N_B.The inclusion of this new nonce prevents the replaying of a compromised version of $\{K_{AB},B\}_{KBS}$ since such a message would need to be of the form $\{K_{AB},A,N'_B\}_{KBS}$ which the attacker can't forge since she does not have K_{BS}.

3.5 Other Attacks

Unfortunately, this protocol is vulnerable to a man-in-the-middle attack [5]. If an impostor I can persuade A to initiate a session with him, he can relay the messages to B and convince B that he is communicating with A.

Ignoring the traffic to and from S, which is unchanged, the attack runs as follows:

$A \rightarrow I: \{N_A, A\}_{KPI}$

A sends N_A to I, who decrypts the message with K_{SI}

$I \rightarrow B: \{N_A, A\}_{KPB}$

I relay the message to B, pretending that A is communicating

$B \rightarrow I: \{N_A, N_B\}_{KPA}$

B sends N_B

$I \rightarrow A: \{N_A, N_B\}_{KPA}$

I relay it to A

$A \rightarrow I: \{N_B\}_{KPI}$

A decrypts N_B and confirms it to I, who learns it

$I \rightarrow B: \{N_B\}_{KPB}$

Here, we re-encrypts N_B, and convinces B that he's decrypted it

At the end of the attack, B falsely believes that A is communicating with him, and that N_A and N_B are known only to A and B.

The attack was first described in a 1995 paper by Gavin Lowe. The paper also describes a fixed version of the scheme, referred to as the *Needham-Schroeder-Lowe* protocol. The fix involves the modification of message six, that is we replace:
$B \rightarrow A: \{N_A, N_B\}_{KPA}$
With the fixed version:

$$B \rightarrow A: \{N_A, N_B, B\}_{KPA}$$

4. The Proposed Scheme

Alice (A) and Bob (B) use a trusted server (S) to distribute public keys on request. These keys are:

- K_{PA} and K_{SA}, respectively public and private halves of an encryption key-pair belonging to A
- K_{PB} and K_{SB}, similar belonging to B
- K_{PS} and K_{SS}, similar belonging to S. (Note this has the property that K_{SS} is used to *encrypt* and K_{PS} to *decrypt*).
- K_A and K_B are encryption keys belonging to respectively Alice (A) and Bob (B).

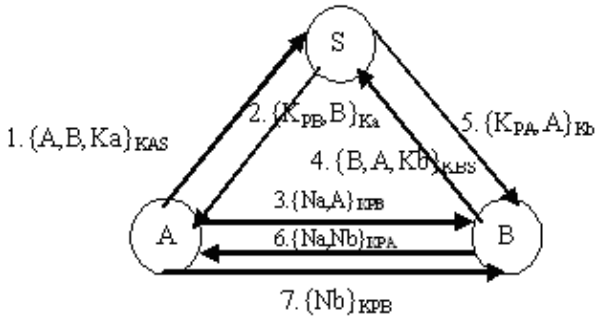

Figure – 3 The Proposed Scheme

The protocol runs as follows:

$A \rightarrow S: \{A, B, K_A\}_{KAS}$

A requests B's public keys from S

$S \rightarrow A: \{K_{PB}, B\}_{Ka}$

S responds. B's identity is placed alongside K_{PB} for confirmation.

$A \rightarrow B: \{N_A, A\}_{KPB}$

A invents N_A and sends it to B.

$B \rightarrow S: \{B, A, K_B\}_{KBS}$

B requests A's public keys.

$S \rightarrow B: \{K_{PA}, A\}_{KB}$

Server responds.

$B \rightarrow A: \{N_A, N_B\}_{KPA}$

B invents N_B, and sends it to A along with N_A to prove ability to decrypt with K_{SB}.

$A \rightarrow B: \{N_B\}_{KPB}$

A confirms N_B to B, to prove ability to decrypt with K_{SA}
At the end of the protocol, A and B know each other's identities, and know both N_A and N_B. These nonces are not known to eavesdroppers.

5. CONCLUSION

In this paper, we have shown the various attacks on Needham-Schroeder protocol, possible attacks on protocol, and the proposed scheme can be able to remove two possible attacks on Needham-Schroeder protocol. This scheme is vulnerable to a server spoofing attack and stolen-verifier attacks. In essence, IBA generally encapsulates the Needham Schroeder Protocol (NSP) and provides client a completely unique and secured authentication tool to work on. Comparison of major password techniques has been shown in Appendix - I
This paper however proposes a hypothesis regarding the use of Needham Schroeder Protocol (NSP) and is a comprehensive study on the subject of using images as the password set. This forms the basis for a secure communication between the communicating entities

Acknowledgments

I (Raman Kumar) deeply indebted to my beloved master, supervisors, my parents and my research laboratory whose help, stimulating suggestions and encouragement helped me in all the time of research for and writing of this paper for journal. The authors also wish to thank many anonymous referees for their suggestions to improve this paper.

References

[1] Andrew S. Tanenbaum and Maarten Van Steen, Distributed Systems, Pearson Education.
[2] C. M. Chen, and W. C. Ku, "Stolen-verifier Attack on two New Strong-password Authentication Protocol," IEICE Transactions on Communications, Vol. E85-B, No. 11, pp. 2519—2521, November 2002.
[3] Cristian Darie, Bogdan Brinzarea, Filip Chereches-Tosa, and Mihai Bucica, AJAX and PHP: Building Responsive Web Applications, Paperback, March 1, 2006.
[4] F. Belli, "A Holistic view for Modeling and Testing User Interactions using Finite-State Techniques," Proceedings of the 1st South-East European Workshop on Formal Methods, SEEFM'03,Thessaloniki, Greece, November 2003.
[5] F. Belli, "Finite-State Testing and Analysis of Graphical User Interfaces", Proc. 12th ISSRE, pp. 34-43, 2001.

[6] F. Belli, K.-E. Grosspietsch, "Specification of Fault-Tolerant System Issues by Predicate/Transition Nets and Regular Expressions – Approach and Case Study", IEEE Trans. On Softw. Eng. 17/6, pp. 513-526, 1991.
[7] Gavin Lowe, "An attack on the Needham-Schroeder public key authentication protocol", Information Processing Letters, 56(3):131—136, November 1995.
[8] John Rushby, "The Needham-Schroeder Protocol in SAL," CSL Technical Note, October 2003 (Updated June 2005).
[9] Richard E. Newman, Piyush Harsh, and Prashant Jayaraman, "Security Analysis of and Proposal for Image Based Authentication," IEEE Carnahan, 2005.
[10] Roger Needham and Michael Schroeder, "Using encryption for authentication in large networks of computers. Communications of the ACM", Journal, 21(12), December 1978.
[11] Sandirigama, A. Shimizu, and M. T. Noda, "Simple and secure password authentication protocol (SAS)," IEICE Transactions on Communications, vol.E83-B, pp.1363-1365, June 2000.
[12] Security Guidelines: Prevention and Response and Hacker Attacks, Digital Edition, June 1, 2001.
[13] Vijay K. Bhargava, H. Vincent Poor, Vahid Tarokh, and Seokho Yoon, Communications, Information and Network Security, Hardcover, December 31, 2002.
[14] William Stallings, "Cryptography and network security design and principles".
[15] Y, Xiao, Security in Distributed and Networking Systems (Computer and Network Security, Hardcover - September 30, 2007.

Mr. Raman Kumar working as a Lecturer with the Department of Computer Science and Engineering, D A V Institute of Engineering and Technology, Jalandhar. Before joining D A V Institute of Engineering and Technology, Jalandhar,
He did his Bachelor of Technology with honours in Computer Science and Engineering from Guru Nanak Dev University; Amritsar (A 5 Star NAAC University). He did his Master of Technology with honours Computer Science and Engineering from Guru Nanak Dev University; Amritsar (A 5 Star NAAC University). His major area of research is Cryptography, Security Engineering and Information security. He has various publications in National as well as International Conferences and Journals on his research areas.

Appendix – I

Techniques	Usability		Security issues	
	Authentication process	Memorability	Password space	Possible attack methods
Text-based password	Type in password, can be very fast	Depends on the password. Long and random passwords are hard to remember.	94^K(there are 94 printable characters excluding SPACE,N is the length of the password).The actual password space is usually much smaller.	Dictionary attack, brute force search, guess, spyware, shoulder, surfing , etc.
Perring and Song	Pick several pictures out of many choices. Takes longer to create than to text password	Limited user study showed that more people remembered pictures than text-based passwords.	N!/K!(N-K)!(N is the total number of pictures; K is the number of pictures in the graphical password)	Brute force search, guess, shoulder surfing
Sobrado and Birget	Click within area bounded by pre-registered picture objects, can be very fast	Can be hard to remember when large numbers of objects are involved	N!/K!(N-K)!(N is the total number of pictures objects; K is the number of pre-registered objects)	Brute force search, guess
Man, et al., Hong, et al.	Type in code of pre-registered picture objects; can be very fast	Users have to memorize both picture objects and their codes. More difficult than text based password	Same as the text based password	Brute force search, spyware
Passface	Recognize and pick the pre-registered pictures; takes longer than the text based password	Faces are easier to remember, but the choices are still predictable	N^K(K is the number of rounds of authentication, N is the total number of pictures at each round)	Dictionary attack, Brute force search, guess, shoulder surfing
Jansen et al	User register as a sequence of images; slower than text based password	Pictures are organized according to different themes to help users remember	N^K(N is the total number of pictures, K is the number of rounds of authentication. N is the small due to the size limit of mobile devices)	Brute force search, guess, shoulder surfing

Takada and Koike	Recognize and click on the pre-registered images; slower than text based password	Users can use their favorite images; easy to remember than system assigned pictures	(N+1)^K(K is the number of rounds of authentication, N is the total number of pictures at each round)	Brute force search, guess, shoulder surfing
Jermyn, et al. Thorpe and van Oorscho	Users draw something on a 2D grid	Depends on what users draw. User studies showed the drawing sequence is hard to remember	Password space is larger than text based password. But the size of DAS password space decreases significantly with the fewer strokes for a fixed password length	Dictionary attack, shoulder surfing
Syukri, et al.	Draw signatures using mouse. Need a reliable signature recognition program	Very easy to remember but hard to recognize	Infinite password space	Guess, Dictionary attack, shoulder surfing Guess, Dictionary attack, shoulder surfing
Goldberg et al.	Draw something with a stylus onto a touch sensitive screen	Depends on what users draw	Infinite password space	
Blonder, Passlogix, Wiedenbeck, et al.	Click on several pre-registered locations of a picture in the right sequence	Can be hard to remember	N^K(N is the number of pixels or smallest units of a picture, K is the number of locations to be clicked on	Brute force search, guess, shoulder surfing