NEW SECURITY PROTOCOL FOR M-LEARNING

Lirong He, Lisha He, Ian Rogers
School of Computer Science, University of Manchester
Manchester, UK
ian.rogers@manchester.ac.uk

Abstract

Mobile Learning (M-Learning) is a new application for wireless technology. By using a wireless network to access the computer network, learners around the world can participate in cooperative learning activities sharing course information, and teachers can change and update the information easily. The course information may be of various digital multimedia types, such as in the form of text, graphics, image, and/or sound. M-Learning will become increasingly important as mobile learners increase.

M-Learning enables mobile learners to access Internet services while on the move, anywhere and anytime. The information of a learner's assessments, feedback, learner records, homework, the answers of exams, and payment is an essential part of M-Learning. Security provision for M-Learning is an open and challenging research problem due to user mobility, limited resources in wireless devices and expensive radio bandwidth.

To achieve secure M-Learning while at the same time not to impose much computational, communication and storage requirements on mobile devices, we envisage an asymmetrical approach. To demonstrate the efficacy of this approach, we have designed a new protocol for improving the security of M-Learning with existing wireless and Internet technologies. The new protocol facilitates mutual authentication, to secure M-Learning, but differs from current approaches that provide mutual authentication through extensive use of computationally expensive cryptographic primitives such as public-key algorithms. It is able to provide the required security services with the assistance of the mobile network providers and the use of inexpensive cryptographic functions, such as symmetric cryptography and hash functions.

This paper presents work on the design of the new protocol. The study and evaluation demonstrates that the network operator assisted approach used in the new protocol design is efficient for mobile learners, and significantly better than current related protocols. The approach allows the provision of security and M-Learning services with very little increase in computational requirements.

Keywords
Mobile Learning, M-Learning, Security, Authentication

1. INTRODUCTION

Mobile Learning (M-Learning) is the next generation of e-learning and is based on mobile devices [1]. M-Learning is proving to be an increasingly useful and powerful technology, inspiring developments for the web and mobile networks. These areas include content, information, and knowledge management; community building; publishing and journalism; teaching, learning, and collaboration; and course management systems [2]. In the meanwhile M-Learning creates a number of challenges, such as costs, usability, choice of technology, roles, equipment management, support for teachers, administration, collaboration, and security [3].

Security is a significant challenge for M-Learning due to user mobility, limited resources in wireless devices and expensive radio bandwidth. M-Learning presents a number of security requirements, including authentication, confidentiality, integrity, non-repudiation, privacy, availability and trust. Among these security services, authentication is the foundation. Authentication is the act of ensuring that someone or something is whom it claims to be. In the M-Learning context, a learner, a teacher and an online education organisation providing software and resources have to make sure that they are communicating with the right entities. In addition, they need to establish a session secret key for subsequent confidential transactions, such as for online examination and assessments purposes.

The problem of how to provide authentication services in a mobile environment has been addressed in recent years, and a number of proposals have been published in the literature [4-11]. Among them, authentication protocols with only two entities normally require heavy operational load at the mobile side [7, 8]. To reduce the computational requirements at the mobile side, asymmetrical authentication protocols make use of a trusted authentication server [5, 6, 9-11]. However, a variety of them require the authentication server to create a session key for the two end users [9, 10]. Therefore the server is able to not only assist the authentication process, but also to get access to subsequent confidential transactions that are encrypted by the session key. To solve this problem, Steiner et al. proposed a protocol that enables two end users to generate the session key without the involvement of the authentication server [11]. Compared with [9, 10], it is more secure because the server cannot get access to subsequent confidential transactions. But later, Lin et al. proved that [11] is insecure since it is susceptible to password guessing attacks [4]. Though the solutions by [5, 6] are secure and more efficient than other proposals, they remain computationally expensive.

The main contribution of this paper is to present a secure and efficient authentication protocol for M-Learning applications. The protocol, called Network Assisted Authentication Protocol (NAAP), achieves mutual authentication and key establishment between a mobile learner and an online education organisation, and at the same time, places less computational requirements than the schemes most related to our work [5, 6]. Therefore, NAAP is more suited to M-Learning applications in which mobile devices are expected to have thin computational and storage capabilities. A trusted authentication service in the network operator is introduced into our protocol to assist the authentication process to reduce computational cost. The use of the network operator has taken the following considerations and observations into consideration [12]:

(1) Network operators build up and operate wireless communication network infrastructures; they therefore can easily implement new platforms and protocols for secure mobile transactions.
(2) Network operators have connections to the Internet and therefore they can use existing Internet-based protocols to communicate with the education organisation on the Internet.
(3) Network operators already have their subscribed mobile users' details, and provide security services to mobile users over the wireless connection. The network operator can reuse this security sensitive information.
(4) Network operators usually have ample resources (storage, computational power and network bandwidth) in contrast to mobile devices, and are always on-line.

The remainder of this paper is organized as follows. Section 2 summarizes the security requirements for authentication for M-Learning. Section 3 outlines the notation and network infrastructure used. Section 4 describes the protocol in details. Section 5 analyses its security against the requirements stated in Section 2. Section 6 compares the NAAP protocol with its most related work [5, 6]. Finally our conclusions are outlined in Section 7.

2. SECURITY REQUIREMENTS

To achieve secure authentication and key establishment between a mobile learner and an education organisation on the Internet, the authentication protocol for M-Learning should meet the following security requirements:
(S1) Authentication of the online education organisation to the mobile learner. The protocol should allow the authentication of the online education organisation to the mobile learner. This prevents an attacker from masquerading as the education organisation to communicate with the mobile learner.
(S2) Authentication of the mobile learner to the online education organisation. The protocol should enable the online education organisation to authenticate the mobile learner in order to make sure the authenticity of the mobile learner.
(S3) End-to-end session key establishment. The protocol should allow the mobile learner and the online education organisation to establish a shared secret session key for subsequent confidential transactions, such as online examination message exchanges.
(S4) Session key confirmation. The protocol should allow the mobile learner to confirm that the online education organisation is in possession of the right session key and vice versa. This prevents the use of an inconsistent session key by the mobile learner or the online education organisation.
(S5) Freshness of the session key. The protocol should ensure the freshness of the session key. This prevents an attacker from reusing a previous session key to get access to confidential information in the transactions.

3. PRELIMINARIES

This section introduces the notation used in the protocol description and the network infrastructure that the authentication protocol is based upon.

3.1 Notation

The notation to be used for the protocol presentation is summarised as follows:

x, y Concatenation of data items x and y

h(x) A one-way hash function with the following properties: (a) for any x, it is easy to compute h(x); (b) given x, it is hard to find x' (≠x) such that h(x') = h(x); and (c) given h(x), it is hard to compute x. An example of such a one-way hash function is SHA-1.

K_{AB} Session key shared between entity A and entity B (A, B ∈ {A, S, B})

pk_A Public key of entity A

sk_A Private key of entity A

{x}K The cipher-text of item x encrypted with a key K using a public-key cryptosystem such as RSA.

3.2 Network infrastructure

The protocol presented in the paper provides secure and efficient authentication services between a mobile learner to access an online education organisation for M-Learning. The infrastructure consists of three functional entities: a mobile learner using a mobile device such as a mobile phone or a PDA (Personal Digital Assistant) (denoted as A hereafter), an online education organisation (denoted as B) and a trusted authentication server inside the network operator (denoted as S). A connects to B to conduct a secure M-Learning transaction, such as for online examinations or online payments. B conducts secure transactions with A. The network operator provides the wireless network connection and bandwidth for A to get access to B; S is responsible for assisting mutual authentication between A and B.

4. PROTOCOL DESIGN

In this section, we present our Network Assisted Authentication Protocol (NAAP) for M-Learning. NAAP consists of four transactions, T1 to T4, as shown in Fig. 1.

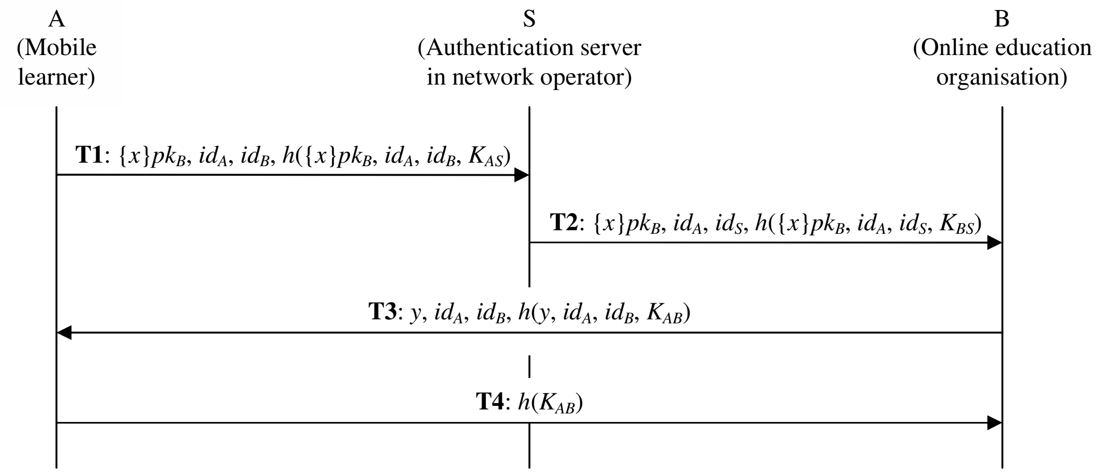
A
(Mobile
learner)
S
(Authentication server
in network operator)
B
(Online education
organisation)
T1: $\{x\}pk_B, id_A, id_B, h(\{x\}pk_B, id_A, id_B, K_{AS})$
T2: $\{x\}pk_B, id_A, id_S, h(\{x\}pk_B, id_A, id_S, K_{BS})$
T3: $y, id_A, id_B, h(y, id_A, id_B, K_{AB})$
T4: $h(K_{AB})$

Fig. 1. The NAAP protocol

T1: A chooses a secret random number x and encrypts it with B's public key pk_B, i.e. $\{x\}pk_B$, as an authentication challenge to B. With the public key algorithm, it is difficult for any entity other than B to get x without knowing B's private key sk_B. Therefore x is a secret value shared only between A and B. A then generates a keyed hash value $h(\{x\}pk_B, id_A, id_B, K_{AS})$ with A's identity id_A, B's identity id_B and a key K_{AS} which is known only to A and S. A sends $\{x\}pk_B$, id_A, id_B and $h(\{x\}pk_B, id_A, id_B, K_{AS})$ to S in T1.

T2: Upon receipt of T1, S computes a new hash value with the received $\{x\}pk_B$, id_A, id_B and its own K_{AS} and compares it with the received hash value. If the two hash values do not match, S may ask A to re-send transaction T1 or terminate the protocol run (this applies to all transactions if any verification fails). Otherwise, S is assured that A is authenticated since A demonstrates its knowledge of the key K_{AS}. S then generates a keyed hash value $h(\{x\}pk_B, id_A, id_S, K_{BS})$ and sends it to B with $\{x\}pk_B$, id_A and its own identity id_S in T2. K_{BS} is the key shared only between B and S.

T3: After receiving T2, B verifies $h(\{x\}pk_B, id_A, id_S, K_{BS})$ by using its own K_{BS}. If the verification is positive, B is assured that T2 is from S. As S is a trusted authentication server, B believes that S authenticates A before sending T2 and passes the authentication challenge from A, $\{x\}pk_B$, honestly. B decrypts $\{x\}pk_B$ with its private key sk_B to obtain the value x. B then generates a random number y and a session key K_{AB}, where $K_{AB} = h(x, y)$. K_{AB} will be used for securing subsequent transactions. In T3, B sends y, id_A, id_B and a hash value $h(y, id_A, id_B, K_{AB})$ to A, for authenticity checking from B to A.

T4: A generates the session key $K_{AB} = h(x, y)$ using the received y and x from its store, and uses it to verify the hash value $h(y, id_A, id_B, K_{AB})$ from B. If the verification is successful, A is assured that B is authenticated because only B can decrypt the authentication challenge to get x using the correct sk_B, and therefore use the correct x to generate the proper K_{AB}. A then sends a hash value of K_{AB}, $h(K_{AB})$, to B for key confirmation in T4.

Finally, B verifies $h(K_{AB})$ received in T4 by hashing its own K_{AB} and comparing them. If they are equal, B is convinced that A holds the same session key for subsequent communication. The NAAP protocol is now complete.

5. SECURITY ANALYSIS

This section presents a security analysis of the NAAP protocol against the requirements stated in Section 2.

(S1) Authentication of the online education organisation (B) to the mobile learner (A).
A authenticates B through the use of the authentication challenge $\{x\}pk_B$. In transaction T3, B computes the response x using sk_B, where $x = \{\{x\}pk_B\}sk_B$, and uses x to compute the session key K_{AB}, where $K_{AB} = h(x, y)$. B then generates the hash value $h(y, id_A, id_B, K_{AB})$ for its authentication to A. In transaction T4, a positive result of the verification of the hash value $h(y, id_A, id_B, K_{AB})$ demonstrates B's knowledge of K_{AB} and therefore the knowledge of the correct x. This x assures A that B has knowledge of the correct corresponding private key, sk_B, as it can correctly decrypt x from the authentication challenge $\{x\}pk_B$. Therefore B is the entity it claims to be.

(S2) Authentication of the mobile learner (A) to the online education organisation (B).
The key K_{AS} in transaction T1 demonstrates A's knowledge of the key to the authentication server S and therefore authenticates A to S. In addition, B believes that S authenticates A on its behalf because S is a trusted server. As a result, once S authenticates A in T2 and sends T2 to B, B is convinced that A is authenticated.

(S3) End-to-end session key establishment.
In NAAP, the session key K_{AB} (= $h(x, y)$) is not transmitted in clear text in any transaction. In transactions T3 and T4, K_{AB} is hashed and therefore another entity is unable to get access to it because hash operations are not reversible. Regards to the two parameters used to generate the key, x and y, y is public but x is always inaccessible to the public. In transactions T1 and T2, x is encrypted by using B's public key pk_B. The public key cryptographic system guarantees that only B is able to gain the correct x by decrypting the challenge$\{x\}pk_B$ using the corresponding private key sk_B. Therefore no entity other than A and B can get access to either x or K_{AB}. As a result, end-to-end session key establishment between A and B is achieved.

(S4) Session key confirmation.
The session key K_{AB} is used by B to generate the hash value $h(y, id_A, id_B, K_{AB})$ in T3. Upon receipt of T3, A generates its own K_{AB} by using x and y, and uses the new key to verify the hash value $h(y, id_A, id_B, K_{AB})$ it received. The positive result of the verification shows A that B has knowledge of the correct K_{AB}. Therefore, A is convinced that B has the fresh session key. In T4, A sends the hash value $h(K_{AB})$ and therefore demonstrates its knowledge of K_{AB} to B. So B is assured that A has the correct session key. Thus session key confirmation is met.

(S5) Freshness of the session key.
The session key K_{AB} is generated by using two random numbers, x and y. In the NAAP protocol, x is freshly generated by A in T1 and y is freshly generated by B in T3. Therefore A and B are both assured the freshness of the session key K_{AB}.

As a result, the NAAP protocol satisfies all the security requirements set in Section 2.

6. COMPARISON WITH RELATED WORK

This section compares the NAAP protocol with the KAAP protocol [5] and the AUTHMAC_DH protocol [6], which are the most related to our protocol. Table 1 shows the comparison of these protocols in terms of numbers of heavy cryptographic operations. Heavy cryptographic operations are time- and resource-consuming, particularly in resource constrained mobile devices.

Heavy cryptographic operations	**KAAP**	**AUTHMAC_DH**	**NAAP**
Public key encryption at A	1	0	1
Exponential operations at A	2	2	0

Table 1. Comparison of KAAP, AUTHMAC_DH and NAAP

With regards to security, these three protocols are able to achieve mutual authentication and key establishment between a mobile learner and an online education organisation in the context of M-Learning with the use of a trusted authentication server. Each of them can achieve all the security requirements set out in Section 2. In terms of protocol performance, each protocol requires the mobile learner A to send two transactions. However, NAAP requires only one heavy cryptographic operation (public key encryption) at A, while AUTHMAC_DH requires 2 (exponential operations) and KAAP requires 3 (1 public key encryption and 2 exponential operations) heavy cryptographic operations. Based on the benchmark [13], public key encryption (for example RSA-1024 encryption) is much more efficient than exponential operations (DH-1024 key-pair generation or DH-1024 key agreement). As a result, NAAP is much more efficient than KAAP and AUTHMAC_DH.

7. CONCLUSION

This paper has presented the design of the NAAP protocol that achieves end-to-end authentication and key establishment for M-learning applications. The protocol uses an authentication server in a network operator to provide authentication service between a mobile learner and an online education organisation. The security analysis of the protocol has demonstrated that the protocol satisfies all the security requirements set in Section 2. The comparison of the NAAP protocol and related work has demonstrated that it is more efficient.

References

[1] Sharples, M., “The Design of Personal Mobile Technologies for Lifelong Learning”, *Computers & Education*, 2000, vol. 34, 177-193.

[2] Leung, C.-H., Chan, Y.-Y, “Mobile Learning: a New Paradigm in Electronic Learning”, proceedings of the 3rd IEEE International Conference on Advanced Learning Technologies, Greece, 2003.

[3] Giasemi, N., Lefrere, P., O’Malley, C., Sharples, M., Taylor, J., “Producing Guidelines for Learning, Teaching and Tutoring in a Mobile Environment”, proceedings of the 2nd IEEE international workshop on Wireless and Mobile Technologies in Education, 2004.

[4] Lin, C.L., Sun, H.M., Hwang, T., “Three-party Encrypted Key Exchange: Attacks and a Solution”, *ACM Operating System Reviews*, 2000, 34 (4), 12-20.

[5] Yeh, H.-T., Sun, H.-M., “Password-based User Authentication and Key Distribution Protocols for Client-server Applications”, *Journal of Systems and Software*, 2004, vol. 72, 97-103.

[6] Alsan, H. K., “AUTHMAC_DH: a New Protocol for Authentication and Key Distribution”, proceedings of the seventh IFIP conference on Communications and Multimedia Security, Italy, 2003.

[7] Horn, G., Preneel, B., “Authentication and Payment in Future Mobile Systems”, proceedings of ESORICS’98, Springer, Berlin, 1998. 277-293.

[8] Jeffs, T.: “Wireless Application Protocol 2.0 Security”, SANS Institute, *http://www.sans.org/*, 2001.

[9] Kwon, T., Kang, M., Jung, S., Song, J., “An Improvement of the Password-based Authentication Protocol on Security against Replay Attacks”, *IEICE Transactions on Communications*, 1999, E82-B (7).

[10] Kwon, T., Song, J., “Authentication Key Exchange Protocols Resistant to Password Guessing Attacks”, *IEE Communications*, 1998, 145 (5) 304-308.

[11] Steiner, M., Tsudik, G., Waidner, M., “Refinement and Extension of Encrypted Key Exchange”, *Operating Systems Review*, 1995, 29 (3), 22-30.

[12] He, L., “An Asymmetrical End-to-end Mobile Payment Protocol for Mobile Commerce”, PhD thesis, University of Manchester, UK, 2004.

[13] Dai, W., “Crypto++ 5.2.1 Benchmarks”, *http://www.eskimo.com/~weidai/benchmarks.html*, 2004.