Authenticated Deniable Internet Key Exchange

Mrs. S. Saranya[1] , R. Pitchandi[2]
[1]*A.P(OG),* [2]*M.Tech(CSE) Scholar*
Department of Computer Science and Engineering, SRM University, Chennai, India

Abstract - We propose two public-key schemes to achieve deniable authentication for the Internet Key Exchange (IKE). Authentication in security had is the essential factor in the key establishment over Internet. The Deniable Internet key exchange protocol gives more value to the IKE standard. Our schemes can in some situations be more efficient than existing IKE protocols as well as having stronger deniability properties. Key-exchange, in particular Diffie–Hellman key exchange (DHKE), is among the core cryptographic mechanisms for ensuring network security. For key-exchange over the Internet, both security and privacy are desired. In this paper, we develop a family of privacy-preserving authenticated DHKE protocols named deniable Internet key-exchange (DIKE), both in the traditional PKI setting and in the identity-based setting. The newly developed DIKE protocols are of conceptual clarity and practical (online) efficiency. They provide useful privacy protection to both protocol participants, and add novelty and new value to the IKE standard.

Keywords- Authentication, Key Exchange, deniability, Diffie–Hellman, restricted random oracle, security.

I. INTRODUCTION

Security is having a good implication over the internet. Key exchange is a interesting and essential area of cryptography. An authentication protocol allows a sender messages to the receiver in the secured manner. The foremost objective of this type of protocol is to establish a link between the sender and the receiver which is authenticated. User authentication gives the legitimacy of the intended parties in the real time. In the case of the client server application the service provider needs to ensure the legitimacy of a user before providing services to the user and the user also needs same. Because of the communication parties need a common key to encrypt and decrypt data, shared common key is known only to the intended parties. The Key exchange session may take place with any one of a set of servers sitting behind a address specified in the session activation or a party may respond to a request coming from a peer that is not willing to reveal its identity over the network and not to responder before the latter has authenticated itself. For key exchange protocols, the security and privacy are desired. This type of Key Exchange protocols providing a certain level of privacy protection serves as one of the major criteria underlying the evolution of a list of important industrial standards which is particularly witnessed by the Internet Key Exchange and the SIGMA Protocol.

II. RELATED WORKS

A Deniability service offered at the IP layer preserves the privacy feature from the upper layers. A Deniable authentication protocol is used to prevent the receiver from proving to a third party that the message is originated from the sender. The security of a communication protocol is based on one or more assumptions. A key agreement protocol is built on one or more cryptographic assumptions. A protocol with multiple independent assumptions with a logic OR relation is like a house with multiple outside doors with different security mechanisms. If the protocol has the more independent OR related assumptions then the attacker can try to attack the protocol in many ways.

Consider the two protocols A and B. If A is based on multiple independent OR related cryptographic assumptions and B is based on the one of the assumptions in A. In this case B is at least securing as A. The Security of the Protocol is assessed based on its entirety. An authenticated key establishment is a process of verifying the legitimacy of communicating parties and establishing the common secrets among the communicating parties. Authenticated key establishment is important for all the communication systems such as e-commerce, wireless, wired and Internet applications. This type of protocol is constructed using multiple cryptographic algorithms based on various cryptographic assumptions.

III. EXISTING SYSTEM

The standard of IKE has gone through two generations. The first generation IKEv1 uses public-key encryption as the authentication mechanism. The second generation IKEv2 uses signatures as the authentication mechanism, with the SIGMA protocol serving as the basis. The IKEv2 protocol is based on DHKE and works in the post-specified peer setting, where the information of who the other party is does not necessarily exist at the session initiation stage and is

learnt by the party only after the protocol run evolves (even just in the last round). Actually, this is quite a common case for KE protocols in practice, particularly for the purpose of preserving players' privacy. For example, the key-exchange session may take place with any one of a set of servers sitting behind a (url/ip) address specified in the session activation; Or, a party may respond to a request (for a KE session) coming from a peer that is not willing to reveal its identity over the network and, sometimes, even not to the responder before the latter has authenticated itself (e.g., a roaming mobile user connecting from a temporary address, or a smart-card that authenticates the legitimacy of the card reader before disclosing its own identity). For key-exchange protocols, both security and privacy are desired. Actually, providing a certain level of privacy protection serves as one of the major criteria underlying the evolution of a list of important industrial standards of KE protocols, which is particularly witnessed by the evolution of IKE that is based on the SIGMA protocol.The main disadvantage of the system is later deny taking part in a particular protocol run and a stronger form of deniability can be achieved using shared key.

IV. PROPOSED SYSTEM

In this work, develop a family of privacy-preserving (particularly, deniable) authenticated DHKE protocols, named deniable Internet key-exchange (DIKE), in the traditional PKI setting and in the identity-based setting. The newly developed DIKE protocols are of conceptual clarity, practical (online) efficiency, provide useful privacy protection to both protocol participants, and add novelty and new value to the IKE standard and the SIGMA protocol. The security of DIKE is analyzed in accordance with the Canetti-Krawczyk framework (CK-framework) with post-specified peers in the random oracle (RO) model. We also make discussions on a list of concrete yet essential security properties of DIKE, most of which are beyond the CK-framework. We then define CNMSZK for DHKE , along with detailed clarifications and justifications. To our knowledge, our formulation of CNMSZK for DHKE stands for the strongest definition of deniability, to date, for key-exchange protocols.

V. SECURE COMMUNICATION TECHNIQUE USING IKE

Deniability is a property that ensures protocol participants can later deny taking part in a particular protocol run. This type of property has been declared for the proposed protocols to secure the Internet Protocol level on Internet Communications. One of the basic secure communication techniques is the key establishment protocol that is known as Internet Key Exchange.

In this paper we develop a family of authenticated Deniable Internet Key Exchange protocols which are of conceptual clarity, practical efficiency and provide useful privacy protection for the participants. The security of the protocol is analyzed in accordance with the CK-Framework with post specified peers in the random oracle model. We also make the discussions about the list of concrete yet essential security properties of DIKE which are beyond the CK Framework. Our formulation of CNMSZK and DHKE stand for the strongest definition of deniability for key exchange protocols. The main advantage of the above system is key exchange protocol can be deniable for both the protocol participants and ID based deniable authentication

VI. IMPLEMENTATION

Let ($A = g^a$, a) (resp., ($X = g^x$, x)) be the public-key and secret-key (resp., the DH-component and DH-exponent) of the initiator ˆA , and ($B = g^b$, b) (resp., ($Y = g^y$, y)) be the public-key and secret-key (resp., the DH-component and DH exponent) of the responder player ˆB , where a, x, b, y are taken randomly and independently from Z*q. Let H, HK : $\{0, 1\}^* \rightarrow \{0, 1\}^{|q|}$ be hash functions, which are modeled as random oracles in security analysis. Here, for presentation simplicity, we have assumed H, HK are of the same output length. In practice, they may be of different output lengths.

The deniable Internet key-exchange protocol, for the main mode of IKEv2 is depicted in Figure 1where CERT ˆA (resp., CERTˆB) is the public-key certificate of ˆA (resp., ˆB) issued by some trusted Certificate Authority (CA) within the underlying public-key infrastructure, and sid is the session-identifier that is assumed to be set by some "higher layer" protocol that "calls" the KE protocol and ensures no two sessions run at a party are of identical Session-identifier. Throughout this work, we assume no proof-of-knowledge/possession (POK/POP) of secret-key is mandated during public-key registration, but the CA will check the non-identity sub-group (i.e., G \ 1G) membership of registered public-keys. Also, each party checks the G \ 1G membership of the DH-component from its peer.

VII. ANALYSIS MODEL OF DENIABLE INTERNET KEY EXCHANGE

A key-exchange (KE) protocol is run in a network of interconnected parties where each party can be activated to run an instance of the protocol called a session. Within a session a party can be activated to initiate the session or to respond to an incoming message. As a result of these activations, and according to the specification of the protocol, the party creating and maintaining a session state, generating outgoing messages, and eventually completes the session by outputting a session-key and erasing the session state. Without generating a session key the session may aborted. A session may also be expired, and for an expired session the session key is also erased. A KE session is associated with its holder or owner (the party at which the session exists), a peer (the party with which the session key is intended to be established), and a unique session identifier. For presentation simplicity, for DHKE protocols, the following two assumptions are made in the basic CK-framework: (i) the activation of a session at a party always specifies the name of the intended peer (i.e., working in the "pre-specified peer model"); and (ii) a session is defined by a tuple (ˆA, ˆB , X, Y), where ˆA is the identity of the holder of the session who sends the DH-component X, ˆB the peer who sends the DH-component Y. The peer that sends the first message in a session is called the initiator and the other the responder. Usually, the peers to a session are denoted by ˆA and ˆB; either one may act as initiator or responder. The session (ˆB , ˆA, Y, X) (if it exists) is said to be matching to the session (ˆA, ˆB, X, Y).

A note on session identifiers in reality. The application invoking KE protocol instances should supply the unique session identifier sid for each session, and the setting mechanism of session identifiers is beyond the CK-framework. In practice and particularly in IKEv2, two participants first exchange random nonce's prior to the actual protocol session run, and then use the concatenation of these nonces as the corresponding session identifier. This is a common approach, for setting session identifiers for two-party protocols like IKEv2 and the DIKE protocol developed in this work. An alternative would be to use an externally generated SID, such as a counter, but the use of such an SID would be inconvenient. However, when it comes to multi-party protocols (e.g., group key exchange) without broadcasting messages, the situation is not so clear.

Attacker Model:

The attacker, denoted A, is an active concurrent man-in-the-middle (CMIM) adversary with full Control of the communication links between parties. A can Intercept, modify messages and sent over these links, inject its own messages, interleave messages from different sessions, etc. (Formally, it is A to whom parties hand their outgoing messages for delivery.) A also schedules all session activations and session-message delivery, and can register a list of public keys (for players already controlled by A at the onset of its attack)

In addition, in order to model potential disclosure of secret information, the attacker is allowed to have access to secret information via session exposure attacks of four types: state-reveal queries, session-key queries, secret-key queries, and party corruptions. A state-reveal query is directed at a single session while still incomplete (i.e., before outputting the session key), and the esult is the attacker learns particulars sessions state (which may include, for example, the DH-exponent corresponding to the DH-component). A session-key query can be performed against an individual session after completion but before expiration, and the result is that the attacker learns the corresponding session-key. A secret-key query can be performed against any uncorrupted party, and the result is that the attacker learns the static secret-key of that party. Finally, party corruption means that the attacker learns *all* information in the memory of that party, including the long-term static secret-key (corresponding to the public-key) as well as session states and session keys stored at the party; in addition, the attacker controlled all actions from the moment of the corrupted party. A session is called exposed, if this session or its matching session suffers from *any* of the above four types of session-exposure attacks.

Secure KE (SK-Security:

A polynomial time attacker with the above capabilities is called a KE- attacker. A key-exchange protocol π is called if for any KE-attacker A running against π it holds:

1) Consider two uncorrupted parties and they complete matching sessions in a run of protocol π under attacker A then, except for a negligible probability, the session key output in these sessions is the same.

2) A succeeds (in its test-session distinguishing attack) with probability not more than that 1/2 plus a negligible function.

Adapting SK-security to the post-specified peer setting. Recall that the CK-framework assumes: a party that is

activated with a new session knows already at activation the identity of the intended peer to the session. By contrast, in the "post-specified peer" setting (particularly for the IPsec and IKE protocols]), the information of who the other party is does not necessarily exist at the session initiation stage. It is actually learnt by the party only after the protocol run evolves. Fortunately, adapting the SK- to the post-specified peer setting only requires some minor modifications (related to the mechanism of defining matching sessions): (1) To distinguish concurrent sessions (run at each party), each session bears a unique session-identifier sid; (2) Supposing (ˆA, sid, ˆB) be a completed session (at the party ˆA) with peer ˆB, the session (ˆB , sid) is called the matching session of (ˆA , sid, ˆB), if either (ˆB , sid) is not completed or (ˆB , sid) is completed with peer ˆA.

Theorem:

The DIKE protocol, with pre-computed and exposed DH components and exponents, is SK-secure in the CK-framework with post-specified peers, under the GDH assumption in the random oracle model, where H is assumed to be a programmable random oracle while HK to be a non-programmable RO.

Proof:

We present the proof with respect to an Unexposed and successfully finished test-session run by ˆA (with peer ˆB), denoted (ˆB , j, ˆA), where $1 \leq j \leq s$ and ˆA and ˆB are both uncorrupted players and can be identical (but ˆA may be impersonated by the attacker A). The proof for the case of an unexposed test-session (ˆA, j, ˆB) run by ˆA (with peer ˆB) is similar. For the unexposed test-session (ˆB, j, ˆA), denote by $X = g^x$ (resp, $Y = g^y$) the DH-component sent by ˆA (resp., ˆB), and by NMZK(a, x) = H(j, ˆA, X, Y,CDH(A, Y),CDH(X, Y)) the authentication value sent by ˆA (maybe impersonated by A) in the third round of the test-session. By Lemma 4.1 (for Event-1), we have that, with overwhelming probability, the uncorrupted player ˆA does indeed send NMZK(a, x) in some session that is matching to (ˆB , j, ˆA). That is, the test-session has the matching session (ˆA, j) in which ˆA sends X in the first round and NMZK(a, x) in the third round. As the session-key is computed as HK (X, Y, g^{xy}) where HK is a (non-programmable) random oracle, there are only two possible strategies for the adversary A to distinguish HK (X, Y, gxy) from a random value:

- Key-Replication Attack: A success in forcing the establishment of a session (other than the test-session or its matching session) that has the same session-key output as the test-session. In this case, A can learn the session key of test-session by simply querying that un matching session to get the same key (without having to expose the test-session or its matching session).

- Forging Attack: At some point in its run, A queries the RO, HK , with the values (X, Y, gxy).

VIII. IDENTITY-BASED DENIABLE INTERNET KEY-EXCHANGE

Identity-based key-exchange (IBKE) simplifies public-key certificate management in traditional PKI-based key-exchange, where users' can serve as the public-keys (but at the price of introducing a trusted authority called private key generator that generates the secret-keys for all the users. However, to the best of our knowledge, deniable IBKE (for both the initiator and the responder simultaneously) with post-specified peers is still unknown. In this section, we present an identity-based variant of the DIKE protocol which is referred to as ID-DIKE for presentation simplicity.

Admissible Pairing:

Let ˆe :GXG→G_T be an admissible pairing where G is a cyclic multiplicative group of order q generated by an element g. Here, an admissible pairing ˆe satisfies the following three properties:

- Bilinear: If x, y ∈Zq, then ˆe(gx , gy) = ˆe(g, g)xy.

- Non-Degenerate: ˆe(g, g) _= 1GT , where 1GT is the identity element in GT . In particular, ˆe(g, g) is the generator of GT in case GT is also a cyclic group of the same order q.

- Computable: If g1, g2 ∈ G, ˆe(g1, g2) ∈ GT can be computed in polynomial time.

Bilinear DH (BDH) Assumption:

Let ˆe : G × G → GT be an admissible pairing as defined above. For any three elements X = gx , Y = gy and Z = gz in G, where x, y, z ∈Zq , we denote by BDH(X, Y, Z) = ˆe(g, g)xyz. An algorithm is called a BDH solver for ˆe if it takes as input of any three elements (X, Y, Z) ∈G3 and its goal is to output the value of BDH(X, Y, Z). We say the BDH assumption holds for ˆe if for any PPT BDH solver, the

probability that on input (X, Y, Z) ← G3 (i.e., each of x, y and z is taken uniformly at random from Zq), the solver computes the correct value BDH(X, Y, Z) is negligible (in k = |q|). The probability is taken over the random coins of the solver, the choice of X, Y, Z uniformly at random in G (and also the random choice of the system parameters for (g, q, G, GT)). The gap BDH (GGDH) assumption [33] essentially says that, for the pairing ˆe defined over (g, q, G, GT), computing BDH(X, Y, Z), for X, Y, Z ← G, is strictly harder than deciding whether U = BDH(X_, Y _, Z_) for an arbitrary tuple (X_, Y _, Z_,U) ∈G3 × GT

IX. DENAIBLE INTERNET KEY EXCHANGE WORKFLOWS

1. Setup:

The trusted authority, Private Key Generator (PKG), chooses a master secret-key s ∈ Z*q , and computes the public-key S = gs . Besides the functions H and HK (that are the same in the description of the DIKE protocol in Section III), PKG also specifies a map-to-point hash function H1 : {0, 1}* → G. The public parameters are: (G, GT , ˆe, g, S, H1, h, HK). We assume the master secret-key s cannot be compromised.

2.User Secret-Key Extract:

For a user with identity ˆA the public-key is given by A = H1(ˆA), and the PKG enerates the associated secret-key of the user as SA = As . Similarly, a user of identity ˆB has public-key B = H1(ˆB) and secret-key SB = Bs .

3.ID-Based DIKE Between Two Users ˆA and ˆB:

The fourround ID-based DIKE protocol, in accordance with the main mode DIKE protocol depicted in Figure 1, is depicted in Figure 2. Most advantageous features of the DIKE protocols described in Section III are inherited by the above ID-DIKE protocols. Below, we explicitly highlight some features of the ID-DIKE protocols.

A. Deniability:

The major difference between DIKE and ID-DIKE is that the value CDH(A, Y) (resp., CDH(B, X)) in DIKE is now replaced by ˆe(SA, Y)(resp., ˆe(SB, X)) in ID-DIKE. Observe that all the authentic values POK(ˆB , y), and NMZK(b, y) (resp., NMZK(a, x)) in ID-DIKE can still be computed merely from peer's DH-exponent x (resp., y). In particular, ˆe(SA, Y) = ˆe(A, S)y (resp., ˆe(SB, X) = ˆe(B, S)x).

B.Online Efficiency:. In case of pre-specified peer identity, ˆA (resp., ˆB) can offline pre-compute ˆe(B, S) and ˆe(B, S)x (resp., ˆe(A, S) and ˆe(A, S)y). That is, the online computation involved at each user side is essentially 1 pairing and 1 modular exponentiation.

X. CONCLUSION AND FUTURE WORK

This work provides the secure and efficient technique of providing security between the sender and the receiver so that the data send by the sender should be made secure from various types of attacks such as desynchronization attack, identity disclosure attack and spoofing attack. Signcryption offers a smaller message size and faster processing speed compared to sign-then-encrypt signature followed by encryption technique. Unlike safeguard that rely on symmetric key, the reliance of Signcryption on asymmetric cryptography makes non-repudiation possible. Sometimes due to network traffic and packet loss key unable to reach the destination point. At that time we can find out the some other path using the Graph Theory technique and resend the key to the receiver.

REFERENCES

[1] S. Al-Riyami and K. Paterson, Certificateless public-key cryptography," in Proc. Asiacrypt 2003, pp. 452–473.

[2] M. Bellare and P. Rogaway, "Entity authentication and key distribution,"in Proc. CRYPTO 1993, pp. 273–289.

[3] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in Proc. ACM CCS 1993, pp. 62–73.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Proc. CRYPTO 2001, pp. 213–229.

[5] C. Boyd, W. Mao, and K. G. Paterson, "Deniable authenticated key establishment for Internet protocols," in Proc. SPW 2003, pp. 255–271.

[6] C. Boyd, W. Mao, and K. G. Paterson, "Key agreement using statically keyed authenticators," in Proc. ACNS 2004, pp. 248–262.

[7] C. Boyd and A. Mathuria, Protocols for Authentication and Key Establishment. New York, NY, USA: Springer-Verlag, 2003.

[8] R. Canetti, "Security and composition of cryptographic protocols: A tutorial," SIGACT News, vol. 37, no. 3, pp. 67–92, 2006.

[9] M. C. Gorantla, R. Gangishetti, and A. Saxena, "A survey on IDbased cryptographic primitives," IACR (The International Association for Cryptologic Research), San Diego, CA, USA, Tech. Rep. 2005/094, 2005.

[10] I. Damgård, "Towards practical public-key systems secure against chosen ciphertext attacks," in Proc. CRYPTO 1991, pp. 445–456.

[11] M. Di Raimondo and R. Gennaro, "New approaches for deniable authentication," in Proc. ACM CCS 2005, pp. 112–121.

[12] M. Di Raimondo, R. Gennaro, and H. Krawczyk, "Deniable authentication and key exchange," in Proc. ACM CCS 2006, pp. 466–475.

[13] Y. Dodis, J. Katz, A. Smith, and S. Walfish, "Composability and on-line deniability of authentication," in Proc. TCC 2009, pp. 146–162.

[14] C. Dwork, M. Naor, and A. Sahai, "Concurrent zero-knowledge," in Proc. STOC 1998, pp. 409–418.

[15] .Digital Signature Standard (DSS), FIPS Standard 186-2, Jan. 2000.

[16] .D. Harkins and D. Carreal, "The Internet key-exchange (IKE)," IETF (The Internet Engineering Task Force), New York, NY, USA, Tech. Rep. 2409, Nov. 1998.

[17] .H. Krawczyk, "SIGMA: The 'SIGn-and-MAc' approach to authenticated Diffie-Hellman and its use in the IKE-protocols," in Proc. CRYPTO 2003, pp. 400–425.

[18]. H. Krawczyk, "HMQV: A high-performance secure Diffie-Hellman protocol," in Proc. CRYPTO 2005, pp. 546–566.

[19] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated Key Exchange Secure against Dictionary Attacks," Proc. 19th Int'l Conf. Theory and Application of Cryptographic Techniques (Eurocrypt '00), pp. 139-155, 2000.

[20] S. Bellovin and M. Merritt, "Encrypted Key Exchange: Password- Based Protocol Secure against Dictionary Attack," Proc. IEEE Symp. Research in Security and Privacy, pp. 72-84, 1992.

[21] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," Proc. 21st Ann. Int'l Cryptology Conf. (Crypto '01), pp. 213-229, 2001.

[22] S. Halevi and H. Krawczyk, "Public-Key Cryptography and Password Protocols," ACM Trans. Information and System Security, vol. 2, no. 3, pp. 230-268, 1999.

[23] H. Jin, D.S. Wong, and Y. Xu, "An Efficient Password-Only Two- Server Authenticated Key Exchange System," Proc. Ninth Int'l Conf. Information and Comm. Security (ICICS '07), pp. 44-56, 2007.

[24] J. Katz, R. Ostrovsky, and M. Yung, "Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques: Advances in Cryptology (Eurocrypt '01), pp. 457-494, 2001.