GLOBAL JOURNAL OF ADVANCED ENGINEERING TECHNOLOGIES AND SCIENCES

CAN WE BE FRIENDS? MATCH-PAIR ME IF WE HAVE ENOUGH ATTRIBUTES IN COMMON

Solomon SARPONG
Department of Biological, Physical and Mathematical Science, School of Natural Resources and Environmental Sciences, Somanya, Ghana

ABSTRACT

In order for some persons to make friends, they indulge in social networking. Since the advent of matchmaking on social networks, many protocols have been proposed. However, security and privacy of users' attributes are the main concerns in most of the existing matchmaking protocols. Also, much consideration has not been given to how many attributes users should have in common before they are matched. Furthermore, only the initiator knows the common attributes they have in common. These issues inhibit the full patronage of mobile social network by some persons as it encourages malicious operations. In lieu of these, this paper proposes protocol that is robust against the upmentioned security issues. In this protocol, the initiator sets a criterion for a match-pair to be made. Only users that meet this criterion qualify to be match-paired. Furthermore, in order to ensure privacy of users' attributes, the attributes are exchanged only when they are match-paired and disclosed to the matched-pair only. The protocol can resist semihonest and malicious attacks.

KEYWORDS: Matchmaking, Social Network, privacy-preserving, matched-pair, and communication range

INTRODUCTION

Private set intersection is used when two users with sets want to know the intersection of their sets without disclosing any other information in their sets apart from the content of the intersection. In some cases, there arises the need for two or more parties to exchange information in some situations. The parties may be willing to exchange the information or maybe under compulsion. In any of these cases, the information should be shared in such a way that, neither parties gets to know more information than they are entitled to. This brings to the fore the need to use private set intersection (PSI). Usually in such information sharing scenarios, one is looking for the information and the other maybe be willing or under compulsion to share it. Hence, the problems encountered are; how can the sharing be done such that the persons involved learn no (or minimal) other information beyond what they are required to and practically, how can it be done [1]. In a situation where two parties have independent set of attributes and want to find their common attributes, this should be done such that, no other information is learnt by any of them apart from what they have in common. To the best of my knowledge, apart from the protocols in [2], [3], [4], [5], [6], most of the existing proposed matchmaking protocols match-pair the users without checking if they have enough attributes to make them a good pair. Furthermore, in these protocols the best match is an individual with the maximum number of common attributes with the initiator. These protocols do not allow the initiator to find a pair that has enough attributes common attributes. It can be observed that in these protocols, a matched-pair may not have enough attributes to be a good pair. However, the matchmaking process in (Sarpong et al., 2015), (Sarpong & Xu, 2015), (Sarpong & Xu, 2014), (Sarpong & Xu, 2014) and (Sarpong & Xu, 2015) address this issue by setting a criterion for matching. As a further improvement on these, the protocols in this paper proposes is efficient and privacy-preserving matchmaking protocol. This paper proposes a protocol that is efficient as the person looking for a matching pair sets the minimum number of common attributes s/he should share with another to qualify as a match-pair. Also, when the protocol ends, they get to know only the number of attributes the users have in common. Furthermore, the protocol is privacy-preserving as only the user(s) that has the most number of attributes in common with the initiator gets to know the actual type of attributes.

RELATED WORKS

A private matchmaking protocol is an aspect of private set intersection (PSI). Variants of PSI can be found in [12], [13] and [14]. In Oblivious transfer (OT) protocol, a server transfers items to a client, the client then chooses the items s/he wants but keeps the choice secret (client does not know anything about the other items). That is, the protocol is one-way. PSI protocols can be constructed from OT [15] and [16]. As improvement on these protocols, [1] used threshold cryptosystem to solve set matching problems. Different forms of PSI can be found in (Ateniese, et al., 2011), [18], [19] and [20]. There was the implementation of PSI and private cardinality of set intersection protocols in protocols based on oblivious pseudo-random function [16]. Using efficiently secure protocol for set intersection and pattern matching, [21] securely computed set intersection functionality based on secure pseudo-random function evaluations. This is in contrast to previous protocols that are based on polynomials. In addition, utilizing specific properties of Naor-Reingold pseudo-random function, a secure pseudo-random function evaluation in order to achieve secure pattern matching is achieved. In [22], there is an improvement in oblivious pseudo-random function. Using threshold cryptography in PSI, [23] proposed a PSI protocol in which the intersection is satisfied if it is greater than a threshold agreed on. [24] used commutative encryption to achieve PSI and cardinality of set intersection. This has the property that $Ek1\ [Ek2\ (x)] = Ek2\ [Ek1\ (x)]$. They demonstrated that the same encryption can be achieved by using two private keys $k1$ and $k2$ despite the order of encryption. [14] also demonstrated that commutative encryption function can be achieved with the power function $f e\ (x) = x\ emod\ p$. A commonly related disadvantage of this method is that it often provides a weaker security [25]. The problem of matchmaking has been how best to protect users' privacy. To address this pertinent issue, some protocols in matchmaking have been proposed. These protocols are categorized as: the use of a trusted central authority [26], [27] and (Li et al., 2008); the distributed technique [3], [29], [30], [31], [32], [33] and (Wang et al., 2012); and the hybrid technique (Wang, Li, et al., 2013), (Sarpong & Xu, 2015), (Sarpong et al., 2016), (Sarpong & Xu, 2014), (Sarpong & Xu, 2015), (Sarpong & Xu, 2014), [10] and [36].

MATCHMAKING PROTOCOL

The proposed matchmaking protocol is based on the one proposed by [14] with some modifications. These modifications are to make it more secured and guard against would be attacks inherent in it. In this protocol, it can be observed that Alice and Bod may not have any common attributes or their common attributes maybe too small to make them a good matching-pair. When this happens, they may not want to continue with any further communication. Hence, this matchmaking scheme would have leaked individual private attributes even though they are not matchpair. Furthermore, the attributes are sorted lexicographically hence, if any of the persons in the matchmaking protocol maliciously randomizes the attributes, the other cannot compute the intersection set whilst the other can (Sarpong et al., 2015). In order to avoid these, we propose a protocol that is efficient, secure and ensures the privacy of users' attributes. In order to maintain the security and privacy of users' attributes, these privacy levels are considered (Sarpong et al., 2016); Privacy level 1: At the end of the protocol, the initiator and the candidate(s) mutually learn their intersection set. An adversary learns nothing. Privacy level 2: At the end of the protocol, the initiator and the candidate(s) mutually learn the size of their intersection set. An adversary learns nothing. Privacy level 3: At the end of the protocol, the initiator and the candidate(s) with at least $AThreshold$ number of attributes will mutually learn the actual attributes they have in common. An adversary learns nothing. This proposed matchmaking protocol consists Alice (the initiator) and a set of other candidates. Alice wishes to form a match-pair with a candidate that has enough attributes with her. All the persons in this matchmaking protocol can communicate with the Bluetooth or WiFi on their phones. To be a match-pair of Alice, the candidate must possess a minimum threshold number of common attributes. When the number of attributes common to all the persons in the protocol is at least the threshold set, Alice and the candidate(s) exchange their attributes. However, if the number of attributes common to Alice and the candidate(s) in the protocol is less than the threshold set, they do not become a matching pair. Hence, only the number of the attributes common to both of them will be compromised but not the actual attributes. In this protocol, all computations are done with modulo p where p is a safe prime. Furthermore, in this protocol two attributes are the same if they are semantically the same. Assume Alice has attributes $A = (a1\ , a2\ , \ldots , an\ )$ and each of the candidates have $Ci = (c1i\ , c2i\ , \ldots , cni)$ attributes. Alice chooses a random number kA; likewise, each candidate chooses a random number kci . These random numbers are chosen from a range of $[1, q - 1]$ and $q = (p - 1)\ 2 ⁄$. They agree on a collision resistant cryptographic hash function, $h()$. Each of them create a and RSA-key pair. Alice creates $(eA, dA\ )$ and makes eA together with her username public. Also, each candidate creates an RSA-key pair $(eci\ , dci\ )$ and makes eci together with the username public. Alice exponentiates each of her attributes with her random number and hashes the output and sends to each candidate. Each candidate also exponentiates his/her attributes with the random number and hashes the output and sends to Alice. Alice uses the random reordering function πA to reorder the values she received from each of the candidates in step 2 to have, $Y = \{h(b1\ )\ kAkci, h(b2\ )\ kAkci, \ldots , h(bn\ )\ kAkci\}$ which she sends to each candidate. With the random reordering, πci , each candidate computes $Zi = \{h(c1i\ )\ kci\ kA, h(c2i\ )\ kci\ kA, \ldots ,$

$h(cni)$ kci $kA\}$ and sends to Alice. Algorithm: Matchmaking Protocol for Computing the Intersection of Attributes Input: Private set of Alice, A = ($a1$, $a2$,. . . , an), a chosen random number kA, RSA-key pair (eA, dA) and a random permutation πA, Alice makes eA public. Private set of the candidates Ci = ($c1i$, $c2i$, . . . , cni); chosen random numbers kci , RSA-key pair (eci , dci) and a random permutation πci . Each candidate makes his/her eci public. 1. Alice does the following computations $\{h(a1$) kA, $h(a2$) kA, . . . , $h(an$) $kA\}$ and sends to each candidate 2. Each candidate does the following computations $\{h(c1i$) kci, $h(c2i$) kci, . . . , $h(cni)$ $kci\}$ and sends to Alice. 3. Alice uses her random permutation πA to reorder the values she received in step 2. After computing the reordering, she sends Y = $\{h(c1i$) $kAkci$, $h(c1i$) $kAkci$, . . . , $h(c1i$) $kAkci\}$ to each candidate. 4. Each candidate uses the random permutation πci to reorder the values they received in step 1. After computing the reordering, s/he sends Zi = $\{h(a1$) kci kA, $h(a2$) kci kA, . . . , $h(an$) kci $kA\}$ to Alice. 5. The intersection $Y \cap Z$ is computed by each of the persons in the protocol. The computation of $Y \cap Z$ makes them know the number of attributes they have in common. In step 5, when Alice and each candidate compute the intersection $Y \cap Z$, the number of attributes common to all the persons in the protocol will be known by each of them (only if $Y \cap Z$ is not an empty set). A candidate and Alice become a match-pair if the intersection $Y \cap Z$ is at the minimum threshold set by Alice. With the minimum threshold number of common attributes achieved, Alice and the candidate(s) exchange their random permutations. Alice sends the random permutation to the candidate(s) by sending $signeci$ ($usernameAlice \| \pi A$). Also, the candidate(s) send the random permutation to Alice by sending $signeA$ ($usernamecandidate(s)$ $\| \pi ci$). After they have successfully exchanged their random numbers, the actual attributes common to all the persons in the protocol will be known by each of them.

SECURITY ANALYSIS OF THE PROTOCOL

In steps 1 and 2 of the algorithm, Alice and the candidates receive exponentiated and hashed attributes from each other. Hence, this makes it computationally impossible for the candidate(s) to map $h(ai$) kA to ai . As a result, even if the candidate(s) happens to know kA, the candidate cannot compute ai from $h(ai$) kA in polynomial time. In like manner, Alice receives exponentiated and hashed attributes from the candidates. This makes it computationally impossible for Alice to map $h(c1i$) kci to $c1i$. Even if Alice knows kci , she cannot compute $c1i$ from $h(c1i$) kci in polynomial time. Furthermore in steps 3 and 4, given the values $\{h(c1i$) kci kA, $h(c2i$) kci kA, . . . , $h(cni)$ kci $kA\}$ Alice received from the candidates, she cannot compute ($c1i$, $c2i$, . . . , cni) in polynomial time. Hence, she cannot map say $cn-1$ correctly to the corresponding attributes in $\{h(c1i$) kci kA, $h(c2i$) kci kA, . . . , $h(cni)$ kci $kA\}$ in polynomial time. Likewise, given the values $\{h(a1$) kci kA, $h(a2$) kci kA, . . . , $h(an$) kci $kA\}$ which the candidates received from Alice, they cannot compute for ($a1$, $a2$,. . . , an) in polynomial time. Hence, the candidates cannot map say $an-1$correctly to the corresponding attributes in $\{h(a1$) kci kA, $h(a2$) kci kA, . . . , $h(an$) kci $kA\}$. Unlike [14], the values Y and Z are not arranged lexicographically. This is to enhance security in this protocol. In this protocol, as Y and Z values are randomly reordered, both Alice and Bob cannot know the attributes in $Y \cap Z$ unless they exchange their random numbers. As a result, in this protocol even if a candidate re-arranges Y, Alice will still be able to compute the intersection. This assertion also applies to the case of a candidate when Alice tries to be malicious by re-arranging Z. Table 1: Comparison of the security features in this protocol with some other matchmaking protocols Protocol Attack on privacy level 1 Attack on privacy level 2 Attack on privacy level 3 semimalicious attack Number of common attributes This protocol Yes Yes Yes Yes Yes Wang et al [3] Yes Yes Yes Yes No Xie and Hengartner [20] Yes Yes Yes Yes No Agrawal et al [14] No No No Yes No

CONCLUSION

We have proposed a protocol that is efficient and privacy preserving. In this protocol, common attributes are exchanged by the individual only when they meet a minimum threshold number of common attributes set by the initiator of the matchmaking. Hence, before Alice and any of the candidates exchange their attributes they would have met a minimum threshold number of common attributes set by Alice. Also, in this proposed protocol only the matchedpair know the attributes they have in common.

REFERENCE

[1] L. Kissner and D. Song, “Privacy-Preserving Set Operations,” in Advances in Cryptology -- CRYPTO 2005, 2005, pp. 241–257.

[2] Y. Wang, T. Zhang, H. Li, L. He, and J. Peng, “Efficient Privacy Preserving Matchmaking for Mobile Social Networking against Malicious Users,” 2012, doi: 10.1109/TrustCom.2012.142.

[3] M. Li, N. Cao, S. Yu, and W. Lou, “FindU: Privacy-preserving personal profile matching in mobile social networks,” Proc. - IEEE INFOCOM, no. 1, pp. 2435–2443, 2011, doi: 10.1109/INFCOM.2011.5935065.

[4] M. Li, S. Yu, N. Cao, and W. Lou, “Privacy-Preserving Distributed Profile Matching in Proximity-Based Mobile Social Networks,” IEEE Trans. Wirel. Commun., vol. 12, no. 5, pp. 2024–2033, 2013, doi: 10.1109/TWC.2013.032513.120149.

[5] Y. Wang, J. Hou, Y. W. Tan, and X. Nie, “A recommendation-based matchmaking scheme for multiple mobile social networks against private data leakage,” in Procedia Computer Science, Jan. 2013, vol. 17, pp. 781–788, doi: 10.1016/j.procs.2013.05.100.

[6] Y. Wang, H. Li, T.-T. Zhang, and J. Hou, “A Privacy Preserving Matchmaking Scheme for Multiple Mobile Social Networks,” in Algorithms and Architectures for Parallel Processing, 2013, pp. 233–240.

[7] S. Sarpong, C. Xu, and X. Zhang, “An Authenticated Privacy-preserving Attribute Matchmaking Protocol for Mobile Social Networks,” 2015.

[8] S. Sarpong and C. Xu, “Privacy-preserving attribute matchmaking in proximity-based mobile social networks,” Int. J. Secur. its Appl., vol. 9, no. 5, pp. 217–230, 2015, doi: 10.14257/ijsia.2015.9.5.22.

[9] S. Sarpong and C. Xu, “A Secure and Efficient Privacy-Preserving Attribute Matchmaking Protocol in Proximity-Based Mobile Social Networks,” in Advanced Data Mining and Applications, 2014, pp. 305–318.

[10] S. Sarpong and C. Xu, “A secure and efficient privacy-preserving matchmaking for mobile social network,” in International Conference on Computer, Network Security and Communication Engineering (CNSCE), 2014, pp. 362–366.

[11] S. Sarpong and C. Xu, “A collusion-resistant privacypreserving attribute matchmaking for mobile social networks,” Int. J. Innov. Sci. Eng. Technol., vol. 2, pp. 485–495, 2015.

[12] V. Kolesnikov, R. Kumaresan, M. Rosulek, and N. Trieu, “Efficient batched oblivious PRF with applications to private set intersection,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 818–829.

[13] V. Kolesnikov, N. Matania, B. Pinkas, M. Rosulek, and N. Trieu, “Practical multi-party private set intersection from symmetric-key techniques,” in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 1257–1272.

[14] R. Agrawal, A. Evfimievski, and R. Srikant, “Information sharing across private databases,” in Proceedings of the 2003 ACM SIGMOD international conference on Management of data, 2003, pp. 86–97.

[15] B. Pinkas, T. Schneider, G. Segev, and M. Zohner, “Phasing: Private set intersection using permutation-based hashing,” in 24th Security Symposium, 2015, pp. 515–530.

[16] M. J. Freedman, K. Nissim, and B. Pinkas, “Efficient Private Matching and Set Intersection,” pp. 1–19, 2004.

[17] G. Ateniese, E. De Cristofaro, and G. Tsudik, “(if) size matters: Size-hiding private set intersection,” in International Workshop on Public Key Cryptography, 2011, pp. 156–173.

[18] D. Dachman-soled, T. Malkin, M. Raykova, and M. Yung, “Efficient Robust Private Set Intersection,” pp. 125–142, 2009.

[19] A. Fiat and A. Shamir, “How To Prove Yourself: Practical Solutions to Identification and Signature Problems,” in Advances in Cryptology --- CRYPTO’ 86, 1987, pp. 186–194.

[20] C. Dong, L. Chen, and Z. Wen, “When private set intersection meets big data: an efficient and scalable protocol,” in Proceedings of the 2013 ACM SIGSAC conference on Computer \& communications security, 2013, pp. 789–800.

[21] C. Hazay and Y. Lindell, “Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries,” in Theory of Cryptography Conference, 2008, pp. 155–175.

[22] S. Jarecki and X. Liu, “Efficient Oblivious Pseudorandom Function with Applications to Adaptive OT and Secure Computation of Set Intersection,” in Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009, San Francisco, CA, USA, March 15-17, 2009. Proceedings, 2009, vol. 5444, pp. 577–594, doi: 10.1007/978-3-642-00457-5_34.

[23] Y. Zhao and S. S. M. Chow, “Are you the one to share? Secret transfer with access structure,” Proc. Priv. Enhancing Technol., vol. 2017, no. 1, pp. 149–169, 2017.

[24] Q. Xie and U. Hengartner, “Privacy-Preserving Matchmaking For Mobile Social Networking Secure Against Malicious Users,” 2011.

[25] B. H. Bloom, “Space/time trade-offs in hash coding with allowable errors,” Commun. ACM, vol. 13, no. 7, pp. 422–426, 1970.

[26] N. Eagle and A. Pentland, “Social Serendipity :,” Time, 2005.

[27] J. Kjeldskov and J. Paay, “Just-for-us: a context-aware mobile information system facilitating sociality,” in Proceedings of the 7th international conference on Human computer interaction with mobile devices & services, 2005, pp. 23–30.

[28] K. A. Li, T. Y. Sohn, S. Huang, and W. G. Griswold, “Peopletones: a system for the detection and notification of buddy proximity on mobile phones,” in Proceedings of the 6th international conference on Mobile systems, applications, and services, 2008, pp. 160–173.

[29] L. Zhang, X.-Y. Li, and Y. Liu, “Message in a sealed bottle: Privacy preserving friending in social networks,” in 2013 IEEE 33rd International Conference on Distributed Computing Systems, 2013, pp. 327–336.

[30] [Z. Yang, B. Zhang, A. C. Champion, D. Li, D. Xuan, and J. Dai, “E-SmallTalker: A Distributed Mobile System for Social Networking in Physical Proximity,” in 2010 IEEE 33th International Conference on Distributed Computing Systems, Jun. 2010, pp. 468–477, doi:10.1109/ICDCS.2010.56.

[31] R. Lu, X. Lin, and X. Shen, “SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 3, pp. 614–624, 2013, doi: 10.1109/TPDS.2012.146.

[32] A.-K. Pietiläinen, E. Oliver, J. LeBrun, G. Varghese, and C. Diot, “Mobiclique: middleware for mobile social networking,” in Proceedings of the 2nd ACM workshop on Online social networks, 2009, pp. 49–54.

[33] X. Liao, S. Uluagac, and R. A. Beyah, “S-match: Verifiable privacy-preserving profile matching for mobile social services,” in 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2014, pp. 287–298.

[34] B. Wang, B. Li, and H. Li, “Gmatch: Secure and privacy-preserving group matching in social networks,” in 2012 IEEE Global Communications Conference (GLOBECOM), 2012, pp. 726–731.

[35] S. Sarpong, C. Xu, and X. Zhang, “PPAM: Privacy-preserving attributes matchmaking protocol for mobile social networks secure against malicious users,” Int. J. Netw. Secur., vol. 18, no. 4, pp. 625–632, 2016.

[36] E. De Cristofaro, A. Durussel, and I. Aad, “Reclaiming privacy for smartphone applications,” 2011 IEEE Int. Conf. Pervasive Comput. Commun. PerCom 2011, no. March, pp. 84–92, 2011, doi: 10.1109/PERCOM.2011.5767598. s