International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 4, April - 2013

Trust Establishment Through Digital Credential For Multisession Transaction

Shruthi. J
M.Tech Student, VTU
Computer Networking, EWIT
Bangalore.

Shruthi T. V
Assistant Professor,
Department Of ISE, EWIT
Bangalore.

Abstract - Trust Negotiation has shown to be a successful, policy-driven approach for automated trust establishment, through the release of digital credentials. Current real applications require new flexible approaches to trust negotiations, especially in light of the widespread use of mobile devices. In this paper, we present a multisession dependable approach to trust negotiations. The proposed framework supports voluntary and unpredicted interruptions, enabling the negotiating parties to complete the negotiation despite temporary unavailability of resources. Our protocols address issues related to validity, temporary loss of data, and extended unavailability of one of the two negotiators. A peer is able to suspend an ongoing negotiation and resume it with another (authenticated) peer. Negotiation portions and intermediate states can be safely and privately passed among peers, to guarantee the stability needed to continue suspended negotiations. We present a detailed analysis showing that our protocols have several key properties, including validity, correctness, and minimality. As by our complexity analysis, the introduction of the suspension and recovery procedures, and mobile negotiations does not significantly increase the complexity of ordinary negotiations.

Keywords— **Security and management, dependability, trust negotiations, access control**

I. Introduction

TRUST negotiation is a mechanism supporting complex, distributed, rule-based access control for sensitive information and resources, through the controlled release of credentials [5], [24], [28]. A trust negotiation is a mutual attribute-based authorization protocol between two entities. Parties are assumed to be strangers who need to establish trust on the fly in order to exchange resources, information, or services. Current real applications require flexible approaches to trust negotiations, especially in light of the widespread use of mobile devices. Consider, for example, mobile clients negotiating accesses to services hosted on servers' clusters: negotiations may interrupt due to communication channel fault or may be voluntarily suspended, to be resumed under more favourable conditions. Mobile devices need to be able to seamlessly migrate from the different physical servers belonging to the same service provider. Also, negotiations may last a considerable time span and the involved parties may not be able to support long negotiations. Existing trust negotiation systems, however, do not currently support any form of suspension or interruption, and do not allow the negotiators to be replaced (or delegated) while the negotiation is ongoing. Interruptions in ongoing trust negotiations can be the result of external, unforeseeable events (e.g., parties' crashes, faulty transmission channels), or decisions by the involved parties. A party may not be able to advance the negotiation for temporary lack of resources. Or the party may not have readily available the credentials required by the counterpart, although eligible to them. For example, users may not have the capabilities or rights of storing certificates such as birth certificates; marriage certificates, and so forth, although entitled to them. Parties may also employ one-time credentials to conduct negotiations. Temporary and one-time credentials allow a party to disclose sensitive information while at the same limiting the possibility for an attacker to steal identity related information. Once such a credential is disclosed, it cannot be reused. Hence, completing a negotiation in which such type of credential is used becomes crucial. Interrupted negotiations however represent not only undesired events, but also vulnerabilities that could facilitate attackers' eavesdropping and other malicious behaviour. Unfortunately, there are no approaches addressing such an issue. Trust negotiation research has mostly focused on the assurance of privacy and confidentiality with the goal of guaranteeing that no actual information about a negotiator's properties is disclosed to the counterpart [28], [19], [3]. Typically, these approaches rely on strong cryptographic assumptions, and are seldom applicable in many real-world scenarios, where properties, stated in digital credentials, actually need to be disclosed in clear and not only proved to be true. For example, just proving the possession of a valid credit card is not sufficient to complete a transaction, and actual account information is to be supplied in order to enable

charging the amount spent. Additionally, protocols that rely on oblivious credentials or anonymous credentials do not allow parties to follow the progress of the negotiation, since information regarding policies satisfaction is hidden for confidentiality purposes [22], [17]. It is thus crucial to extend trust negotiation protocols along several dimensions. First and foremost, the protocols must be able to adapt to context changes and be dependable. A long lasting trust negotiation should successfully withstand suspensions and interruptions. Also, given the ubiquitous nature of online peer-to-peer systems, and the increasing number of moving objects involved in online transactions, negotiators must be allowed to switch roles while the negotiation is ongoing, so to guarantee dependability, when contextual conditions, such as availability of resources and peers. In this paper, we introduce a novel approach to trust negotiations that offers a general solution to those issues by developing major extensions to previous approaches by us and others [4], [37], [30]. The core of our approach is a trust negotiation protocol supported by the Trust-X system. This protocol, referred to as multisession trust negotiation, involves the exchange of digital credentials protected by rule based disclosure policies (referred to as disclosure policies) which make it possible for two (or more) peers to establish mutual trust, so to carry on tasks such as the exchange of sensitive resources or access to a protected service. The main innovative feature of our proposed protocol is that it supports crash recovery and the possibility of completing the negotiation over multiple sessions. To support the execution of multisession negotiations, we extend the original Trust-X conventional negotiation steps. Save points are employed to save the negotiation state, validity checks concerning events which may happen during the negotiation suspension and could possibly invalidate the negotiation steps executed before the suspension. Examples of those events include credential revocation or expiration, or modification of disclosure policies by one of the peers. An additional novel feature of the proposed framework is that it supports mobile negotiations, that is, negotiations that can be transferred among different peers in different sessions. With mobile we mean that a peer is able to suspend an ongoing negotiation and resume it with a peer different from the peer with which the negotiation started. Under our approach, negotiation portions and intermediate states can be safely and privately be transferred among peers. To support the secure transfer of negotiations, we have defined an authentication protocol, based on a secret splitting scheme combined with a zero-knowledge proof protocol, to verify the identity of the peer recovering the negotiation and to assure the validity of the exchanged data. Our negotiation protocol also provides a mechanism for recovering from data losses which may occur at one of the involved peers. In the paper, we present a detailed analysis showing that our protocols have several key properties, including validity, correctness, and minimality. Also, we show how our negotiation protocol can withstand the most significant attacks. As by our complexity analysis, the introduction of the suspension and recovery procedures and mobile negotiations does not significantly increase the complexity of ordinary negotiations. We provide some evaluation results, showing the protocols' performance. In summary, the contribution of this paper is an approach supporting multisession and mobile trust negotiations

II. Problem Statement

Existing trust negotiation systems, however, do not currently support any form of suspension or interruption, and do not allow the negotiators to be replaced (or delegated) while the negotiation is ongoing. Interruptions in ongoing trust negotiations can be the result of external, unforeseeable events or decisions by the involved parties. A party may not be able to advance the negotiation for temporary lack of resources. Or the party may not have readily available the credentials required by the counterpart, although eligible to them. For example, users may not have the capabilities or rights of storing certificates such as birth certificate, marriage certificates, and so forth, although entitled to them. Parties may also employ one-time credentials to conduct negotiations. Temporary and one-time credentials allow a party to disclose sensitive information while at the same limiting the possibility for an attacker to steal identity related information. Once such a credential is disclosed, it cannot be reused. Hence, completing a negotiation in which such type of credential is used becomes crucial. Interrupted negotiations however represent not only undesired events, but also vulnerabilities that could facilitate attackers' eavesdropping and other malicious behavior. Unfortunately, there are no approaches addressing such an issue.

Disadvantages in Existing System

- Existing trust negotiation systems, however, do not currently support any form of suspension or interruption.
- Do not allow the negotiators to be replaced (or delegated) while the negotiation is ongoing.

- Interrupted negotiations however represent not only undesired events, but also

vulnerabilities that could facilitate attackers' eavesdropping and other malicious behavior.

III. Related Work

The proposed system is multisession dependable approach to trust negotiations. The proposed framework supports voluntary interruptions, enabling the negotiating parties to complete the negotiation despite temporary unavailability of resources. In designing the protocols, we have considered all possible issues related to authentication, validity, content secrecy of the trust negotiation tickets in the system. To this extent, we introduced protocols for mobile negotiations. Using Trust-X, a peer is able to suspend an ongoing negotiation and resume it with another (authenticated) peer. The protocols presented in this work can be applied to any trust negotiation system that adopts a two phase negotiation protocol. Proposed system uses the trust negotiation in online movie selection and purchase process. In online movie purchase following task are take place.

- Movie list display
- Movie selection
- Discount Coupon entry and validation
- Movie purchase cost calculation considering with discount coupon
- Credit Card Payment
- Credit Card Validation
- Payment Approval
- Movie Download

Proposed system has two applications one is running in Web Server and another one is running in Android mobile phone. Admin user who is the online trade management person will interact with application in Web Server and upload the movies in the cloud. End user is a movie buyer who is having the android mobile and application is installed in his mobile.

IV. Framework of Multisession

Suppose that user Alice (A, from now on) would like to buy from Best Buy (B, from now on) a DRM-protected digital movie using a coupon allowing her to obtain a discount on the movie price. We refer to Fig for a graphical representation of the example. A connects to B from her PDA, and initiates a negotiation with one of the servers operating for B and identified as in charge of the negotiation for B's. Let this server be denoted by B1, in Fig. we use the double stroke to highlight the active server of B. In order to provide the required movie, B1 requests from A the coupon and the amount of e-cash required to buy the movie. Once B1 is collected the coupon and calculate the amount, it will send to A, Now A can able to go for payment or suspension process. If A is going for payment he has to fill his credit card details and proceed or he wan to suspend the operation then A requires some credentials from B1. Before generating the credential B1 ask A to enter a secure 4 digit pin number, which is going to use for verification process. Once A enter the pin number B1 pass the process to B2 which will create the credentials and send it to the A through SMS. Once B1 is collected the coupon and calculate the amount, it will send to A, Now A can able to go for payment or suspension process. If A is going for payment he

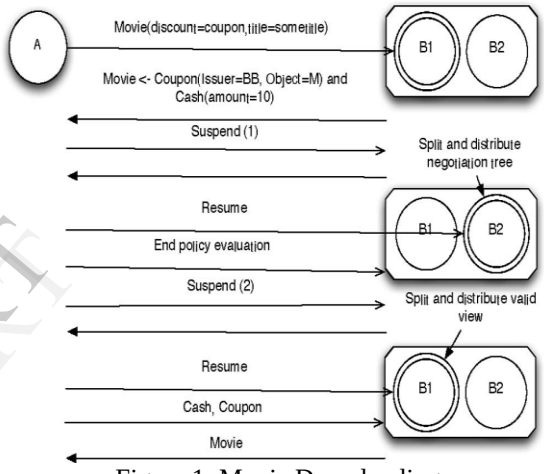

Figure 1: Movie Downloading

This policy is encoded by a rule of the form:

$$Movie(Discount = coupon, title = sometitle) \leftarrow Coupon(Issuer = BestBuy, Object = Movie) \wedge Cash(amount = 10).$$

has to fill his credit card details and proceed or he wan to suspend the operation then A requires some credentials from B1. Before generating the credential B1 ask A to enter a secure 4 digit pin number, which is going to use for verification process. Once A enter the pin number B1 pass the process to B2 which will create the credentials and send it to the A through SMS. Then A can able to end the session. When A is next time entering it is not necessary for A to select the movie and produce the coupon etc, just he can enter into multi-session option and produce the credential which was previously generated he can able to proceed in the transaction where he left early.

Advantages of Proposed System

- Proposed system is a trust negotiation system, which support two type of suspensions.

- Allow the negotiators to be replaced (or delegated), that means with one customer suspension ticket another valid customer can able to enter into the system and continue in transaction with efficient validation.

- Proposed system is Attackers proof system in multi-session trust negotiation.

V. Proposed Algorithm

The security analysis is done using AES algorithm the technique of encryption decryption is done using this algorithm.AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits , and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification *per se* is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.AES operates on a 4×4 column-major order matrix of bytes, termed the *state*, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. The numbers of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

High-level description of the algorithm

1. KeyExpansion—round keys are derived from the cipher key using Rijndael's key schedule.

2. Initial Round
    1. AddRoundKey—each byte of the state is combined with the round key using bitwise xor.
3. Rounds
    1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
    3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
    4. AddRoundKey
4. Final Round (no MixColumns)
    1. Sub Bytes
    2. ShiftRows
    3. AddRoundKey

The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the secret level. Top secret information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use. AES has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. By 2006, the best known attacks were on 7 rounds for 128-bit keys, 8 rounds for 192-bit keys, and 9 rounds for 256-bit keys.

VI. System Design

Proposed system is for Android mobile users, this system has two applications one is J2EE application which is going to run in web server and another one is Android application which going to run on the users mobile phone. This system has following modules

J2EE Application

Admin User Session

- Login
- User Module (View, Add, Delete, Edit)
- Coupon Type (View, Add, Delete, Edit)
- Discount Coupon (View, Add, Delete, Edit)
- Movie Module (View, Add, Delete, Edit)
- View Transaction (View)
- Change Password

Android Application

- User Registration
- Login
- Home Page
  - View Movies Details
  - Purchase Movies
    - Select Movie
    - Provide Discount Coupon and Get the amount to be paid
      - Payment Suspend Transaction [Optional]
        - Generate Credentials and Send as SMS / Mail
      - Payment (Card Details)
        - Download Suspend Transaction [Optional]
          - Generate Credentials and Send as SMS / Mail
        - Start Download
  - Multisession Trust Negotiations
    - Upload Credentials
      - Identify The Credentials Type (Payment / Download)
      - Credential Result (Valid / Invalid)
      - Resume Operation
        - Type 1 – Start with Payment
        - Payment Details (Card Details)
        - Card Validation
          - Download Movie
          - Suspend Transaction [Optional]
            - Generate Credentials and Send as SMS / Mail
        - Type 2 – Start with Download
          - Show Confirmation
          - Start Download
      - Change Password

VII. CONCLUSION

In this paper, we have presented a multisession dependable approach to trust negotiations. The proposed framework supports voluntary interruptions, enabling the negotiating parties to complete the negotiation despite temporary unavailability of resources. In designing the protocols, we have carefully considered all possible issues related to validity, temporary loss of data, and extended unavailability of one of the two negotiators. To this extent, we introduced protocols for mobile negotiations. Using Trust-X, a peer is able to suspend an ongoing negotiation and resume it with another (authenticated) peer. The protocols presented in this work can be applied to any trust negotiation system that adopts a two phase negotiation protocol. It is part of our future work to further investigate how to migrate the proposed protocols to any general trust negotiation infrastructure.

REFERENCES

[1] A.V. Aho, J.E. Hopcroft, and J.D. Ullman, The Design and Analysis of Computer Algorithms. Addison-Wesley, 1974.
[2] M.Y. Becker, C. Fournet, and A.D. Gordon, "Design decentralize authorization and Semantics of Decentralized Authorization Language," Proc. IEEE 20th Computer Security Foundations Symp. (CSF), pp.3-15,2007.
[3] E. Bertino, E. Ferrari, and A.C. Squicciarini, "Privacy-Preserving Trust Negotiation," Proc. Fourth Privacy Enhancing TechnologiesWorkshop, May 2004.
[4] E. Bertino, E. Ferrari, and A.C. Squicciarini, "Trust-X: A Peer-to-Peer Framework for Trust Establishment," IEEE Trans. Knowledge Data Eng., vol. 16, no. 7, pp. 827-842, July 2004.
[5] E. Bertino, E. Ferrari, and A.C. Squicciarini, "Trust Negotiations:Concepts, Systems and Languages," Computing in Science Eng.,vol. 6, no. 4, pp. 27-34, 2004.
[6] E. Bertino, I. Ray, A.C. Squicciarini, and E. Ferrari, "Anonymity Preserving Techniques in Trust Negotiations," To appear in Proc. Fifth Privacy Enhancing Technologies Workshop, 2005.
[7] F. Boudot, "Efficient Proofs that a Committed Number Lies in an Interval," Proc. EUROCRYPT, pp. 431-444, 2000.
[8] K.D. Bowers, L. Bauer, D. Garg, F. Pfenning, and M.K. Reiter, "Consumable Credentials in Linear-Logic-Based Access-Control Systems," Proc. Network and Distributed System Security Symp. (NDSS), 2007.
[9] S.A. Brands, Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, 2000.
[10] J. Camenisch and E.V. Herreweghen, "Design and Implementation of the Demix Anonymous Credential System," Proc. ACM Conf. Computer and Comm. Security, pp. 21-30, 2002.
[11] D. Chaum, "Showing Credentials without Identification Transferring Signatures between Unconditionally Unlinkable Pseudonyms," Proc. Int'l Conf. Cryptology on Advances in Cryptology (AUSCRYPT), pp. 246-264, 1990.
[12] I. Damga°rd and E. Fujisaki, "A Statistically-Hiding Integer Commitment Scheme Based on Groups with Hidden Order," ASIACRYPT '02: Proc. Eighth Int'l Conf. Theory and Application of

Cryptology and Information Security: Advances in Cryptology, pp. 125- 142, 2002.
[13] E. Ferrari, A. Squicciarini, and E. Bertino, "X-tnl: An Xml Language for Trust Negotiations," Proc. IEEE Fourth WorkshopPolicies for Distributed Systems and Networks, June 2003.
[14] A. Fiat and A. Shamir, "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," Proc. Int'l Cryptology Conf. (CRYPTO '86), pp. 186-194, 1986.
[15] D. Garg, L. Bauer, K.D. Bowers, F. Pfenning, and M.K. Reiter, "ALinear Logic of Authorization and Knowledge," Proc. European Symp. Research in Computer Security (ESORICS), pp. 297-312, 2006.
[16] A. Hess, J. Jacobson, H. Mills, R. Wamsley, K.E. Seamons, and B. Smith, "Advanced Client/Server Authentication in TLS," Proc. Network and Distributed System Security Symp. (NDSS), 2002.
[17] J.E. Holt, R.W. Bradshaw, K.E. Seamons, and H. Orman, "Hidden Credentials," WPES '03: Proc. ACM Workshop Privacy in the Electronic Soc., pp. 1-8, 2003.
[18] W. Hu, N. Jian, Y. Qu, and Y. Wang, "Gmo: A Graph Matching for Ontologies," Proc. Workshop Integrating Ontologies, 2005.
[19] T. Yu, K.E. Seamons, and M. Winslett, "Protecting Privacy During
on Line Trust Negotiation," Proc. Second Int'l Conf. Privacy Enhancing Technologies, Apr. 2002.
[20] H. Krawczyk, "Secret Sharing Made Short," CRYPTO '93: Proc. 13th Ann. Int'l Cryptology Conf. Advances in Cryptology, pp. 136-146, 1993.
[21] A.J. Lee and M. Winslett, "Enforcing Safety and Consistency Constraints in Policy-Based Authorization Systems," ACM Trans. Information and System Security, vol. 12, no. 8, pp. 1-33, Dec. 2008.
[22] J. Li and N. Li, "Oacerts: Oblivious Attribute Certificates," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 4, pp. 340-352, Oct.-Dec. 2006.
[23] N. Li and J.C. Mitchell, "Datalog with Constraints: A Foundation for Trust Management Languages," Proc. Fifth Int'l Symp. Practical Aspects of Declarative Languages, Jan. 2003.
[24] W. Nejdl, D. Olmedilla, and M. Winslett, "PeerTrust: Automated Trust Negotiation for Peers on the Semantic Web," Proc. Workshop Secure Data Management in a Connected World (SDM '04), Aug. 2004.
[25] Organization for the Advancement of Structured Information Standards (OASIS) "Security Assertions Markup Language (SAML), Version 2.0," http://wiki.oasis-open.org/security, 2005.
[26]T.P. Pedersen, "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing," CRYPTO '91: Proc. 11th Ann. Int'l Cryptology Conf. Advances in Cryptology, pp. 129-140, 1991.
[27]Y. Qu, W. Hu, and G. Cheng, "Constructing Virtual Documents for Ontology Matching," Proc. 15th Int'l Conf. World Wide Web (WWW), pp. 23-31, 2006.