Secure Key Distribution over TOR Networks in Mobile Social Networks

Mr.S.Sasikumar[1], Ms.N.Radhika[2], Mr.U.Saravanakumar[3]

[1]PG Student, [2]Assistant Professor, [3]PG Student, Department of Computer Science and Engineering,

PRIST University, Trichy District, India

[1] sasik817@gmail.com

Abstract

In this paper, we explore the functional and security requirements for these new systems, such as availability, security, and privacy, and present several design options for building secure encounter-based social networks. To construct a flexible framework for secure encounter-based social networks. This can be used to construct networks that offer different security, privacy, and availability guarantees. To ideal encounter-based social networks need to satisfy, and introduce a generic framework for constructing encounter-based social networks.

INTRODUCTION

Encounter-based social networks and encounter-based systems link users who share a location at the same time, as opposed to the traditional social network. In this paper, we provide the functional and security requirements for these new systems, such as availability, security, and privacy. In our design, we use the X.509 standard for certification without any modification to the structure of the certificate, but limit the attributes in the certificate to preserve the privacy of our users. Our certification and visual authentication schemes are very simple. Here, we consider two design schemes. 1. Immediate Key Exchange 2. Delayed Key Exchange. First, an sender generates a pair of public and secret keys (PK,SK), computes the hash value of her own image and other relevant information to a certificate request, and sends it to a signing authority.

Second, the signing authority checks the validity of the metadata in the certificate request and verifies the validity of relation with the certificate. If the verification process is successful, the signing authority signs the certificate using its own private key and sends to sender. In Receiver side tries to verify if the certificate along with the photo have a valid signature from a trusted authority. Receiver computes the hash of the photo and other information sent by sender, comparing it to the value embedded in the certificate. If the signature is valid, then the data transmission is occurring between the sender & receiver.

In Immediate Key Exchange process, each user in the vicinity will detect the transmission and attempt to decrypt it & also it is time based process, when the user gives acknowledgement to the sender. However, only the target user will be able to decrypt the message correctly. In Delayed key exchange process is a time released process, the user public key & image are send to the user, here also only the target user will be able to decrypt the message correctly & there by providing better security in communication process.

LITERATURE SURVEY

Safe slinger: An easy-to-use and secure approach for human trust establishment

To achieve secure transmission between sources to destination Over TOR networks. To construct a flexible framework for secure encounter-based social networks. In this project, to use immediate key exchange, delayed key exchange process for secure transmission. This can be used to construct networks that offer different security, privacy, and availability guarantees.

To propose Safe Slinger, a system leveraging the proliferation of smart phones to enable people to securely and privately exchange their public keys. Safe Slinger establishes a secure channel offering secrecy and authenticity, which we use to support secure messaging and file exchange. Safe Slinger also provides an API for importing applications' public keys into a user's contact information

Drawbacks: Its requirement that users check the received contact list entries before finally importing them into their address book

Location based trust for mobile user-generated content: applications, challenges and implementations

In this paper is how to establish some trust level in the authenticity of content created by untrusted user. Advocate a secure localization and certification service that allows content producers to tag their content with a spatial timestamp indicating its physical location our approach preserves the privacy of producers by not exposing their identity to the potential content consumers.

Draw backs: Cost is high

Socialaware: Context-aware multimedia presentation via mobile social networks

Increased use of smart phones capable of running applications which access social network information enable applications to be aware of a user's location and preferences To present several of these privacy and security issues, along with our design and implementation of solutions for these issues location-based services to query local mobile devices for users' social network information, without disclosing user identity or compromising users' privacy and security

Draw backs:malicious user that wants to issue some content with false location information in the DLT certificate would move to that particular location and obtain the certificate

SMILE: encounter-based trust for mobile social services

A privacy-preserving "missed-connections" service in which the service provider is entrusted and users are not assumed to have pre-established social relationships with each other.

At a high-level, SMILE uses short-range wireless communication and standard cryptographic primitives to mimic the behavior of users in existing missed-connections .A trust is founded solely on anonymous users' ability to prove to each other that they shared an encounter in the past

Draw backs: This service is prone to linking attacks by malicious servers since users reveal their actual location information to the service provider.

MobiClique: middleware for mobile social networking

MobiClique forms and exploits ad hoc social networks to disseminate content using a store-carry-forward technique Our approach distinguishes itself from other mobile social software By removing the need for a central server to conduct exchanges, by leveraging existing social networks to bootstrap the system.

Drawbacks: Users are completely trust with a centralized service with their location.

EXISTING SYSTEM

In Existing system (SMILE) is used to facilitate secure data exchange among groups in an authentic manner using simple human factor techniques. A few malicious users colluding with the rendezvous server may possess enough information about activities of other honest users such as timestamps, locations information, and encounter keys for the server to unmask users, determining the identities of communicating parties. A specific problem of SMILE but every system using such a building block, the k-anonymity in SMILE requires that each user know the number of other nearby SMILE users in order to make sure that there are enough people around to mask the activity of an individual.

Disadvantages

In existing system does not protect against a number of common security vulnerabilities, such as the “man-in-the-middle” attack, which leads to several breaches. It does not consider location privacy & importance. SMILE is prone to an impersonation attack performed by a user present during the encounter.

Since no authentication is done during key agreement, any user can eavesdrop on the encounter information and later claim to be the party of interest. SMILE is prone to user collusion.

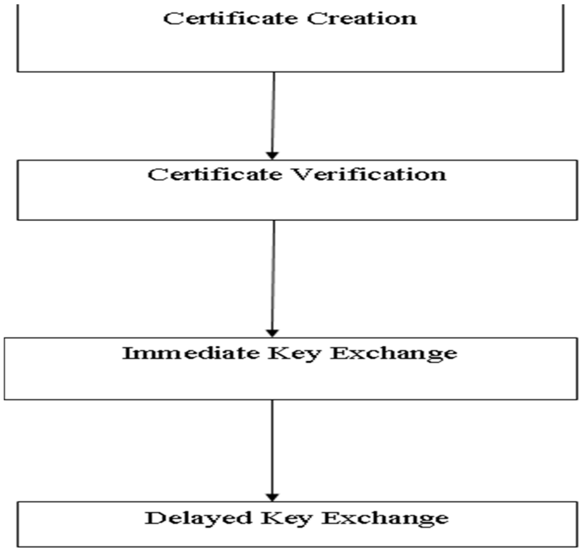
PROPOSED SYSTEM

In existing system does not protect against a number of common security vulnerabilities, such as the "man-in-the-middle" attack, which leads to several breaches. It does not consider location privacy & importance. SMILE is prone to an impersonation attack performed by a user present during the encounter. Since no authentication is done during key agreement, any user can eavesdrop on the encounter information and later claim to be the party of interest. SMILE is prone to user collusion.

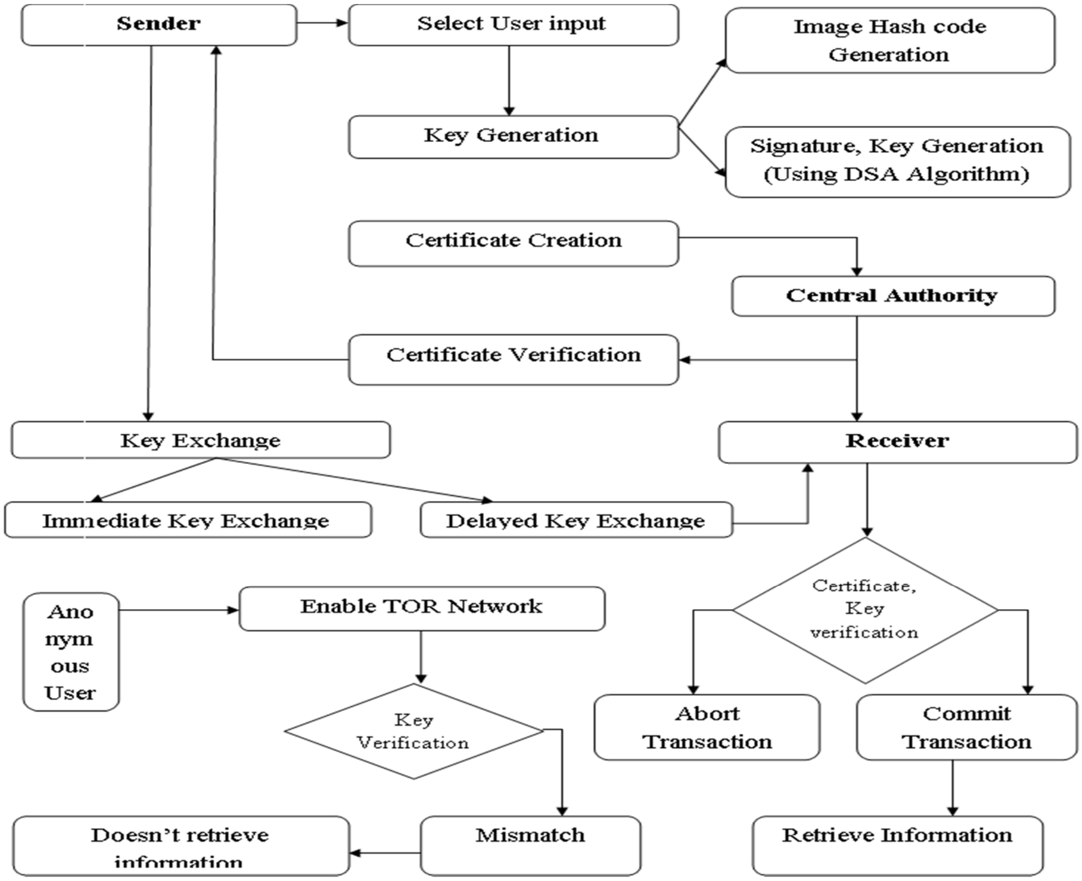
Advantages

It does not require a certification entity, yet the certification entity provides stronger guarantees for the authenticity of participants. Secure encounter-based social networks satisfy the reasonable security guarantees. These systems should provide several security guarantees, including privacy in the form of unlink ability of users sharing an encounter. And also confidentiality of data exchanged among encounter participants, and authentication of both users in a two-party conversation.

DATA FLOW DIAGRAM



Architecture Diagram



MODULES

Key Generation

In this module, the user selects the user wants to be communicate in the network. Then the user selects the file for data transmission. Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted. Modern cryptographic systems include symmetric-key algorithms (such as DES and AES) and public-key algorithms (such as RSA). Symmetric-key algorithms use a single shared key; keeping data secret requires keeping this key secret. Public-key algorithms use a public key and a private key. The public key is made available to anyone (often by means of a digital certificate). A sender encrypts data with the public key; only the holder of the private key can decrypt this data.

Image Hash code Generation

In this module, for high authentication process, the hash code is generated for the user own image, because that simple unauthenticated key agreement during the encounter is vulnerable to a man-in-the middle attack. To provide user authentication, we assume each user to have a digital certificate signed by a trusted authority with sufficient information and also to identify users, including a photo of the user. The signing authority's public key would be known to all other nodes that use our encounter-based social network.

Certificate Verification

In our design, we use the X.509 standard for certification without any modification to the structure of the certificate & also include photo of the user. Indeed, the X.509 standard allows optional attributes for biometric information such as photos, which enables us to embed visual information into the certificate. The trusted authority is responsible for ensuring that the photo provided by user for certification is an actual representative picture, and allows others to visually identify the user. The verification of the signatures embedded in the certificate is verified at the side of the receiving party of the certificates using a publicly known public key of the authority.

Immediate Key Exchange

The user select an encounter key, encrypt it to the selected user's public key, and broadcast the resulting message. Each user in the network will detect the transmission and attempt to decrypt it. However, only the target user will be able to decrypt the message correctly, and thus recover the encounter key. This method prevents the rendezvous server and colluding adversaries from determining which two users are communicating.

CONCLUSION

In our output, the certificate creation process is done with user hash value generation process. Our proposed method fulfill more requirements in terms of system security, reliability, and privacy than previous work. Our proposed encounter-based social networks satisfy, and use a generic framework for constructing encounter-based social networks. Finally, our system obtains much more security compare to other previous approaches.

REFRENCES

[1] M. Farb, M. Burman, G. Chandok, J. McCune, and A. Perrig, “Safeslinger: An easy-to-use and secure approach for human trust establishment,” Carnegie Mellon University, Tech. Rep. CMU-CyLab-11-021, 2011.

[2] C. M. Gartrell, W. C. M. Gartrell, D. S. Mishra, S. Charles M. (m., and C. Science, “Socialaware: Context-aware multimedia presentation via mobile social networks,” 2008.

[3] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, “Locationbased trust for mobile user-generated content: applications, challenges and implementations,” in HotMobile ’08: Proceedings of the 9th workshop on Mobile computing systems and applications. New York, NY, USA: ACM, 2008, pp. 60–64.

[4] J. Manweiler, R. Scudellari, and L. P. Cox, “SMILE: encounter-based trust for mobile social services,” in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 246–255.