Secure Anonymous Communication with Conditional Traceability

Ma Zhaofeng[1,2], Zhao Xibin[1,2], Guo Zhi[1,2], Gu Ming[2], Sun Jiaguang[2]

[1] Department of Computer Science and Technology, Tsinghua University
[2] School of Software, Tsinghua University
100084 Beijing, China
{mzf,zxb,guozhi,guming,sunjiaguang}@tsinghua.edu.cn

Abstract. A new anonymous secure communication protocol with conditional traceability is proposed to provide personal anonymity and privacy protection, in which a secure mapping function is introduced to provide anonymity and personal information protection, when necessary, only authority principal part can act as arbitrator for communication validation. The proposed protocol has 3 advantages: 1) mutual communication; 2) anonymity of communication. 3) conditional traceability.

1 Introduction

Information exchange and sharing are the basic target for communication network including traditional connection-oriented computer network and modern wireless, in which with the commercial development security became an important and permanent issue were concerned much more, especially in E-business, electronic cash, electronic election applications in real life. For the history reason that current IP-address-based computer network communication and wireless communication are designed initially for their communication and data exchange, which involved communication content, communication address(such as destination and source IP address in computer communication, SIM, ME,TMSI et al.), message header, control information, which are close related to user identity or the location and topology of user's network, content-based behavior analysis, usage pattern mining can be employed to deduce user's habit, preference easily. For the reason of fairness, privacy and legislation, user anonymity becomes another important issues in security-related subjects.

In this paper, a generic and secure anonymous communication protocol was proposed both for user privacy of computer-oriented communication and for wireless phone communication, the protocol is conditional traceable under the control of independent authoritative institute(IAI). Comparing with current approaches, the advantage of our protocol is it is full privacy protection during the anonymous communication, even the administrator can not recover user's privacy information, while when necessary to recover the user's identity its must work under the legislation authority, while the system are efficient and effective for normal communication.

2 Related work

Concern over user privacy is constantly mounting as the role of the communication network.In 1983, Chaum D. proposed untraceable electronic mail[1], then in 1988, he proposed unconditional sender and recipient untraceability approach for privacy protection[2]. Kesdogan D, proposed Location management strategies in mobile communication systems for privacy protection[3]. Reed M proosed onion routing as anonymous access method[4]. In fact, blind signature, fair blind signature, group signature, group blind signature, zero-knowledge proof, undiable protocol, fairly good exchange protocol, secret sharing, verifiable secret sharing are the most popular technologies that can be employed to enhance privacy and anonymity[5-8]. Current methods for privacy protection are mainly concerned on special applications, the approaches are limited in practice.

The entire behavior of a user may be considered private. In mobile environments we can identify four types of sensitive user information: (1)identity;(2)message contents; (3)location (especially in million communication); (4)actions (content of navigation). The level of protection of this information may also vary depending on the trust the user has in various parts of the system, which can be classified as: (1)level-0: no privacy; (1) level-1: hiding information from external attackers;(3) level-2: hiding identity from foreign networks; (4)level-3: hiding the relationship between the user and the home network; (5)level-4: hiding identities of home and foreign networks;(6) level-5: hiding user behaviour from home authority. Personal identification includes: (1) Legal name; (2) Locatability;(3)Traceable pseudonymity or pseudo-anonymity;(4) Untraceable pseudonymity;(5) Pattern knowledge; (6)Social categorization;(7) Symbols of eligibility/non-eligibility. There are 4 types anonymous communications on the Internet: (1) Traceable anonymous communication;(2)Untraceable anonymous communication; (3) Traceable pseudonymous communication;(4) Untraceable pseudonymity.

3 Secure Anonymity with Conditional Traceability

The infrastructure of current communication network is de factor traceable network, which can be easily trace with the aid of special tools, such as IP-tracer tool, Hardware-based location discovery in GPRS system. Thus in this paper we contribute to conditional traceable anonymity in general communication system.

(I) System Preliminary

Param	Expression
IAI	Independent Authoritative Institute
U	End User
CSC	Commercial Service Center
E_k	Encryption with Symetric Key *k*
D_k	Decryption with Symetric Key *k*
E_{Apk}	Encryption with Public Key *pk* owned by A

D_{Ask}	Decryption with Secret Key *sk* ownered by A
Sig	Signature of Message given
Ver	Verification of Sig given
H	Secure Hash function

(II) Privacy-Enable Initialization

Step1: Independent Authoritative Institute IAI authorizes to Commercial Service Center CSC the privacy-related but anonymous ID AID:

$$AID=E_{CSCPK}(RID)$$

where $RID=\begin{cases} IP_{addr} \| MAC_{addr} \| HID_{mchn} & , \ if\ Cmpt\ net; \\ UID \| Ph_{No} \| ISMI & , \ if\ \ Mobl\ net. \end{cases}$

Together, IAI creates secret key $K_{sk_{IAI}}$ for transactional communication session content signature, where Hash function H (.) may be employed fro anonymity.

Step2: IAI releases AID to CSC in communication in secure channel:

IAI->CSC: AID'= $E_{k_{IAI,CSC}}(AID)$

(III) Privacy-Enable Communication

Step3: CSC secretly gets AID' from IAI, then decrypt the AID' to recover the AID:

CSC -> IAI: AID'= $D_{k_{IAI,CSC}}(AID')$

Step4: Each end user Ui, Uj communication in a common secret way:

U_i>U_j: C= $E_{k_{i,j}}(M)$, and U_j->U_i: M= $D_{k_{i,j}}(C)$

Step5: Under control of CSC, creates transactional session signature between U_i and U_j under the signature key:

$$S_{Content} =< AID_i \| AID_j \| T_{start} \| T_{end} \| S_{Type} > , < S_{Content}, Sig_{SK_{IAI}}(S_{Content}) >$$

where $S_{content}$ stands for session content, Sig. is the signature of the session content $S_{content}$.

(IV) Conditional Trace for Illegitimate Communication Intervention

Step6: When necessary to intervene to validate the historical transaction session content, IAI acts as arbiter to resolve the dispute CSC sends the signature of session between U_i and U_j to IAI:

CSC -> IAI: $E_{k'_{IAI,CSC}}(S_{Content}, Sig_{SK_{IAI}}(S_{Content}))$

Step7: IAI decrypts the message from CSC:

IAI ->CSC : $D_{k'_{IAI,CSC}}(E_{k'_{IAI,CSC}}(S_{Content}, Sig_{SK_{IAI}}(S_{Content})))$

Step8: IAI verifies the historical session transaction that recorded in $S_{content}$:

bverRslt= $Ver_{PK_{IAI}}(Sig_{SK_{IAI}}(S_{Content}))$

If bVerRslt=TRUE, it manifests the session trace is unassailable, then IAI open the session content and decide what ever happened during the session. Otherwise IAI disregards the request from CSC.

In fact, in step8, IAI has some optional ways to solve the dispute by pre-record mechanism to record the session message of what happened. By the way, conditional traceability can use escrowed encryption system (ESS) and threshold cryptography system to enhance privacy protection.

4 Conclusion

With fast development of Internet and mobile and wireless computing technologies such as GSM, CDMA, privacy-enhancement became an important issue in personal communication system (PCs). The approach proposed in this paper is a raw and roase discuss for controllable anonymous communication with privacy-enable application, efficient and effective approaches are to be studied in future, the art of how to ensure fairly good privacy-enable communication but can trace latent attacks legislatively is a trade off between privacy and security issues.

References

1. David Chaum: Untraceable Electronic Mail, Retum Addresses, and Digital Pseudonyms. Communications of the ACM, (1981)84-88
2. David Chaum: The Dining Cryptographers Problem: Unconditional sender and recipient untraceability. Journal of Cryptology, (1988) 65–75
3. Kesdogan D, Federrath H, Jerichow A, Ffitzmann A.: Location management strategies increasing privacy in mobile communication systems. IFIP 12th International Information Security Conference. (1996):39-48
4. Reed M G, Syverson P F , Goldschlag D M: Anonymous connections and onion routing. IEEE Journal on Selected Areas in Communication Special Issue on Copyright and Privacy Protection, (1998)482-494
5. Sholmi Dolev and Rafail Ostrovsky. Xor-Trees for Efficient Anonymous Multicast Receiption. Advances in Cryptography – CRYPTO'97, 1997
6. Michael K. Reiter and Aviel D. Rubin. Crowds :Anonymity for Web Transactions. ACM Transactions on Information and System Security, (1998)66–92
7. Clay Shields and Brian Neil Levine. A protocol for anonymous communication over the Internet. In Proceedings of the 7th ACM Conference on Computer and Communications Security, (2000) 33–42
8. Wang C J, Leung H F:Anonymity and security in continuous double auctions for Internet retails market[A]. Proceedings of the 37th Annual International Conference on Hawaii System Sciences (CD/ROM)(2004) 5-8