Manuscript ID : 00000-60439

Source ID : 00000005

International Journal of Computer Engineering and Technology

Volume 3, Issue 3, October - December 2012, Pages 66-74, Page Count - 9

AN APPROACH TO REVOKE BLACKLISTED ANONYMOUS CREDENTIAL USERS THROUGH TTP

H. Jayasree [(1)] A. Damodaram [(2)]

[(1)] Associate Professor Department of IT, Aurora's Technological and Research Institute, Hyderabad, Telangana, India.
[(2)] Professor of CSE Department and Director – Academic Audit Cell, Jawaharlal Nehru Technological University, Hyderabad, Telangana, India.

Abstract

Many of us use the Internet on a daily basis for purposes ranging from accessing information to electronic commerce and e-banking to interactions with government bodies. This requires that transactions are securely authenticated, and that we protect privacy by not revealing more about ourselves than necessary. Anonymous credentials promise to address both of these seemingly opposing requirements at the same time. Anonymous authentication can give users the ability to misbehave since there is no fear of retribution. To tackle such misbehaving users several schemes have been proposed that strike different tradeoffs between privacy and accountability. In this paper, we significantly make an attempt to generalize the basic form of revocation amounting to "revoke anybody on the blacklist" immediately through our proposed scheme. Depending on the type of misbehaving action we also consider revocation based on the threshold value of number of negative credits of a user.

Author Keywords

Pseudonym, Anonymous Credentials, Certification Authority, Blacklist, Revocation

Index Keywords

Anonymous credential system, Demonstrate possession, Implement trimming technique

ISSN Print:
Source Type: Journals
Publication Language: English
Abbreviated Journal Title:
Publisher Name:
Major Subject: Physical Sciences
Subject area: Computer Science Applications

ISSN Online:
Document Type: Journal Article
DOI:
Access Type: Open Access
Resource Licence: CC BY-NC
Subject Area classification: Computer Science
Source: SCOPEDATABASE

Reference

References (12)

1. Jan Camenisch and Anna Lysyanskaya
   An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation

(2001) proceedings of the International conference on the Theory and Application of Cryptographic Technique, Page No 93-118,
Article Link: https://link.springer.com/chapter/10.1007/3-540-44987-6_7

2. I.Teranishi, J.Furukawa and K.Sako
   K-times Anonymous Authentication (extended abstract)

   (2004) ASIACRYPT, Volume 3329, Page No 308-322,
   Article Link: https://link.springer.com/chapter/10.1007/978-3-540-30539-2_22

3. I.Teranishi and K.Sako
   K-times Anonymous Authentication with a Constant Proving Cost

   (2006) Public Key Cryptography, Volume 3958, Page No 525-542,
   Article Link: https://link.springer.com/chapter/10.1007/11745853_34

4. P. P. Tsang, M. H. Au, A. Kapadia, and S. W. Smith
   Blacklistable anonymous credentials: blocking misbehaving users without TTPs

   (2007) proceedings of the 14th ACM Conference on Computer and Communications Security, Page No 72-81,
   DOI: https://dl.acm.org/doi/10.1145/1315245.1315256

5. M. H. Au, A. Kapadia, and Willy Susilo
   BLACR- TTP free Blaclistable Anonymous Credentials with Reputation

   (2011) proceedings of the 19th Annual Network and Distributed System Security Symposium,

6. Andreas Pashalidis and Chris J. Mitchell Royal Holloway
   Limits to Anonymity when Using Credentials

   (2004) International Workshop on Security Protocols, Volume 3957, Page No 13-19,
   Article Link: https://link.springer.com/chapter/10.1007/11861386_3

7. D. Critchlow, N. Zhang
   Revocation Invocation for Accountable Anonymous PKI Certificate Trees

   (2004) Proceedings ISCC Ninth International Symposium on Computers And Communications, Page No 386-391,
   Article Link: https://ieeexplore.ieee.org/document/1358435

8. David Chaum
   Untraceable electronic mail, return addresses, and digital pseudonyms

   (1981) Communications of the ACM, Volume 24, Issue 2, Page No 84-88,
   DOI: https://dl.acm.org/doi/10.1145/358549.358563

9. David Chaum
   Blind signatures for untraceable payments

   (1983) Advances in Cryptology - Proceedings of CRYPTO, Page No 199-203,
   Article Link: https://link.springer.com/chapter/10.1007/978-1-4757-0602-4_18

10. David Chaum
    Security without identification: Transaction systems to make big brother obsolete

    (1985) Communications of the ACM, Volume 28, Issue 10, Page No 1030-1044,
    DOI: https://dl.acm.org/doi/10.1145/4372.4373

11. David Chaum and Jan-Hendrik Evertse
    A secure and privacy-protecting protocol for transmitting personal information between organizations

(1986) Advances in Cryptology - CRYPTO of Lecture Notes in Computer Science, Volume 263, Page No 118-167,
Article Link: https://link.springer.com/chapter/10.1007/3-540-47721-7_10

12. Stefan Brands
Rethinking Public Key Infrastructure and Digital Certificates —Building in Privacy

(1999) Eindhoven University of Technology, Netherlands,