Anonymous-Accountable Forums

Motivation


ANONYMITY
Protecting social activists since 73BC.


anonymity = bad behavior

Security Goals

- Identity (*I*) not compromised
  - Unless threshold number of regular users and moderators vote to unmask a user

- Authenticated messages
  - Unless the user sending the message has been unmasked

Primitives

- Public Key Encryption
- Digital Signatures
- Secret Sharing
  - Trivial
  - Threshold - (n,k) secret sharing
  - Verifiable secret sharing

Secret Sharing

Shamir defines (k,n) threshold secret sharing as dividing some data D into n pieces $D_1,...,D_n$ such that

- D is easily computable given k or more D_i pieces
- D is completely undetermined given fewer than k of the D_i pieces

Protocol

- Operations: setup, add user, post, vote to unmask
- Each user has (pk_s, sk_s), (pk_e, sk_e), and I
- Group decides on t_m, t_u, and who will be a moderator or a user ($m > t_m$, $u > t_u$) beforehand

Protocol - Setup

Each user does the following:

1. publish pk_e, pk_s
2. Encrypt I with pk_s and publish
3. XOR pk_s with random string k_m; Call the result k_u
4. Distribute k_m and k_u among users with verifiable secret sharing (encrypt with recipient's pk_e):
   - (t_m, m) secret sharing for moderators
   - (t_u, u) secret sharing for regular users

Protocol - Add User

Follow the same procedure as setup, but with only one additional user

Each existing user gives the new user an additional share of their k_m or k_u

Protocol - Post

Poster publishes message signed with sk_s

Protocol - Vote

In order to vote to unmask a user, publish your share of k_m or k_u from that user's sk_s

If more than t_m moderators and t_u users vote to unmask a user, anyone can reconstruct the user's sk_s and decrypt *I*

Proof Sketch

- Goal: *I* not compromised unless there are enough votes from both users and moderators
  - Need sk_s (public-key crypto)
  - need both k_m and k_u (XOR)
  - need enough votes (Secret Sharing)

Proof Sketch

- Goal: posts are authenticated
  - messages can only be forged by negligible probability by one who doesn't have sk_s (Digital Signature)
  - sk_s is not made known unless there are enough votes from both regular users and moderators (from previous slide)

Drawbacks

- Morality assumption
- Threshold proportion shrinks as user population grows
- Need sizeable group to start forum
- What is identity?

Hope is that user/moderator structure helps mitigate the first two drawbacks

Sources

- A. Shamir, How to Share A Secret, CACM Vol. 22 No. 11, 1979

- Chor, Benny; Goldwasser, S.; Micali, S.; Awerbuch, Baruch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," Foundations of Computer Science, 1985., 26th Annual Symposium on , vol., no., pp.383,395, 21-23 Oct. 1985

- Jonathan Katz , Yehuda Lindell, Introduction to Modern Cryptography, Chapman \& Hall/CRC, 2007

- http://cdn.cpnwz.us/wp-content/uploads/2013/07/That-Was-Easy-Button.png
- http://www.trulioo.com/wp-content/uploads/anonymity-3.jpg
- http://venusinlivingcolor.files.wordpress.com/2012/11/6334951402227369 26_anonymity_xlarge.jpeg