Denúncia Anônima Segura

Fernando Cézar de Oliveira Lopes[1], **Ricardo Felipe Custódio (orientador)**[2]

[1]Instituto Superior Tupy – IST, Sociedade Educacional de Santa Catarina – SOCIESC
Rua Albano Schmidt, 3333 – 89201-972 Joinville, SC

[2]Departamento de Informática e Estatística – Universidade Federal de Santa Catarina
Campus Universitário, INE-CTC-UFSC
Caixa Postal 476 – 88.040-900 Florianópolis, SC

lopes@sociesc.com.br, custodio@inf.ufsc.br

Abstract. *This work proposes several cryptographic protocols for the sending of anonymous messages with the possibility of the revelation of the identity of the sender in a certain period of time in the future. All of the protocols are analyzed in relation to a list of safety requirements that they should attend to. Finally, a system was developed for safe anonymous accusation on the Web.*

Resumo. *Este trabalho propõe vários protocolos criptográficos para o envio de mensagens anônimas com a possibilidade da revelação da identidade do emissor num determinado período de tempo no futuro. Todos os protocolos são analisados em relação a uma lista de requisitos de segurança que os mesmos devem atender. Finalmente foi desenvolvido um sistema para a denúncia anônima segura na Web.*

1. Introdução

O crescimento acentuado das tecnologias da Informação e a grande utilização de redes de computadores, dificulta o sigilo das informações privadas das pessoas. As empresas armazenam informações sobre os hábitos de navegação, consumo e preferências dos usuários da Internet. Estas informações podem ser utilizadas tanto para beneficiar como para prejudicar os usuários.

Em muitos casos de troca de informações, a questão do anonimato deve ser considerada. Suponha-se uma eleição através da Internet: no momento da entrega do voto, a autoridade de votação deve reconhecer que recebeu um voto, porém não deve ter meios para associar este voto ao votante. Da mesma forma, uma aplicação sobre denúncia anônima também deve garantir o anonimato do denunciante, sem que isto infrinja os preceitos contidos na lei.

O tema do trabalho enfoca uma aplicação de denúncia, pois os sistemas que se propõem a este fim não garantem o anonimato ao denunciante, apenas a sua privacidade.

Com o intuito de resolver esta situação propõem-se um protocolo criptográfico que produza uma mensagem com a ocultação da identidade do emissor, passível de revelá-la futuramente, se necessário; caso contrário, destruí-la-á.

Para um melhor entendimento do processo no decorrer do tempo, a Figura 1 mostra a linha do tempo com marcações para análise dos acontecimentos. Observa-se nesta figura que existe um intervalo bem definido de ocultamento da identidade, um período ou janela para possível revelação da identidade e o período final onde a mensagem deve permanecer anônima.

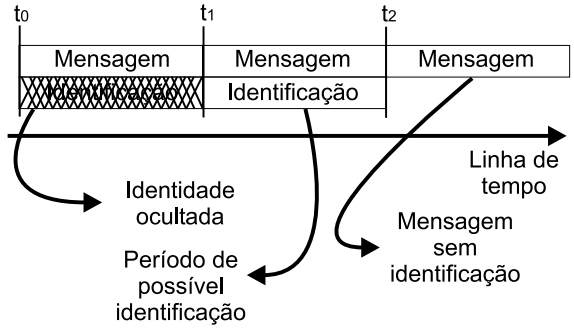

Figura 1: Linha de tempo

O restante do artigo está organizado como segue: a seção 2 apresenta os requisitos de segurança necessários; a 3 lista as técnicas usadas; a 4 apresenta a notação usada; a 5 descreve o funcionamento do protocolo; na 6 comenta-se sobre a implementação e na 7 as considerações finais.

2. Requisitos de Segurança do Protocolo

Os requisitos de segurança têm grande importância na definição de um protocolo, pois dão uma visão do que ele pode fazer. O protocolo deve atender a alguns requisitos básicos para a garantia do funcionamento correto e com segurança conforme segue:

1. **Anonimato no envio**: Deve ser possível ao emissor enviar uma mensagem de forma anônima;
2. **Confiança distribuída**: A identidade do emissor da mensagem pode ser conhecida por qualquer dos subgrupos formados de um grupo de entidades previamente autorizadas;
3. **Anonimato temporal**: A mensagem deve permanecer anônima desde o seu envio pelo emissor até um determinado tempo t_1 no futuro;
4. **Cifra temporal**: A identidade do emissor da mensagem poderá ser conhecida no período de tempo entre t_1 e $t_2 > t_1$;
5. **Destruição da identidade**: A mensagem deverá permanecer anônima para qualquer $t > t_2$;
6. **Aviso ao emissor**: O emissor deve ser avisado que a sua identidade foi revelada;
7. **Autenticação**: A toda mensagem anônima deve ser possível identificar seu emissor no período de tempo adequado, sendo que a identidade do emissor deve estar incluída corretamente;
8. **Prova (não-coação)**: O emissor de uma mensagem anônima não pode provar que foi ele que a emitiu;
9. **Autonomia**: O emissor da mensagem não deve precisar confiar em qualquer entidade, a menos que ele queira;

3. Técnicas Usadas no Protocolo

Para a realização do objetivo, foram utilizadas as técnicas de Redes de Misturadores de David Chaum [Chaum, 1981] para a geração de anonimato, Compartilhamento de Segredo de Adi Shamir [Shamir, 1979] para a divisão do segredo entre um grupo de entidades participantes, Criptografia Temporal introduzida por Timothy C. May [May, 1993] e desenvolvida por Rivest, Shamir e Wagner [Rivest et al., 1996] para a garantia dos intervalos tempo estabelecidos e *Bloco Inverso de Shamir* apresentado na Dissertação de Mestrado de Fernando Cézar de Oliveira Lopes [Lopes, 2003], com a função de reunir todas as partes do segredo para a reconstrução do segredo original e garantir que para qualquer tempo $t > t_2$ seja impossível a reconstrução do segredo por falta de partes suficientes.

4. Notação Usada

Para facilitar o entendimento do protocolo criptográfico proposto, serão usadas as seguintes notações:

Alice Entidade ou usuário emissor da mensagem;
Beto Entidade ou usuário receptor da mensagem anônima;
Carol Entidade ou usuário receptor da mensagem anônima;
Davi Entidade ou usuário receptor da mensagem anônima;
Elisa Entidade ou usuário receptor da mensagem anônima;
Teodoro Entidade ou usuário terceiro confiável do sistema;
Mario Entidade ou usuário malicioso do sistema;
Fernando Bloco responsável pela divisão de segredo através do esquema limiar de Shamir;
Pedro Bloco responsável por aplicar o quebra-cabeça temporal e duplicar os segredos;
Roberto Bloco da rede de misturadores, responsável por criar o anonimato de envio;
Fernando^{-1} *Bloco Inverso de Shamir*, responsável por resolver os quebra-cabeças e destruir partes quando necessário;
AD Autoridade de Datação ou Protocoladora Digital de Documentos Eletrônicos (PDDE);
AC Autoridade Certificadora, é o ponto de mútua confiança.

5. Protocolo Completo com Requisitos de Segurança

O desenvolvimento do protocolo passou por várias etapas que deram origem a cinco protocolos intermediários, passíveis de serem usados em aplicações: votação, leilões por exemplo. Contudo o protocolo cujo funcionamento será descrito a seguir atende aos requisitos de segurança impostos (Figura 2).

1. Alice envia uma mensagem x, a sua identidade Id_a e o endereço do grupo dos destinatários A_g para Fernando;
2. Fernando sabe quem são os destinatários do grupo de participantes autorizados no esquema limiar (m, n), prepara a divisão da identidade de Alice como o segredo $S = Id_a$ e envia todas as partes com o endereço A_{f1} (endereço de $Fernando^{-1}$) para Pedro;

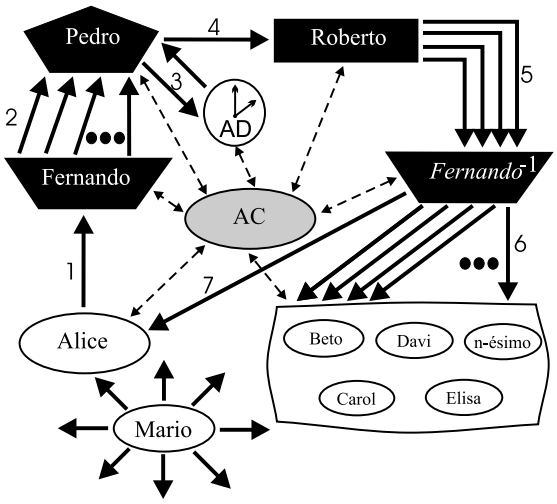

Figura 2: O Protocolo com Todas as Técnicas

3. Pedro duplica o conjunto s_i para s_i' idêntico e solicita a data e hora para AD, para os dois conjuntos;
4. Pedro aplica no conjunto s_i o quebra-cabeça temporal com parâmetros de configuração iguais, e no conjunto s_i' aplica o quebra-cabeça com parâmetros de revelação diferentes. Pedro agora concatena estes quebra-cabeças temporais, mais o endereço A_{f1} com a mensagem x e envia através de Roberto;
5. Roberto envia estas informações para o endereço físico A_{f1}, através da rede de misturadores, e este distribui a mensagem x ao grupo;
6. $Fernando^{-1}$ envia uma cópia das partes para cada participante do grupo autorizado e começa a resolver todos os quebra-cabeças, sendo que em t_1, os quebra-cabeças s_i estão resolvidos, e que os quebra-cabeças s_i' vão se resolvendo entre t_1 e t_2. À medida que os s_i' são resolvidos, faz-se uma comparação de igualdade com os s_i já resolvidos, se forem iguais, $Fernando^{-1}$ os destrói. Caso seja solicitada a identidade do autor dentro do período permitido, então $Fernando^{-1}$ reúne as partes necessárias e revela aos participantes a identidade;
7. $Fernando^{-1}$ envia uma notificação ao autor (Alice) de que a sua identidade foi revelada.

6. Implementação do Sistema

Com intuito de demonstrar o funcionamento do protocolo SDAS (Sistema de Denúncia Anônima Segura), foi implementado um protótipo para viabilidade prática utilizando alguns dos recursos apresentados na seção 3. Escolheu-se apenas a técnica característica de anonimato a título de exemplificação.

O Sistema de Denúncia Anônima Segura, é um sistema que trata as denúncias que são feitas através da Internet, utilizando certificados digitais e criptografia assimétrica com ElGamal [ElGamal, 1985]. O Sistema foi dividido em duas partes:

1. Acesso para usuários que irão cadastrar as denúncias;
2. Acesso para os administradores do sistema.

7. Considerações Finais

O principal objetivo deste trabalho foi propor uma solução para a emissão de um documento eletrônico, de tal forma que somente em um período de tempo pré-determinado no futuro a identidade do emissor pudesse ser revelada. O protocolo proposto é inédito, pois não foi encontrado protocolo similar na literatura. Mesmo em casos de leilões eletrônicos os protocolos propostos nestas aplicações não atendem aos requisitos especificados na seção 2. Uma possível aplicação para esta solução é a implementação de um sistema de denúncia anônima usando a Internet. De fato, o problema acima surgiu durante a discussão de como implementar este sistema. Dentre os resultados obtidos, pode-se destacar:

- Definição de um problema inédito relacionado à comunicação anônima;
- Desenvolvimento de um sistema para Internet de Denúncia Anônima Segura - DAS;
- Proposição de seis protocolos criptográficos e análise de segurança em relação aos requisitos pré-definidos;
- A proposta de um *Bloco Inverso de Shamir*, responsável pela resolução do quebra-cabeça temporal, comparações entre partes de segredo, e a destruição das partes do quebra-cabeça iguais.

Referências

Chaum, D. (1981). Untraceable electronic mail, return address and digital pseudonyms. *Communications of the ACM*, 24:84–88.

Lopes, F. C. de O. (2003). Denúncia anônima segura. Dissertação de mestrado, UFSC - Universidade Federal de Santa Catarina, Florianópolis - SC.

ElGamal, T. (1985). A public key cryptosystem and signature schema based on discrete logarithms. *IEEE Transactions on Information Theory*, 31:473–481.

May, T. C. (1993). Timed-release crypto. Disponível em: http://cypherpunks.venona.com/date/1993/02/index.html.

Rivest, R. L., Shamir, A., and Wagner, D. A. (1996). Time-lock puzzles and timed-release crypto. Disponível em: http://theory.lcs.mit.edu/r̃ivest/RivestShamirWagner-timelock.ps.

Shamir, A. (1979). How to share a secret. *Communication of the ACM*, 22(11):612–613.