Votação Anônima Segura Utilizando Lista de Discussão

Júlio S. Dias[1]*, Fabiano C. Pereira[2], Ricardo F. Custódio[2] , Carlos R. De Rolt[1]

[1]Universidade do Estado de Santa Catarina
Av. Madre Benvenuta, 2037 – 88035-001 Florianópolis, SC

[2]Laboratório de Segurança em Computação – Universidade Federal de Santa Catarina
Caixa Postal 476 – 88040-900 Florianópolis, SC

{jdias,castro,custodio}@inf.ufsc.br, rolt@bry.com.br

Abstract. *Democracy is an important subject, and its importance is concentrated in the possibility of discussing about a specific subject, going beyond the simple choice among the available options. This article proposes a way of conducting discussions and also polling among the members of a mailing list, which is available through the use of electronic mail, a known and quite used infra-structure. We propose to use mix-networks and secret sharing technics in order to achieve the required security requirements to the polling system using a mailing list.*

Resumo. *A democracia é um tema bastante discutido, sendo que a sua importância concentra-se na possibilidade de se debater um assunto em específico, indo além da simples escolha dentre as opções disponíveis. Neste artigo propõe-se um meio de se realizar debates e também votações entre os participantes de uma lista de discussão, que é um serviço disponibilizado utilizando a infra-estrutura de correio eletrônico existente. Esta infra-estrutura é bastante utilizada e tem sido submetida a testes ao longo dos anos, provando sua confiabilidade. Propõe-se contudo, adicionar a possibilidade de anonimato e um mecanismo de coleta e processamento de dados, através do uso de técnicas criptográficas, para que as votações sejam feitas de forma segura.*

1. Introdução

Apesar de serem muitas vezes utilizadas como meios eficazes de se realizar avisos e outros comunicados aos seus integrantes, as listas de discussão foram originalmente concebidas para facilitar uma colaboração entre seus assinantes, facilitando a intercomunicação de todos, com o objetivo principal de se discutir e argumentar temas variados, dentro das preferências de cada assinante.

A funcionalidade de uma lista de discussão pode ser estendida de diversas formas, uma delas seria o seu uso na realização de votações ou eleições entre os participantes da lista. O uso de um mecanismo automatizado para o processamento e armazenamento das

*Apoiado pela Universidade do Estado de Santa Catarina e pela CAPES.

informações relativas a uma votação em uma lista de discussão pode facilitar bastante a realização das mesmas, pois os integrantes não teriam necessidade de coletar e apurar manualmente os votos emitidos.

Uma lista de discussão com esta funcionalidade torna-se uma ferramenta bastante útil para a realização de votações mais democráticas, pois em uma democracia ideal a necessidade de se discutir os assuntos e opções disponíveis acaba sendo maior do que o próprio ato de votar. A discussão e apresentação dos argumentos dos diversos participantes da lista contribui para o amadurecimento das opiniões individuais de cada integrante a respeito do tema que está sendo posto sob votação.

A discussão provida pelas listas possui a limitação de não permitir mensagens anônimas de seus integrantes, pois as mesmas são identificadas pelo endereço de correio eletrônico do emissor. Esta limitação muitas vezes impede uma discussão mais ampla, pois um participante pode sentir receio em fazer determinado questionamento, ou emitir determinada opinião, por não poder fazê-lo de forma anônima.

Apesar de o anonimato ser desejável, para se permitir uma discussão mais abrangente, também é preciso ter meios de se restringir as mensagens enviadas com o objetivo de se impedir o envio de mensagens ofensivas, que estejam fora dos objetivos definidos para a lista de discussão. Este artigo propõe o uso de mecanismos criptográficos para a obtenção de anonimato parcial no envio de mensagens para uma lista de discussão. Desta forma permite-se o envio de mensagens anônimas enquanto estas não violarem as regras determinadas pelo administrador da lista. As votações são realizadas utilizando a infraestrutura de uma lista de discussão a qual os usuários podem utilizar de forma anônima para o envio dos votos.

Uma descrição do sistema que é utilizado como base neste trabalho é apresentada na seção 2. As seções 3 e 4 apresentam detalhes da proposta de adaptação do sistema eVote. A seção 3 apresenta os conceitos envolvidos na utilização de uma rede de mistura, utilizada para comunicações anônimas. Para a obtenção de anonimato parcial, faz-se uso da técnica de compartilhamento de segredos, apresentada na seção 4. Uma comparação dos resultados obtidos a partir da arquitetura proposta com outras arquiteturas existentes é apresentada na seção 5. A seção 6 conclui o artigo.

2. Votação eletrônica com o sistema eVote

Através do estudo de vários sistemas de votação eletrônica [Araújo, 2002] foram listados os seguintes requisitos de segurança: exatidão, unicidade, privacidade, verificabilidade, escalabilidade e flexibilidade. Em sistemas que atendem ao requisito exatidão as células não podem ser alteradas, toda cédula deve ser contabilizada, não sendo consideradas cédulas inválidas ou duplicadas. O requisito unicidade determina que somente votantes autorizados podem participar da votação emitindo um único voto. O requisito privacidade busca garantir ao votante o anonimato, não sendo possível coagir o votante nem determinar o conteúdo dos votos antes do final da votação. O requisito verificabilidade determina que o processo pode ser auditado determinando quais os usuários votaram e se os votos destes votantes foram corretamente contabilizados. A escalabilidade

está relacionada a capacidade de suportar grandes quantidades de votantes sem que a infra-estrutura utilizada na votação sofra alterações substanciais. A flexibilidade está relacionada com a possibilidade de realização de várias formas de votação sem que sejam necessárias grandes alterações no sistema utilizado.

As propostas feitas neste artigo têm o objetivo de garantir os requisitos citados, e tomam como base o sistema **eVote** [Davis, 2003], apresentado nesta seção. O sistema eVote (www.deliberate.com), na forma proposta originalmente, atende aos requisitos de escalabilidade, flexibilidade e unicidade. Não há mecanismos que permitam o atendimento dos requisitos de privacidade, exatidão e verificabilidade.

Este sistema age como um servidor especializado de dados que mantém informações de votações criadas e administradas pelos usuários. Ele interage com um servidor de listas de discussão para usar a lista como meio de comunicação entre os participantes de uma votação, os usuários do sistema.

Além da criação de votações, também é possível a criação de petições, que são votações onde qualquer pessoa pode participar, mesmo aquelas que não fazem parte da lista de integrantes. Quando alguém envia uma mensagem para uma lista-petição, o remetente da mensagem recebe um recibo de participação naquela petição.

2.1. O servidor de votação

O servidor de votação é denominado **Secretário**, e é responsável por prover as funcionalidades da votação aos votantes. Através do **Secretário** um usuário pode criar uma votação e os demais usuários podem produzir seus votos. Os tipos de votação que podem ser criadas são os seguintes:

- **Pública**: este tipo de votação permite que cada votante tenha acesso ao voto dos demais participantes;
- **Privada**: nas votações privadas os votos são mantidos em segredo;
- **Se_votou (*if_voted*)**: neste tipo de votação os votantes podem saber quem realizou um voto, mas não podem saber qual foi a escolha feita.

Os tipos de voto podem ser de simples escolha (sim/não), com valores numéricos, ou para se escolher itens de um grupo. Também é possível especificar se o resultado parcial estará disponível no decorrer da votação, ou se apenas ao final da votação ele será divulgado.

2.2. A interface com os votantes

Como o sistema interage com o servidor de listas de discussão, toda a comunicação entre o sistema e os votantes é feita através do envio de mensagens de correio eletrônico.

As atividades realizadas pelos usuários do sistema dependem da função que aquele usuário exerce:

- **Votante**: um usuário votante pode utilizar o sistema para votar e também pode alterar seu voto no decorrer da votação. Além disso ele pode solicitar a visualização dos votos já realizados, de acordo com o tipo da votação em questão;

- **Usuário/Administrador**: qualquer usuário do sistema pode iniciar uma votação, tornando-se assim o administrador daquela nova votação. Desta forma ele também poderá encerrar a votação ou retirá-la do sistema;
- **Proprietário da lista (*list owner*)**: este é o usuário proprietário da lista definido no servidor de listas, e além das suas atribuições normais ele tem poder para encerrar ou excluir qualquer votação, e para alterar os privilégios de voto dos usuários. Alguns dos comandos do proprietário são protegidos por senha;

2.3. Componentes do sistema

O sistema é composto por cinco aplicações. A principal, denominada **eVote_clerk**, é a responsável pelas atividades do **Secretário**. Ela opera sobre votações, ativando as novas e retirando as encerradas; e sobre os votos, aceitando, contabilizando, armazenando e exibindo os mesmos. Esta aplicação não possui uma interface com o usuário, ela opera como processo *daemon*, e é iniciada através de outro componente, a aplicação denominada **eVote**.

A aplicação **eVote**, além de inciar, encerrar, e verificar o funcionamento do **Secretário**, também pode ser usada para verificar e sincronizar os dados, e para atualizar ou reiniciar os registros de atividade.

A integração do sistema com o servidor de listas é feita através da aplicação **eVote_insert**. Este componente é responsável por gerar a interface do sistema com os usuários, através das mensagens de correio eletrônico. Para que esta aplicação seja ativada são necessárias alterações nas configurações do servidor de listas, fazendo com que o **eVote_insert** seja invocado em determinadas situações. Ele intercepta as mensagens enviadas para uma lista de discussão e, caso a primeira palavra no corpo da mensagem não seja "eVote", a mesma é encaminhada normalmente para a lista de discussão; do contrário trata-se de uma mensagem de comunicação entre o usuário e o sistema. O componente processa a mensagem em cooperação com o **eVote_clerk**, sendo que o resultado pode ser uma mensagem de informações retornada ao usuário, ou pode ser uma nova mensagem direcionada à lista informando sobre uma nova votação criada ou o encerramento de uma votação em andamento.

O quarto componente do sistema trata-se do **eVote_mail**. Esta aplicação permite ao administrador sincronizar a lista de usuários do sistema com a relação de usuários do servidor de listas. Esta aplicação pode ser utilizada para bloquear determinado endereço de correio eletrônico, impedindo-o de participar de votações; ou ainda para remover um endereço de todas as listas. O administrador também pode utilizar o **eVote_mail** para tratar mensagens que necessitem de confirmação.

O último componente do sistema **eVote** é o **eVote_petition**. Este componente funciona de forma semelhante ao **eVote_mail**, interceptando mensagens que são enviadas para a lista e tratando-as. Caso a primeira palavra do corpo da mensagem seja "*help*"ou "info", o sistema envia para o usuário informações sobre a petição em questão. Este componente também verifica se a primeira palavra é "*remove*", o que fará com que o remetente seja removido da petição. Em qualquer outro caso a mensagem é considerada como um comentário sobre a petição, demonstrando que a pessoa está aderindo ao que

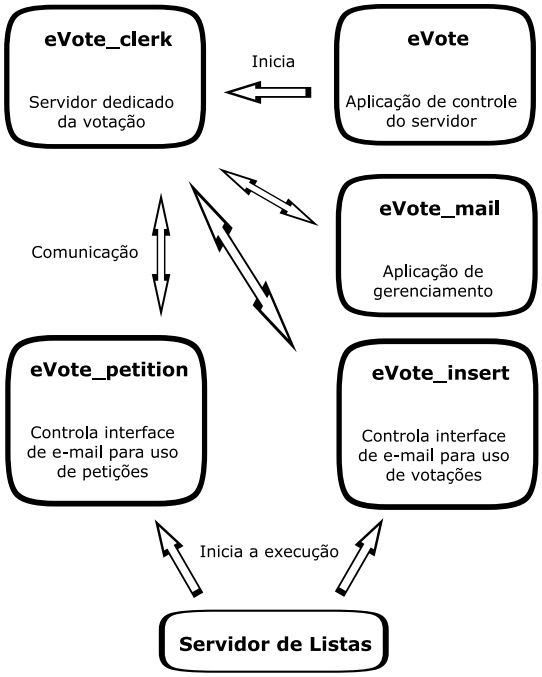

Figura 1: Componentes do sistema eVote

foi definido na petição. Neste caso a aplicação gera um recibo e o envia ao remetente da mensagem.

A figura 1 exibe a interação entre as aplicações do sistema **eVote** e também o servidor de listas.

3. Rede de mistura

Para aprimorar o sistema **eVote**, propõe-se a possibilidade de envio de mensagens anônimas, porém sem se obter anonimato completo, inibindo o envio de mensagens que não contribuam para o processo democrático ou apresentem acusações ou ataques pessoais infundados.

Para se obter anonimato no envio de mensagens de correio eletrônico, inclusive no caso de listas de discussão, utiliza-se um mecanismo conhecido como **rede de mistura**, proposto por Chaum [Chaum, 1981].

A rede de mistura é um mecanismo que visa resolver os problemas da análise de tráfego de informações, os quais resultam nos ataques ao anonimato na comunicação, sem que seja necessária a confiança em uma única autoridade central. Para tanto a rede de mistura faz uso da criptografia assimétrica, e distribui a segurança da rede ao longo de ***n*** servidores (denominados **misturadores**) que compõem os pontos da rede, de forma que, mesmo tendo ***n-1*** servidores comprometidos por um atacante, o anonimato da comunicação ainda é mantido.

A rede de mistura faz duas considerações para garantir a segurança do anonimato:

- (a) Nenhum participante pode determinar qualquer coisa sobre a relação entre o conjunto de mensagens cifradas e o conjunto de mensagens decifradas, nem pode criar falsificações sem o conhecimento da chave envolvida na cifragem;
- (b) Qualquer participante pode saber a origem, destino, e representação de todas as mensagens no sistema de comunicação utilizado, e qualquer participante pode inserir, remover ou modificar mensagens.

A primeira consideração diz respeito à segurança das técnicas de criptografia utilizada, como confia-se que as mesmas são invioláveis, é preciso fazer a mesma consideração para a rede de mistura, pois a mesma faz uso destas técnicas. A segunda consideração diz respeito à forma como os dados trafegam em uma rede de computadores, em especial a Internet, a qual, com o uso de determinadas ferramentas, permite a captura de dados e as demais operações citadas.

3.1. Comunicação anônima na rede

De forma simplificada, considerando uma rede de mistura que tenha apenas um misturador, o envio de mensagens de forma anônima é feito da seguinte forma: o emissor deve cifrar cada mensagem com a chave pública do receptor. Junto a esta mensagem cifrada o emissor coloca o endereço do receptor e cifra estes dados com a chave pública do misturador.

Ao receber uma mensagem, o misturador utiliza sua chave privada para decifrá-la, obtendo assim a mensagem a ser encaminhada e o endereço para onde deve ser encaminhada. Ao receber a mensagem do misturador, o receptor utiliza sua chave privada para decifrar a mensagem, obtendo assim a mensagem original, enviada de forma anônima pelo emissor.

O propósito de um misturador é o de esconder a relação entre as mensagens que entram no servidor e as que saem. A ordem de chegada das mensagens é escondida através do encaminhamento das mesmas em pacotes de dados do mesmo tamanho e em ordem diferente da recebida.

Outra função importante do misturador é garantir que nenhuma mensagem seja processada mais de uma vez. Para tanto o misturador mantém um registro das mensagens processadas durante sua operação, descartando qualquer mensagem que tenha seu registro já presente, o que caracteriza uma repetição da mesma. Outra solução proposta na rede mistura para esta questão é o uso de **marcas de tempo** (*time-stamp*) em cada mensagem, fazendo com que cada uma delas seja processada apenas se estiver dentro do período de tempo indicado na marcação feita ao ser enviada.

O uso de diversos misturadores na rede é a melhor forma para se obter o anonimato, pois esta medida faz com que a segurança da rede esteja distribuída ao longo dos diversos servidores. Entretanto, o uso de diversos servidores faz com que o envio de mensagens necessite de alguns passos a mais: é preciso que a mensagem, juntamente com o endereço do receptor, seja cifrada com a chave pública de cada um dos misturadores da rede, na ordem inversa a que eles serão utilizados. Este procedimento forma uma estrutura similar à colocação de vários envelopes um dentro do outro.

No caso do sistema **eVote**, o integrante de uma lista de discussão que deseje enviar uma mensagem anônima deverá montar um envelope com a mensagem, conforme descrito acima, e enviá-lo para a rede de mistura, a qual se encarregará de fazer com que a mensagem chegue até a lista de discussão de forma anônima.

3.2. Endereço de retorno não-rastreável

A rede de mistura também permite comunicação bi-direcional sem a revelação do endereço do emissor para o receptor. Para tanto o emissor (usuário A) deve enviar junto com suas mensagens um **endereço de retorno não-rastreável**, que consiste do seu endereço real, juntamente com uma chave simétrica por ele escolhida, ambos cifrados com a chave pública do misturador, e também uma chave pública escolhida por ele, única para aquele envio.

Para enviar uma resposta ao usuário A, o receptor (usuário B) deve proceder da seguinte forma: de posse do endereço de retorno enviado pelo usuário A, ele deixe intacta a primeira parte (que contém uma chave simétrica e o endereço real do usuário A cifrados com a chave pública do misturador) e utiliza a segunda parte (a chave pública escolhida pelo usuário A) para cifrar o seguinte par: uma chave simétrica escolhida pelo usuário B, e sua mensagem de resposta cifrada com esta chave. O usuário B então envia para o misturador a primeira parte do endereço de retorno recebido do usuário A juntamente com a cifragem da sua mensagem de resposta.

Ao receber uma mensagem de resposta, o misturador utiliza sua chave privada para decifrar a primeira parte e obter o endereço real (do usuário A) para onde se dirige a resposta, e a chave simétrica que deve ser utilizada para cifrar a mensagem de resposta, de forma a alterar sua codificação ao passar pelo misturador. Assim o misturador envia, para o usuário A, a mensagem de resposta recebida, cifrada com a chave simétrica obtida no passo anterior.

Apenas o usuário A pode obter o conteúdo da mensagem de resposta, pois foi ele quem definiu tanto a chave simétrica utilizada pelo misturador para lhe enviar a resposta cifrada, quanto a chave assimétrica utilizada na cifragem inicial da mensagem de resposta, realizada pelo usuário B.

Da mesma forma que as mensagens enviadas não podem ser repetidas para se evitar ataques, os endereços de retorno enviados por um emissor de mensagens também não podem se repetir. Desta forma, para cada mensagem enviada da qual o emissor deseje receber uma resposta, ele deve gerar chaves diferentes para acompanhar cada endereço de retorno.

No sistema **eVote** esta funcionalidade da rede de mistura seria útil caso alguém deseje responder em particular a um remetente de uma mensagem anônima, ao invés de ter que responder para toda a lista.

3.3. Uso genérico da rede

Originalmente a proposta da rede de mistura foi feita tendo o envio de correio eletrônico como a principal aplicação para se usar o mecanismo. Entretanto, a sua estrutura e procedimentos de manipulação dos dados permitem um uso mais genérico da rede,

a qual pode ser aplicada a diversas aplicações em rede, que necessitem do anonimato na comunicação.

Como as mensagens enviadas em uma aplicação de comunicação de dados têm tamanhos variados, para o envio de mensagens grandes a rede de mistura prevê que uma mensagem seja primeiro cifrada para depois ser dividida em diversas partes. Para que o número de mensagens enviadas não seja revelado, a rede de mistura também prevê o envio de mensagens aleatórias, sem um conteúdo real, com o único objetivo de dificultar a análise de tráfego.

O envio das mensagens através da rede não necessita ser feito através de todos os misturadores, principalmente se a rede estiver implementada com uma grande quantidade deles. Desta forma, cada mensagem deve passar por uma seqüência de misturadores selecionados, a qual pode ser baseada na topologia da rede ou no nível de confiança de cada ponto.

Para o sistema **eVote**, a aplicação da rede de mistura encontra-se de acordo com o objetivo inicial do uso de tal rede, para o anonimato de mensagens de correio eletrônico.

4. Compartilhamento de segredo

A garantia de que o anonimato no envio de mensagens não será total pode ser feito com o uso da técnica do compartilhamento de segredo. Com o uso desta técnica pode-se fazer com que o usuário remetente de uma mensagem anônima seja descoberto, desde que um número determinado de integrantes da lista de discussão concordem com isto e julguem necessário, no caso de aquela mensagem ter sido ofensiva, ou com conteúdo inadequado.

A técnica de compartilhamento de segredos foi inicialmente proposta por Shamir [Shamir, 1979]. O esquema de Shamir para compartilhamento de segredo é baseado em interpolação polinomial. Um polinômio de grau $(m-1)$ apresentado na equação 1 é construído de tal forma que o coeficiente a_0 é o segredo a ser preservado e todos os outros coeficientes são elementos aleatórios. Cada um dos n segredos compartilhados é um ponto (x_i, y_i) na curva definida pelo polinômio. Onde x_i não é igual a 0. Tomando-se m segredos compartilhados o polinômio é unicamente determinado e então o segredo a_0 pode ser recuperado. Entretanto com $(m-1)$ ou menos segredos não é possível reconstruir o segredo a_0.

$$F(x) = a_0 + a_1.x + ... + a_{m-1}.x^{m-1} \quad (1)$$

A escolha de m deve ser realizada de forma a evitar possíveis fraudes no processo. Um valor de m inicial seria a metade mais um dos integrantes do processo. Este valor poderia ser aumentado caso fosse necessário.

Este esquema é relativamente simples, não apresentando a robustez necessária em votações. Nada no esquema impede os integrantes de entregarem falsos segredos compartilhados. A solução para este tipo de falha pode ser obtida utilizando-se métodos mais elaborados como os que garantem a verificabilidade dos segredos compartilhados (VSS). Um exemplo de método que pode ser facilmente utilizado no presente trabalho é

o proposto por Gennaro [Gennaro, 1998].

O segredo a ser preservado seria a identidade do participante do processo democrático. Caso o participante apresentasse um comportamento constrangedor ou que perturbasse a ordem do processo, este poderia ter a identidade revelada. O processo para tornar pública a identidade passaria por reunião dos integrantes que, com o consentimento da maioria, entregariam os seus segredos compartilhados a um juiz, que realizaria a identificação do elemento perturbador. Este seria então responsabilizado pelos seus atos.

5. Implementação e Comparação com outros sistemas

Obtém-se a verificabilidade do sistema através da garantia de que os registros do sistema não sejam fraudados. A forma utilizada para preservar a integridade destes registros consiste no uso de autoridades de datação que fornecem referências temporais a estes registros. Qualquer tentativa de fraudar os registros do sistema pode ser facilmente identificada através da verificação dos pontos de confiança estabelecidos pela datação do arquivo onde os registros são armazenados.

O sistema eVote é implementado sobre um servidor de listas amplamente conhecido que é o **mailman** (www.list.org). A rede de mistura foi implementada utilizando o serviço de correio eletrônico. O votante envia a mensagem para um servidor de correio eletrônico. Este servidor seleciona aleatoriamente o próximo servidor para o qual a mensagem será enviada. O processo é repetido continuamente até um limite determinado pelo emissor da mensagem. Neste ponto a mensagem deixa a rede e é enviada ao servidor de listas. A identidade do usuário é conhecida somente pelo primeiro servidor de correio eletrônico do sistema que oculta os dados do emissor utilizando técnicas de compartilhamento de segredo.

O mecanismo de datação dos registros do sistema é realizado de forma independente do sistema de votação. Uma rotina específica é executada periodicamente. O registro de eventos do sistema é analisado e todos os eventos relacionados ao sistema é armazenado em arquivo específico. Um resumo criptográfico é calculado e enviado à Autoridade de Datação que fornece um ponto de confiança ao processo garantindo que qualquer alteração dos dados será constatada pela verificação da integridade dos registros.

Os sistemas encontrados localizam-se em extremos do processo eleitoral. A maioria do sistemas de votação desenvolvidos busca atender aos requisitos de uma eleição majoritária como a realizada para escolha de presidentes ou prefeitos. O **eVote** é um sistema voltado para uma situação onde os requisitos de segurança não são tão elevados. Pode-se utilizar um sistema como este em tomadas de decisão, eleições privadas como as realizadas em condomínios ou empresas. A agregação da capacidade de discussão dos temas de forma anônima é importante para a criação de um processo democrático avançado.

O uso de servidores de correio eletrônico e listas de discussão proporcionam boa escalabilidade. São serviços largamente utilizados, apresentando robustez necessária à aplicação.

A necessária autenticação dos interessados e a escala limitada do sistema reduz a probabilidade de ataques visando a negação de serviço.

6. Conclusão

A agregação de uma rede de mistura, utilizando servidores de correio eletrônico, técnicas de compartilhamento de segredos e uma autoridade de datação amplia as funcionalidade do sistema **eVote**. O sistema eVote aprimorado é uma ferramenta que permite discussões e votações mais democráticas.

As principais contribuições são o anonimato parcial e a verficabilidade. O anonimato parcial, permite que o usuário possa fazer questionamentos e emitir opiniões mais enfáticas ao mesmo tempo que fornece um mecanismo que impede o uso indevido dos recursos disponibilizados.

A primeira implementação utiliza componentes bastante conhecidos como listas de discussão e servidores de correio eletrônico, não apresentando maiores problemas com relação à implementação. O maior problema encontrado foi na operacionalização do sistema eVote.

As primeiras tentativas mostraram que a integração com a rede de mistura leva a mudanças do sistema original. Uma forma de contornar o problema foi a utilização de redes de mistura utilizando servidores de correio eletrônico (remailers). Desta forma as adaptações forma deslocadas do sistema eVote para um elemento externo que trata as mensagens antes de realizar a entrega ao sistema eVote.

O uso prático de uma versão aprimorada do **eVote**, incluindo as alterações propostas, traz diversos benefícios aos processos democráticos encontrados atualmente. O serviço de correio eletrônico é amplamente utilizado não apresentando maiores dificuldades aos usuários. Desta forma o sistema pode ser utilizado em discussões ou votações de maior porte sem maiores problemas.

Referências Bibliográficas

Araújo, R. S. D. S. (2002). Protocolos criptográficos para votação digital. Master's thesis, Universidade Federal de Santa Catarina.

Chaum, D. (1981). Untraceable eletronic mail, return addresses, and digital pseudonyms. *Comunication of the ACM*, pages 84 – 88.

Davis, M. (2003). evote adds election to mailing lists. *Linux Journal*, 107.

Gennaro, R., R. M. O. R. T. (1998). Simplified vss and fast-track multiparty computations with applications to threshold cryptography. *Proceedings of the 1998 ACM Symposium on Principles of Distributed Computing.*

Shamir, A. (1979). How to share a secret. *Communications of the ACM, Volume 22, pages 612-613*.