Farnel: Um protocolo criptográfico para votação digital

Roberto Samarone S. Araújo[1] sama@inf.ufsc.br
Augusto J. Devegili[2] devegili@ulbra-to.br
Ricardo F. Custódio[1] custodio@inf.ufsc.br

[1]Curso de Pós-Graduação em Ciência da Computação
Universidade Federal de Santa Catarina
88040-900, Florianópolis, SC

[2]Centro Universitário Luterano de Palmas
Universidade Luterana do Brasil
77054-970, Palmas, TO

Resumo: *Apresentamos o Farnel, um protocolo criptográfico para esquemas de votação eletrônica, que utiliza redes de misturadores, assinatura cega e escrutinadores para permitir a execução de votações seguras sobre redes de computadores. O Farnel foi desenvolvido tendo como base o processo eleitoral brasileiro tradicional, utilizado antes da introdução das urnas eletrônicas.*

Palavras Chaves: *segurança, protocolos criptográficos, votação digital*

Abstract: *We present Farnel, a cryptographic protocol for electronic voting schemes which uses mix nets, blind signatures and scrutinizers in order to allow the execution of secure voting over computer networks. Farnel has been developed based on the Brazilian election process before the use of electronic voting machines.*

Keywords: *security, cryptographic protocols, digital voting*

1 INTRODUÇÃO

Com o desenvolvimento de recursos criptográficos cada vez mais tolerantes a criptoanálise e com o surgimento de tecnologias de redes de computadores que proporcionam maior velocidade de comunicação, foi possível integrar, de forma viável, criptografia a aplicações que utilizam redes de computadores para se comunicarem. Por conseguinte, foi possível o desenvolvimento de aplicações que necessitam de segurança para garantir sua correta funcionalidade, como foi o caso de aplicações de *home banking* e comércio eletrônico.

Hoje, devido a esse avanço da criptografia e das redes, já é possível o desenvolvimento de sistemas que exigem avançados recursos criptográficos tais como as aplicações para votação digital. A votação é uma das atividades que o homem mais exercita. Um sistema de votação digital que facilite esta tarefa ajuda a melhorar qualidade de vida das pessoas visto que elas poderão fazer opções de forma rápida. Dependendo do tipo de votação, seja ela uma enquete, eleição ou tomada de decisão, e do grau de segurança que a mesma requer, diferentes requisitos de segurança e de implementação tornam-se necessários para assegurar a correção e robustez do sistema.

A procura por protocolos de votação digital que atendam ao maior número de requisitos de segurança e de implementação começou em 1981 quando David Chaum [CHA 81] propôs o primeiro protocolo criptográfico de votação digital. Desde então pesquisadores em todo o mundo

têm buscado desenvolver protocolos cada vez mais seguros. Segundo Riera [RIE 99a], um esquema de votação digital é uma aplicação distribuída constituída por um conjunto de protocolos e mecanismos criptográficos que juntos permitem que uma votação aconteça inteiramente sobre redes de computadores, de maneira segura, mesmo assumindo que seus legítimos participantes possam ter comportamento malicioso.

Existe uma variedade de protocolos criptográficos propostos na literatura para os mais diversos tipos de votação que visam a definir esquemas de votação digital seguros. Tradicionalmente estes protocolos são agrupados da seguinte forma: baseados em homomorfismos (tais como os de Benaloh [BEN 86]) e os baseados em canais de comunicação anônima (Fujioka [FUJ 92], Riera [RIE 99b] e Borrel [BOR 96]). Os baseados em homomorfimos receberam pouca atenção devido ao alto custo computacional necessário para sua implementação. Ademais, muitos protocolos são extremamente complexos e foram projetados sem levar em conta aspectos reais de implementação: o protocolo de Wen-Sheng [JUA 97] que utiliza uma grande quantidade de cálculos matemáticos que o inviabiliza devido ao tempo de realização desses cálculos e o protocolo sem autoridades apresentado em [SCH 96] que tem a quantidade de cálculos aumentada de acordo com a quantidade de votantes.

O protocolo Farnel [DEV 01] foi desenvolvido para atender a todos os requisitos de segurança de uma votação digital.

Na seção 2 é apresentado uma análise de confiança das entidades de um sistema de votação digital. Na seção 3 são descritos os requisitos de segurança necessários para que um protocolo de votação digital seja considerado seguro. Na seção 4 são apresentadas as fases de um processo de votação digital. Na seção 5 é descrito o protocolo Farnel. Na seção 6 é realizada a análise de segurança do protocolo Farnel. Finalmente na seção 7 tem-se as considerações finais.

2 CONFIANÇA NO SISTEMA DE VOTAÇÃO

Uma votação digital consiste em um conjunto de entidades que resumem-se basicamente em: o votante, o meio de comunicação e o sistema de votação. O perfeito funcionamento do processo de votação é alcançado se essas três entidades forem totalmente confiáveis mas, na prática, a necessidade de confiança em uma ou mais entidades pode comprometer todo o processo. O ideal é que nenhuma das entidades participantes do processo de votação possa alterar ou influir de forma maliciosa no resultado da votação. Para que o meio de comunicação seja considerado confiável, basta que nenhuma entidade externa ao processo de votação consiga obter e/ou alterar as informação que trafegam neste meio. Isso pode ser alcançado utilizando protocolos que ofereçam o serviço de confidencialidade, como por exemplo o SSL. Para evitar que votantes maliciosos possam influenciar o processo com a tentativa de burlar o sistema de votação, mecanismos de autenticação podem ser utilizados em conjunto com certificados digitais padrão X509v3 [IT 00]. Um sistema de votação digital malicioso poderia influenciar de várias formas, tais como a adição de votos inválidos e/ou a remoção de votos inválidos. Para resolver problemas relativos à maliciosidade de um sistema de votação digital, é necessária a utilização de um protocolo criptográfico de votação digital que atenda aos requisitos de segurança descritos na próxima seção.

3 REQUISITOS DE SEGURANÇA

Desde que o homem tem utilizado a votação como forma de expressar sua vontade, surgiu a necessidade de se estabelecer critérios de segurança e de implementação que pudessem garantir a transparência e a honestidade do processo de votação. Partindo do trabalho de [RIE 99a], de [CRA 97] e da experiência prática dos autores deste artigo, chegou-se aos requisitos de segurança:

Exatidão Um sistema de votação digital é exato se:

- A cédula de votação, onde é posto o voto, não pode ser alterada. Isto implica que ninguém pode alterar uma cédula sem ser descoberto;
- Toda cédula válida deve ser contata na apuração;
- Nenhuma cédula inválida deve ser contada na apuração. Ninguém pode duplicar um voto.

Unicidade Um sistema de votação atende a este requisito se:

- Apenas votantes autorizados participam da votação;
- Cada votante emite somente um voto.

Privacidade Um sistema de votação possui privacidade se:

- Não é possível associar a cédula ao eleitor que a depositou (**Anonimato**);
- Nenhum votante pode provar qual foi seu voto (**não-coação**);
- Todos os votos permanecem em segredo até o fim da votação (**Imparcialidade**).

Verificabilidade Um sistema de votação é verificável se permitir a recontagem dos votos. A verificabilidade pode ser de duas formas:

Universal Qualquer entidade pode verificar se todas as cédulas foram contabilizadas corretamente. Todos podem saber quem votou e quem não votou.

Individual Cada votante pode verificar se sua cédula foi contabilizada corretamente.

Os diversos tipos de votação e o propósito a que se destinam influem o estabelecimento de quais requisitos de segurança o sistema deve atender. Por exemplo, uma enquete sobre a mulher mais bonita do Brasil não precisa atender a todos os requisitos, porém uma eleição para governador de estado precisaria atender a todos esses requisitos.

Os requisitos de privacidade e verificabilidade parecem ser contraditórios visto que a adição de privacidade a um protocolo compromete diretamente a verificabilidade e vice-versa. A maioria dos protocolos de votação digital, como por exemplo o de [CRA 97], não atende a este requisito. Acredita-se que o Farnel seja um dos poucos protocolos que atende a ambos os requisitos simultaneamente.

4 FASES DE UM PROCESSO DE VOTAÇÃO DIGITAL

Um processo de votação digital é composto de várias fases com atividades específicas. Um bom exemplo é a estrutura do processo eleitoral brasileiro: há um período para alistamento de votantes onde os mesmos requerem seus títulos de eleitor, um período para os candidatos se inscreverem no processo, outro período para realização da votação e um período para apuração e divulgação dos resultados.

De forma geral, pode-se definir as seguintes fases para um processo de votação digital: **configuração**, **alistamento**, **votação**, **encerramento** e **apuração e divulgação dos resultados**. A fase de configuração é onde se dá início ao processo: nesta fase o sistema de votação é estruturado para realizar atividades relativas à configuração do mesmo. Um exemplo de atividade realizada nesta fase é a definição das opções de votos. A fase de alistamento é a fase onde os eleitores que desejam emitir voto manifestam seu desejo de votar perante uma autoridade de alistamento (entidade que realiza o cadastro dos votantes). Na fase de votação os votantes emitem seus votos. No encerramento o processo de recebimento de votos é finalizado de forma a não permitir mais a emissão de votos pelos votantes. A fase de apuração é onde os votos são contados e o resultado é divulgado.

5 O PROTOCOLO FARNEL

O protocolo possui cinco entidades principais: O votante-**V**, certificados digitais que são utilizados como títulos de eleitor; a Autoridade de Alistamento-**AA** responsável pelo registro de eleitores aptos a votar; a Autoridade de Votação-**AV** responsável pela condução da votação; as Autoridades de Escrutínio-**AE** fiscais; o diretório público-**DP** responsável por publicar informações relativas à votação; uma rede de misturadores ou **Cesto 1** responsável pelo recebimento dos votos; e o **Cesto 2** que recebe votos enviados pelo **Cesto 1**.

A idéia básica do protocolo é a existência de dois cestos. O **Cesto 1** é inicializado com k votos em branco assinados pelas **AE**. Esta inicialização acontece da seguinte forma: se existirem por exemplo dois candidatos (A e B) e, o valor de k for igual 100, são depositados 100 votos do candidato A e 100 votos do candidato B no **Cesto 1**, sendo esses votos previamente assinados pelas **AE** antes do depósito. O **Cesto 2** inicia a votação vazio. No início da votação, **V** recebe o voto assinado cegamente [SCH 96] da **AV**, remove o fator de ocultação e envia o voto para o **Cesto 1**. O **Cesto 1** é então embaralhado e um novo voto é retirado para ser depositado por **V** no **Cesto 2**.

O funcionamento total do protocolo consiste em cinco fases: configuração, alistamento, votação, encerramento da votação e apuração. A **fase de configuração**, que possui dentre outras funções a geração dos certificados digitais das autoridades, é onde acontece a criação pela **AV** de um **arranjo C** composto por todas as possíveis combinações de votos. Este arranjo é verificado e assinado por **AE** e em seguida publicado em **DP**. O fato de esse arranjo ter sido gerado com todas as possíveis cédulas evita que, durante a fase de votação, seja possível saber qual a cédula inserida por **V**. Por outro lado, se apenas um sub-arranjo das cédulas disponíveis está na urna, existe a possibilidade de a cédula do **V** não pertencer a este sub-arranjo e ser retirada logo em seguida da urna, quebrando portanto o requisito de privacidade. A **fase de alistamento**, que possui dentre outras funções a geração de certificados digitais para eleitores

que não os possuem, é onde o arranjo inicial de cédulas é criado baseado no **arranjo C**. Essas cédulas serão depositadas no **Cesto 1**. O arranjo é criado de forma que para cada opção de voto existem k cédulas idênticas. Esse arranjo é assinado pelas **AE** e disponibilizado no **DP**. A **fase de votação** é o coração do protocolo. Esta fase consiste em: etapa de autenticação mútua, etapa de obtenção de cédula em branco e etapa de emissão da cédula com os votos. A figura 1 ilustra esta fase do protocolo. Os números desta figura representam os passos do protocolo e são descritos a seguir.

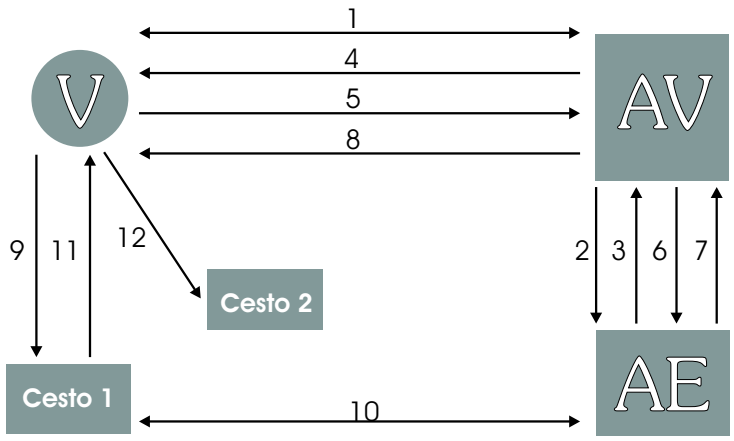

Figura 1: Fase de Votação do Protocolo Farnel.

Na etapa de autenticação mútua os **V**s e a **AV** identificam-se de forma recíproca utilizando seus certificados digitais (1).

Após a autenticação, acontece a etapa de obtenção da cédula em branco. A cédula é gerada pela **AV** com as opções de voto e enviada para as **AE** (2) que fazem a verificação e assinatura da cédula, devolvendo-a em seguida para a **AV** (3) que a repassa para o **V** (4).

Após o recebimento da cédula em branco por **V** acontece a etapa de emissão da cédula com votos. Nesta etapa o **V** assina a cédula em branco que será enviada posteriormente para a **AV**, confirmando que o **V** recebeu a cédula em branco. O **V** faz sua opção de voto gerando a cédula preenchida, que é ocultada com um fator de ocultação w, gerando a cédula preenchida ocultada. **V** então envia para a **AV** (5) um envelope assinado contendo sua identidade digital, a cédula em branco e a cédula preenchida ocultada. A **AV** então repassa (6) este envelope para as **AE** que verificam a assinatura do **V**, registram em suas listas particulares de **V**s a entrega da cédula preenchida e procedem a assinatura cega da cédula preenchida ocultada por **V**. Após todas as autoridades de escrutínio assinarem cegamente a cédula preenchida, ela é repassada à **AV** (7) que a envia para **V** (8).

De posse da cédula preenchida ocultada assinada pelas autoridades de escrutínio, **V** remove o fator de ocultação w e obtém a cédula preenchida assinada pelas **AE**. Esta cédula é então enviada (9) para o **Cesto 1** que, ao receber a cédula, verifica (10) com as **AE** se **V** já depositou sua cédula antes. Em caso de resposta negativa de todas as **AE**, o **Cesto 1** recebe o voto e embaralha o conjunto de votos que ele possui, retirando um outro voto qualquer de forma aleatóriaque é enviado (11) A **V**. **V** então de posse do voto enviado pelo **Cesto 1**, o envia (12) para o **Cesto 2** finalizando o processo de emissão de voto.

Na **fase de encerramento** as **AE** solicitam o esvaziamento do **Cesto 1** e assinam o arranjo

resultante depositando-o no **Cesto 2**. A partir deste momento, nenhuma cédula pode ser inserida no arranjo. As cédulas do arranjo são publicadas em **DP**. A apuração é dada a partir da diferença entre os votos do **Cesto 2** e, o arranjo inicial que fora adicionado ao **Cesto 1**. O arranjo final resultante da diferença é publicado em um **DP**.

6 ANÁLISE DO PROTOCOLO FARNEL

Esta seção analisa os requisitos de segurança do Farnel. Para a análise parte-se do princípio que pelo menos uma autoridade de escrutínio é honesta e, de acordo com [CHA 81], que pelo menos um dos servidores que compõem o **Cesto 1** é honesto.

A seguir é apresentado a análise do protocolo quanto ao cumprimento dos requisitos.

A cédula não pode ser alterada Como as cédulas inseridas no **Cesto 1** são previamente assinadas pelas **AE**, qualquer alteração nessas cédulas pode ser detectada.

Toda cédula válida deve ser contada na apuração Como os **V**s encaminham suas cédulas ao **Cesto 1**, pressupõe-se que o arranjo inicial contenha todas as cédulas válidas. Neste caso a apuração é exata desde que o componente computacional que faça a apuração seja correto. A exatidão da apuração está ligada diretamente à exatidão da verificação: se o componente responsável pela apuração falhar por algum motivo é possível que entidades independentes consigam verificar esta falha na contagem.

Nenhuma cédula inválida deve ser contada na apuração Analogamente ao item anterior, a correção do componente computacional é fator a ser considerado, e a possibilidade de verificação da apuração resolve a confiança na exatidão da apuração. Quaisquer cédulas inválidas que porventura tenham sido inseridas no **Cesto 1** não terão a assinatura das **AE** e conseqüentemente não podem ser consideradas na apuração.

Apenas Vs autorizados participam da votação Para **V** receber uma cédula em branco válida é necessário que ele se autentique perante a **AV** e receba uma cédula em branco assinada pelas **AE**. Para que **V** consiga depositar a cédula no **Cesto 1** é necessário que ele se identifique através de uma assinatura com sua chave privada, a qual é contrastada com a chave pública presente no certificado digital que está na lista de **V**s autorizados durante a fase de alistamento. Desta forma, **V**s que não estejam presentes na lista de **V**s não conseguirão depositar cédulas no **Cesto 1**.

Cada V emite somente um voto O **Cesto 1**, antes de aceitar uma cédula preenchida, verifica com todas as **AE** se o **V** autenticado já não depositou a cédula antes. Caso alguma **AE** indique que **V**s já entregou a cédula, ele é impedido de entregar quaisquer outras cédulas.

Não é possível associar a cédula ao eleitor que a depositou Como a cédula preenchida por **V** é inserida no **Cesto 1**, e por definição o **Cesto 1** é honesto, o rastreamento entre **V** e a cédula é inexeqüível. Além disso, a cédula em branco que **V** recebe para poder gerar a cédula preenchida com seus votos não contém nenhuma identificação que permita o rastreamento de **V**.

Nenhum V pode provar qual foi seu voto Como a cédula preenchida POR **V** é inserida no **Cesto 1**, não é possível estabelecer a ligação entre **V** e a cédula. Ademais, a cédula que **V** recebe do **Cesto 1** após inserir sua cédula preenchida e assinada pelas **AE** é uma cédula aleatória. Por conseguinte, **V** não consegue provar qual foi a cédula que ele preencheu. Observa-se que **V** detém em seu poder duas cédulas assinadas pelas **AE**: a sua própria cédula, por ele preenchida, e outra cédula que foi-lhe enviada pelo **Cesto 1**. Estas duas cédulas são indistinguíveis. Nenhuma delas pode ser utilizada como prova dos votos de **V** por que elas também são idênticas a todas as outras cédulas.

Todos os votos permanecem em segredo até o fim da votação As cédulas permanecem no **Cesto 1** cifradas com as chaves públicas de cada servidor. Enquanto o **Cesto 1** não for instruído a esvaziar todo o seu conteúdo garante-se a confidenciabilidade de todas as cédulas.

Verificabilidade universal Considerando-se que todos os arranjos envolvidos na fase de apuração, bem como a lista de **V**s, estão publicados em DP, qualquer entidade pode utilizar estes arranjos para verificar a correta apuração da votação.

Considera-se assim que o protocolo Farnel atende a todos os requisitos definidos na seção 3.

7 CONSIDERAÇÕES FINAIS

Este artigo apresentou o Farnel, um protocolo criptográfico que pode ser utilizado em votações digitais através da Internet. Buscando mimetizar o processo eleitoral brasileiro antes do advento da urna eletrônica, o protocolo baseia-se em entidades conhecidas: o **V** (eleitor), certificados digitais (títulos de eleitor), a autoridade de votação (equiparável ao papel do TSE e TREs nas eleições brasileiras), autoridades de escrutínio (fiscais) e os cestos de votos (urnas). O **Cesto 1** é implementado através de uma rede de misturadores, primitiva esta que propicia o anonimato dos **V**s ao transmitirem a cédula de votação. Assinaturas cegas são utilizadas para garantir que as autoridades de escrutínio possam assinar as cédulas sem que tenham conhecimento de seu conteúdo. A utilização de autoridades de escrutínio provê maior lisura ao processo de votação, distribuindo a relação de confiança de forma a diminuir a dependência de uma única entidade. Uma vez que atende os requisitos de segurança enumerados neste documento, o protocolo pode ser considerado seguro.

Redes de misturadores para o protocolo Farnel precisam de duas características especiais: (i) autenticação de transmissor: no caso do protocolo, apenas **V**s que ainda não tenham depositado cédulas podem enviá-las para a rede de misturadores; e (ii) esvaziamento autenticado, em que apenas um grupo de entidades podem solicitar o esvaziamento da rede de misturadores. A especificação de uma rede de misturadores com estas características está em andamento.

Atualmente está sendo desenvolvido um sistema de votação digital que utiliza o protocolo Farnel para conduzir votações na Internet a fim de que se possa analisar o protocolo sob o ponto de vista de implementação.

Referências Bibliográficas

[BEN 86] BENALOH, J. D. C.; YUNG, M. Distributing the power of a government to enhance the privacy of voters (extended abstract). In: PROCEEDINGS OF THE 5TH SYMPOSIUM ON PRINCIPLES OF DISTRIBUTED COMPUTING, CALGARY, AB, AUGUST 1986, 1986. **Proceedings...** New York: ACM, 1986. p.52–62.

[BOR 96] BORRELL, J.; RIFÀ, J. An implementable secure voting scheme. **Computer & Security**, [S.l.], v.15, n.4, p.327–338, 1996.

[CHA 81] CHAUM, D. Untraceable electronic mail, return addresses and digital pseudonyms. **Communications of the ACM**, [S.l.], v.24(2), p.84–88, 1981.

[CRA 97] CRANOR, L. F.; CYTRON, R. K. Sensus: A security-conscious electronic polling system for the internet. In: PROCEEDINGS OF THE HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 1997. **Proceedings...** Wailea, Hawaii: [s.n.], 1997.

[DEV 01] DEVEGILI, A. J. **Farnel: Uma Proposta de Protocolo Criptográfico Para Votação Digital**. Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina, 2001. Dissertação de Mestrado.

[FUJ 92] FUJIOKA, A.; OKAMOTO, T.; OHTA, K. In auscrypt '92, a practical secret voting scheme for large scale elections. In: LECTURE NOTES IN COMPUTER SCIENCE, 1992. Springer-Verlag, 1992. p.244–251.

[IT 00] ITU-T. The directory - authentication framework. 2000. Recommendation x509.

[JUA 97] JUANG, W.-S.; LEI, C.-L. A secure and practical electronic voting scheme for real world enviroments. **IEICE Trans. on Fundamentals of Electronics**, [S.l.], v.E80-A, n.1, p.64–71, 1997.

[RIE 99a] RIERA, A. **Design of Implementable Solutions for Large Scale Electronic Voting Schemes**. Autonomous University of Barcelona, dec, 1999. Tese de Doutorado.

[RIE 99b] RIERA, A.; BORRELL, J. Practical approach to anonymity in large scale electronic voting schemes. In: NETWORK AND DISTRIBUTED SYSTEMS SECURITY, NDSS '99, 1999. Internet Society, 1999. p.69–82.

[SCH 96] SCHNEIER, B. **Applied Cryptography: Protocols, Algorithms, and Source Code in C**. 2. ed. New York: John Wiley & Sons, 1996. 758 p.