Ostracon: Um Sistema de Votação Digital Segura pela Internet

Fabiano Castro Pereira , Ricardo Felipe Custódio

[1]Laboratório de Segurança em Computação – Universidade Federal de Santa Catarina
Caixa Postal 246 – 88040-900 Florianópolis, SC

castro@inf.ufsc.br, custodio@inf.ufsc.br

Abstract. *It is presented the Ostracon System of secure digital voting through the Internet, which implements the Farnel cryptographic protocol. It is made a comparison of this system among others.*

Resumo. *Apresenta-se o Sistema Ostracon de votação digital segura pela Internet, que implementa o protocolo criptográfico Farnel. É feita uma comparação deste sistema com outros existentes.*

1. Introdução

Com o grande crescimento da Internet surgem novas oportunidades no que diz respeito a novas aplicações. Por exemplo a realização de votações, que permitem aos usuários da grande rede realizarem escolhas e tomarem decisões a respeito de temas diversos. Entretanto, uma questão fundamental é a segurança, não apenas a segurança computacional mas principalmente a segurança associada ao processo de votação, o qual precisa ser muito bem elaborado para evitar fraudes.

A pesquisa por soluções em sistemas de votação digital segura tem sido realizada por empresas e universidades em diversos locais, principalmente nos Estados Unidos, que no ano de 2000 viveu um incidente desagradável, onde as eleições para presidente, feitas de forma manual, tiveram uma demora incômoda até que se obtivesse o resultado final. Em geral, a segurança de sistemas informatizados é obtida com o uso da criptografia, entretanto, as técnicas criptográficas não são suficientes, o processo de votação como um todo precisa ser seguro, pois possui requisitos de segurança que vão além daqueles tradicionais: autenticidade; integridade; não repúdio; e tempestividade. Para determiná-los e garanti-los é preciso estabelecer protocolos criptográficos para os processos de votação, sendo este o principal foco da pesquisa em votação digital.

Com o objetivo de realizar pesquisas na área de votação digital iniciou-se no ano de 2000 o **Projeto Ostracon**. Uma primeira etapa do projeto, resultou na proposta de um protocolo criptográfico para votação digital, o protocolo **Farnel** [Devegili, 2001] e numa implementação simplificada denominada **Sistema Ostracon** [Pereira and Mazzi, 2001]. Uma segunda implementação, com várias melhorias, foi fruto de um estudo sobre protocolos criptográficos para votação digital [Araújo, 2002].

Este artigo mostra os esforços realizados no Projeto Ostracon, e está dividido da seguinte forma: a seção 2 apresenta as características e problemas presentes em uma votação digital, a seção 3 apresenta o protocolo Farnel, a seção 4 faz uma análise do

cumprimento dos requisitos de segurança, a seção 5 apresenta o andamento do projeto Ostracon, a seção 6 faz uma comparação com outras propostas, e a seção 7 conclui o artigo.

2. Votação Digital

Tanto para votações com pequeno número de pessoas quanto para grandes eleições com milhares de participantes, o uso de sistemas informatizados para a realização das votações apresenta como vantagem o reduzido custo e a velocidade na apuração e publicação dos resultados quando comparado aos sistemas tradicionais de votação baseados em cédula papel. Com o uso da Internet, conseguiu-se também a mobilidade, onde o votante necessita apenas de um computador conectado à grande rede para exercer seu direto de votar. Entretanto, para se desfrutar destas vantagens existem problemas que põem em risco a segurança das informações tal como a alteração de um voto trafegando na rede, a emissão de votos falsos ou ainda a divulgação do conteúdo de um voto.

O uso de criptografia soluciona os problemas relacionados à segurança da informação que trafega nas redes de computadores de forma a tornar impossível a obtenção não autorizada de informações sigilosas, no caso os votos, nem a produção ou alteração das mensagens trocadas. Entretanto, existem requisitos de segurança que tem por objetivo garantir a transparência e a honestidade do processo de votação, que precisam de outros mecanismos e ferramentas para serem garantidos. Eles podem ser classificados em requisitos de: **exatidão**, **democracia**, **privacidade** e **verificabilidade**.

Partindo-se destas classes definiu-se os seguintes requisitos de segurança [Riera, 1999, Cranor and Cytron, 1997]: a cédula não pode ser alterada; toda cédula válida deve ser contada na fase de apuração; nenhuma cédula inválida deve ser considerada no momento da apuração; apenas os votantes autorizados podem participar da votação; cada votante pode emitir apenas um voto; não pode ser possível a associação de uma cédula ao seu respectivo eleitor (Anonimato); não pode ser permitido que um votante consiga provar qual foi seu voto (Não-coação); todos os votos devem ficar em segredo até o fim da eleição (Imparcialidade); deve ser possível verificar que as cédulas foram contadas corretamente. Este último requisito apresenta-se de duas formas: uma, denominada *verificabilidade universal*, diz que qualquer entidade, independentemente, pode verificar que todas as cédulas foram contadas corretamente; e outra, denominada *verificabilidade individual*, diz que cada votante deve ter meios para verificar que sua cédula foi contada corretamente. Estes requisitos podem ser utilizados para se avaliar protocolos criptográficos de votação digital, existindo situações onde alguns destes requisitos não precisam ser necessariamente cumpridos.

3. Protocolo Farnel

Este protocolo [Araújo et al., 2002] é voltado para a fase de votação, entretanto, outras fases também são importantes para a segurança do processo como um todo. Para a operação do protocolo são definidas algumas entidades, denominadas autoridades, que interagem entre si para a realização das comunicações. A **Autoridade de Votação (AV)** é a responsável por coordenar as tarefas da votação; a **Autoridade de Alistamento (AA)** emite certificados digitais para que um **Votante (V)** esteja autorizado a votar, e mantém

a lista de votantes; e as **Autoridade de Escrutínio (AE)** garantem que a **AV** agirá honestamente. Além das autoridades, existem duas outras entidades, denominadas **Cesto 1 (C1)** e **Cesto 2 (C2)**, que participam do processo recebendo os votos e tratando-os de forma anônima. **C2** consiste de um repositório final para os votos efetuados. **C1** é o responsável pelo anonimato e consiste de uma rede de mistura, mecanismo proposto em [Chaum, 1981] que funciona da seguinte forma: a rede consiste de diversos servidores que encaminham mensagens que chegam, porém escondendo a relação entre as que chegam e as que saem. Para tanto o servidor agrupa um número de mensagens que chegam, misturando-as antes de serem encaminhadas. Como os servidores são concatenados, enviando suas mensagens uns para os outros, ao final da rede a mensagens alcançará seu destino de forma anônima desde que ao menos um servidor mantenha secreta sua relação de entrada/saída.

3.1. Fases de configuração e alistamento

Na configuração da votação é emitido um certificado digital para a **AV** que indica a qual votação aquele certificado se destina. É definido um conjunto de **AEs**, e cada autoridade recebe um certificado digital. Os certificados, juntamente com outras informações, são publicados em um local denominado **diretório público**. Também é gerado um conjunto de cédulas contendo todas as possíveis combinações de opções de votos, visando garantir o requisito de privacidade, pois durante a fase de votação é retirado um voto aleatoriamente deste conjunto e inserido o voto recebido, como todos os possíveis votos estavam presentes, não se pode saber qual o voto inserido. Este conjunto inicial é assinado pelas **AEs** e colocado no diretório público. No alistamento os votantes se autenticam perante a **AA** e recebem um número de identificação que é incluído na lista de votantes.

3.2. Fase de Votação

A figura 1 ilustra o funcionamento do protocolo. O primeiro passo consiste na autenticação mútua entre **V** e **AV**. **V** apresenta seu número de identificação e o certificado correspondente, presente na lista de votantes. Para ter certeza de que está se comunicando com a **AV** correta, **V** obtém o certificado da mesma e verifica a existência do número de identificação da votação.

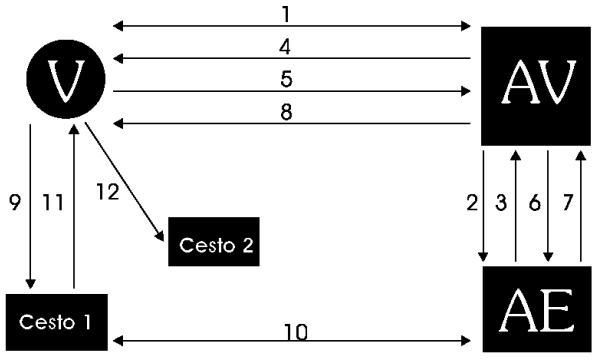

Figure 1: Passos do Protocolo Farnel

No segundo passo é gerada a cédula em branco, ela é criada por **AV** contendo as opções de voto. As **AEs** verificam a cédula e assinam, enviando-a de volta para **AV** (terceiro passo). Ao receber de **AV** a cédula assinada (quarto passo) **V** verifica a assinatura das **AEs**, através da chave pública de cada autoridade, e obtém a cédula em branco.

A última parte desta fase consiste na emissão da cédula com votos. Primeiramente **V** assina a cédula em branco, que posteriormente será enviada à **AV** como comprovante do recebimento de uma cédula em branco e entrega de uma preenchida. Esta

cédula preenchida precisa ser assinada pelas **AEs**, porém sem que as mesmas vejam o voto realizado. Para tanto o Farnel faz uso do mecanismo de assinaturas cegas, proposto por [Chaum, 1981], e que consiste em se poder assinar determinada informação sem que seja necessário conhecer seu conteúdo. Faz-se uso de algumas propriedades dos números primos envolvidos em assinaturas com chave assimétrica RSA. Primeiramente é feita uma operação denominada **ocultação**, onde a mensagem é ocultada com um **fator de ocultação**. A mensagem ocultada é então enviada para assinatura. Após ter recebido a mensagem já assinada é então retirado o fator de ocultação, obtendo-se a mensagem original, porém com uma assinatura válida da mesma.

No Farnel **V** oculta a cédula preenchida com um fator de ocultação e depois cria um envelope digital contendo seu número de identificação, a cédula em branco assinada, e a cédula preenchida oculta. Este envelope é então assinado por **V** e enviado à **AV** (quinto passo), a qual o repassa às **AEs** (sexto passo). Cada **AE** verifica a assinatura do envelope, de acordo com o certificado digital presente na lista de votantes, registra a entrega do voto, e realiza a assinatura cega da cédula preenchida. Com o voto assinado cegamente por cada **AE**, a cédula é devolvida à **AV** (sétimo passo), que a envia para **V** (oitavo passo). Ao recebê-la **V** remove o fator de ocultação e obtém então a cédula preenchida e assinada, que é enviada ao **C1** (nono passo) com seu número de identificação. Ao receber a cédula, o **C1** verifica com as **AEs** que aquele votante ainda não realizou seu voto (décimo passo). Após a confirmação das **AEs**, **C1** retira uma cédula aleatória e a envia para **V** (décimo primeiro passo). **V** então deposita a cédula recebida em **C2** (décimo segundo passo), finalizando o processo de emissão do voto.

3.3. Fases de encerramento e apuração

No encerramento as **AEs** solicitam o esvaziamento das cédulas que ainda restarem em **C1**, assinam este conjunto, e o depositam em **C2**, que passa a conter todas as cédulas que foram assinadas pelas **AEs** desde o início do processo de votação. Este conjunto de cédulas é então publicado no diretório público. Na apuração os votos criados para preencher **C1**, que abrangiam todas as possibilidades de voto, são retirados do conjunto obtido no encerramento. Este conjunto final, que consiste dos votos realizados pelos votantes, é então colocado no diretório público, bem como o resultado da votação em formato apropriado. Como o conjunto inicial de votos foi publicado na fase de alistamento, o conjunto presente em **C2** foi publicado na fase de encerramento, e o conjunto final resultante da apuração foi também publicado, qualquer entidade pode fazer a verificação da exatidão da apuração.

4. Análise dos Requisitos de Segurança

Para se demonstrar que o protocolo Farnel cumpre os requisitos de segurança é preciso considerar, *a priori*, dois princípios. O primeiro princípio diz que ao menos uma **AE** deve ser honesta. O segundo é que ao menos um dos servidores da rede de mistura seja honesto.

Primeiramente tomemos os requisitos de **exatidão**. A impossibilidade de se alterar uma cédula (primeiro requisito) é garantida pelo fato de que as cédulas inicialmente inseridas em **C1** foram antes assinadas pelas **AEs**, permitindo a detecção de qualquer

cédula alterada. A garantia de que toda cédula válida é contada na fase de apuração (segundo requisito) é dada pelo fato de que a rede de mistura contém inicialmente as cédulas válidas, as quais vão sendo substituídas por aquelas emitidas pelos votantes, sendo que na apuração todos os votos realizados, e apenas eles, ficam disponíveis para apuração, que pode ser realizada por qualquer entidade. Também nenhuma cédula inválida é contada na apuração (terceiro requisito), pelo mesmo motivo de que as cédulas válidas são assinadas pelas **AEs**, qualquer cédula inválida que porventura venha a estar presente no **C1** será facilmente identificada e descartada. Os dois requisitos de **democracia** também são cumpridos. Para que apenas votantes autorizados participem da votação (quarto requisito), é feita a autenticação de **V** perante as entidades com as quais ele se comunica, e é verificada sua presença na lista de votantes autorizados. Especificamente quando **V** se comunica com **C1** é feita uma verificação para saber se **V** já realizou algum voto, o que garante que **V** emita apenas um voto (quinto requisito).

O anonimato (sexto requisito), que é o primeiro requisito de **privacidade**, é cumprido por se utilizar uma rede de mistura (**C1**), o que torna impossível a associação entre **V** e seu voto. A não-coação (sétimo requisito) também é garantida pelo fato de se utilizar uma rede de mistura, além disso a cédula que **V** recebe de **C1** no final não é a sua cédula preenchida, o que também impossibilita a **V** mostrar seu voto a alguém. E a imparcialidade (oitavo requisito) é obtida pois as cédulas permanecem cifradas dentro de **C1** até que o mesmo seja esvaziado, mantendo os votos em segredo até o final da votação. A verificabilidade **universal** é garantida (nono requisito). Esta é garantida pois todos os dados envolvidos no processo da votação são publicados no diretório público, o que habilita qualquer entidade a verificar a apuração.

5. Sistema Ostracon

O Sistema Ostracon, parte do esforço do Projeto Ostracon, tem o objetivo de ser completo em todas as necessidades de uma votação digital, tanto no ponto da implementação de protocolos quanto no que se refere à imunidade a ataques. O sistema ainda se encontra em desenvolvimento, sendo que as implementações funcionais já realizadas não contemplam alguns aspectos que só passam a ter grande influência quando é utilizado em larga escala.

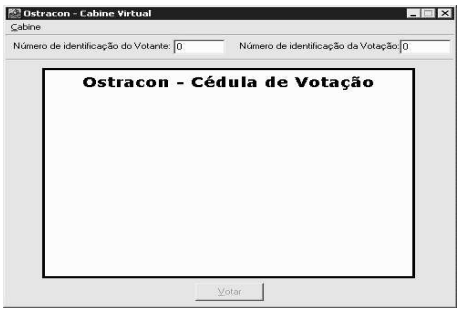

Figure 2: Cabine Virtual

5.1. Implementação inicial

A primeira versão do Sistema Ostracon implementou de forma parcial o Farnel. Foi feita uma análise da especificação do protocolo visando identificar as necessidades de aplicações para torná-lo funcional. Foram implementadas seis aplicações, sendo que três refletem as entidades do protocolo (Alistamento, Votação e Escrutínio), uma gerencia o diretório público, outra atua como rede de mistura, e a última atua como interface do sistema para com um votante (Figura 2). Quanto às entidades implementadas foram feitas duas simplificações com o objetivo de tornar a implementação

viável em tempo reduzido, a primeira foi com relação à **AE**, sendo implementada apenas uma autoridade, e não um conjunto delas como prevê o protocolo Farnel; e a segunda simplificação foi com relação à rede de mistura, que na implementação foi concentrada em apenas uma aplicação, ao invés de diversos servidores. Mesmo com essas simplificações o sistema continuou apresentando as características de segurança proporcionadas por estas entidades, apenas em um nível menor. Nesta primeira implementação é preciso instalar cada aplicação no seu respectivo local, o que difere da segunda versão do sistema, descrita na próxima seção, feita para o ambiente web, tornando mais simples o uso do sistema.

5.2. Implementação Web

A segunda implementação do Sistema Ostracon teve como objetivo maior tornar possível o teste de outros protocolos para votação digital além do protocolo Farnel. O sistema foi concebido tendo em vista as fases de um processo de votação digital. Estas fases em geral são aquelas descritas anteriormente: **configuração**, **alistamento**, **votação** e **apuração** (com a devida divulgação dos resultados), sendo que a fase de alistamento pode estar incluída na de configuração caso seja uma votação onde o administrador mesmo cadastra os votantes aptos, e as demais fases são sempre necessárias para a realização de uma votação digital.

Também foram implementadas funcionalidades que vão além daquelas necessárias para um protocolo de votação digital. Pode-se definir características extras de uma votação, tais como os horários de início e término, e regras para aceitação de votantes que desejem alistar-se. Também criou-se mecanismos que permitem a realização de auditorias nos procedimentos da votação, através da publicação dos dados da votação, periodicamente, à medida que a votação vai avançando ao longo das fases. Contudo, apesar destas possibilidades de auditoria, é de fundamental importância a escolha de um protocolo que tenha implementado o requisito da verificabilidade dos resultados.

A implementação do sistema foi feita utilizando-se linguagem de script no servidor, sendo que para as funcionalidades que necessitam de criptografia foi utilizada a biblioteca *OpenSSL*, que permite o uso de certificados digitais, criptografia simétrica e assimétrica, funções resumo, e demais ferramentas criptográficas. Para a operação dos protocolos de votação digital é necessário que alguns processamentos sejam realizados pelo cliente, no caso o navegador web. Para tanto utilizou-se applets JAVA, e scripts em JavaScript para se ter acesso à biblioteca CryptoAPI, através do objeto Capicom [Microsoft, 2002]. Os scripts da parte servidora são executados no sistema operacional Linux, enquanto que o acesso pela parte cliente precisa ser feito utilizando-se o navegador Internet Explorer, devido às funções da CryptoAPI estarem disponíveis apenas no sistema operacional Windows. A figura 3 exibe a interface do cliente ao acessar o Sistema Ostracon.

Figure 3: Interface Web

Por buscar implementar diferentes protocolos para votação digital o sistema per-

mite que se personalize cada votação, pois se em uma votação em especial não for necessário o requisito do anonimato, então pode-se escolher um protocolo mais simples, que cumpra apenas os requisitos desejados àquela votação em especial. Os protocolos atualmente implementados na segunda versão do Sistema Ostracon são dois: um protocolo simples e um protocolo de assinatura cega. O protocolo simples considera que se está trabalhando com uma **AV** confiável, assim, cumpre-se os requisitos de uma votação digital, exceto o requisito da verificabilidade. O outro protocolo implementado faz uso de assinaturas cegas, e pode ser utilizado quando não se tem plena confiança na autoridade de votação, apesar de este protocolo não atender a todos os requisitos de uma votação digital.

O protocolo Farnel faz uso principalmente de dois mecanismos, o de assinaturas cegas e o de rede de mistura, como a assinatura cega já está implementada nesta segunda versão do sistema, para a implementação do Farnel torna-se necessária uma implementação web de uma rede de mistura. O desenvolvimento atual do Sistema Ostracon está voltado a acrescentar outros protocolos de votação digital ao grupo de protocolos implementados, principalmente o protocolo Farnel. Está se estudando a possibilidade e a viabilidade de uso de uma rede de mistura proposta recentemente [Jakobsson et al., 2002], e que permite uma implementação via web, em conjunto com o Sistema Ostracon.

6. Outros Protocolos e Sistemas

Em [Riera, 1998] encontra-se uma proposta de protocolo de votação que se propõe a resolver principalmente o problema de anonimato através do mecanismo de assinatura cega. Entretanto, este protocolo não se preocupa com o requisito da não-coação [Araújo, 2002], pois conforme a descrição do protocolo o votante tem a possibilidade de exibir o resultado da assinatura cega da **AV** a uma outra pessoa, caso seja coagido para tanto. Os pontos fortes deste protocolo são a garantia do anonimato, através da assinatura cega, impedindo a autoridade de votação de saber o voto de cada votante; e a garantia da verificabilidade individual, pois cada votante tem meios para verificar que seu voto foi contabilizado. Entretanto, existem pontos fracos que inviabilizam o uso do protocolo em diversas situações. Um ponto fraco é que não existe uma lista de votantes autorizados, o que impede o cumprimento de diversos requisitos de segurança, principalmente os de democracia. O principal ponto fraco do protocolo é a necessidade de confiança plena na autoridade de votação. Caso ela venha a agir de forma desonesta, outra parte dos requisitos deixa de ser cumprido.

O sistema de votação Sensus [Cranor and Cytron, 1997] também faz uso de assinatura cega para prover anonimato, mas também não cumpre o requisito de não-coação. O diferencial é a existência de uma outra entidade, denominada **autoridade de registro**, que age em conjunto com a **AV** e tem o objetivo de autorizar votantes a participar da votação. Os pontos fortes são a garantia do anonimato e a verificabilidade individual, além do que a existência da autoridade de registro faz com que os requisitos de democracia sejam cumpridos. O sistema também apresenta pontos fracos. O principal ponto fraco é o fato de que a lista de votantes autorizados não é previamente publicada [Araújo, 2002]. Isto faz com que alguns requisitos sejam comprometidos caso a autoridade de registro venha a agir de forma desonesta. Também ocorre que outros requisitos podem deixar de ser cumpridos caso a **AV** também venha a agir de forma desonesta.

7. Considerações Finais

O Projeto Ostracon tem obtido resultados bastante satisfatórios, principalmente com a definição do protocolo Farnel, que tem capacidade de atender a todos os requisitos de segurança presentes em uma votação digital. Também trouxeram grande contribuição as duas implementações realizadas do Sistema Ostracon, principalmente para a identificação das necessidades de implementação de sistemas deste tipo e com esta complexidade.

As limitações ainda presentes no projeto, principalmente quanto à implementação do sistema, já possuem propostas de solução em andamento, sob pesquisa, e com o desenvolver do projeto deverão ser solucionadas, bem como o aprimoramento das características e funcionalidades já implementadas. Quanto ao protocolo Farnel, a principal necessidade é a da sua formalização, o que permite uma validação formal, mais confiável e completa. Entretanto, a especificação formal de protocolos criptográficos ainda é um campo pouco estudado e possui poucas propostas de técnicas que permitam tal tarefa.

References

Araújo, R. S. D. S. (2002). Protocolos criptográficos para votação digital. Master's thesis, Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina.

Araújo, R. S. D. S., Devegili, A. J., and Custódio, R. F. (2002). Farnel: Um protocolo criptográfico para votação digital. *WSeg 2002 - Workshop em Segurança de Sistemas Computacionais*, pages 113–120.

Chaum, D. (1981). Untraceable electronic mail, return addresses and digital pseudonyms. *Communications of the ACM*, 24(2):84–88.

Cranor, L. F. and Cytron, R. K. (1997). Sensus: A security-conscious electronic polling system for the internet. In *Proceedings of the Hawai'i International Conference on System Sciences*, Wailea, Hawai'i.

Devegili, A. J. (2001). Farnel: Uma proposta de protocolo criptográfico para votação digital. Master's thesis, Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina.

Jakobsson, M., Juels, A., and Rivest, R. (2002). Making mix nets robust for electronic voting by randomized partial checking. *USENIX'02*.

Microsoft (2002). Capicom. http://msdn.microsoft.com/library/en-us/dnsecure/html/intcapicom.asp.

Pereira, F. C. and Mazzi, C. E. (2001). Ostracon: Sistema de votação digital na internet. Trabalho de Conclusão do Curso de Bacharelado em Ciência da Computação da Universidade Federal de Santa Catarina.

Riera, A. (1998). An introduction to electronic voting schemes. Technical Report PIRDI 9-98, Universitat Autònoma de Barcelona.

Riera, A. (1999). *Design of Implementable Solutions for Large Scale Electronic Voting Schemes*. PhD thesis, Autonomous University of Barcelona.