SIGEleição – Um Novo Jeito Seguro de Votar

Jadson Santos[1], Clarissa Lins[1], Marcos Madruga[1]

[1]Superintendência de Informática – Universidade Federal do Rio Grande do Norte (UFRN)
Caixa Postal 1524 – 59078-970 – Natal– RN – Brasil

{jadson, clarissa, madruga}@info.ufrn.br

Abstract. *The effort and cost of setting up several electronic voting machines or the work for the manual counting of hundreds or thousands of paper ballots led to emerge a demand for implementation of a web system to manage elections. This required that the system had extra safety features not present in the other systems developed by UFRN. This paper describes the SIGEleição voting system, highlighting the security mechanisms that have been implemented to provide elections for the various management positions inside UFRN.*

Resumo. *O esforço e custo de se configurar diversas urnas eletrônicas ou o trabalho para contagem manual de centenas ou milhares de votos em papel fez com que surgisse uma demanda para implementação de um sistema web para realizar votações. Nesse sentido, a UFRN desenvolveu o sistema de votação SIGEleição para que se pudesse realizar pleitos para os diversos órgãos que compõem a instituição. Este artigo descreve o sistema SIGEleição, destacando os mecanismos de segurança que foram implementados.*

1. Introdução

As instituições de ensino superiores brasileiras necessitam realizar periodicamente eleições para a escolha dos seus cargos de direção tais como: reitoria, diretoria de centros, diretoria de departamentos ou coordenações de cursos.

Normalmente essas eleições são realizadas presencialmente em várias localidades da instituição. Algumas vezes até em localidades geograficamente distintas. Isso acarreta um custo considerado para realizar essas eleições, tanto financeiro, como de recursos humanos para organizar e para trabalhar na eleição.

Nesse cenário de melhoria organizacional, efetividade e eficiência dos recursos públicos, surgiu a demanda de se desenvolver um sistema eleitoral em que se pudesse registrar votos de qualquer localidade, sem a necessidade de montar uma estrutura física grande e custosa. A votação *on-line* vem maximizar a conveniência e acesso dos eleitores, permitindo o pleito eleitoral em qualquer lugar onde se tenha acesso à Internet.

2. Métodos

Nesta seção são descritos os mecanismos de segurança que foram implementados no SIGEleição, de forma a possibilitar o uso de um sistema *on-line* para registros de votos.

2.1 Sigilo do Voto

A primeira propriedade que um sistema de votação eletrônico deve possuir é garantir que os votos registrados sejam sigilosos. Ou seja, ninguém, nem mesmo o administrador da base de dados, pode obter a informação de em que candidato o eleitor votou. Para conseguir essa propriedade, o SIGEleição foi projetado para salvar as informações dos votos em duas tabelas distintas e não relacionadas entre si. A Tabela 1 mostra uma representação da tabela denominada "Voto" e a Tabela 2 mostra uma representação da tabela VotoEleitor.

Tabela 1. Tabela Voto

id_voto	id_eleicao	id_chapa	valor	hash (128 caracteres)
12345	398221	1202	V	sdfjslfj930238dsofj20wes...
12346	398221	1203	V	92nwds923ksf923f923323...
12347	398221		B	8sd39sfds9823030909wfe0...

Tabela 2. Tabela VotoEleitor

id_eleicao	data_votacao	id_pessoa	ip_eleitor	hash (128 caracteres)
398221	22/05/2015	23423	10.3.20.123	d4slkf2989udf23wedsddf...
398221	22/05/2015	5342343	10.4.20.122	kd92lksfj20j02jwl320wd...
398221	22/05/2015	192302	192.0.2.120	80ksdfl23we0sdf0sdf0d...

A tabela Voto guarda os votos que foram computados para as eleições (coluna id_eleicao), com a indicação do valor do voto (V = válido, B = Branco e N = Nulo) e para qual candidato esse voto foi computado (coluna "id_chapa"). Nessa tabela não existe nenhuma indicação do eleitor que realizou o voto. Para salvar essa informação foi criada uma outra tabela chamada VotoEleitor.

A funcionalidade da tabela VotoEleitor é guardar o eleitor que realizou o voto, identificado pela coluna "id_pessoa", a eleição na qual o eleitor votou (coluna "id_eleicao"), a data em que o voto foi registrado (coluna "data_votacao") e algumas informações a mais para auditoria como o endereço IP do computador que o eleitor utilizou para votar (coluna "ip_eleitor"). A cada voto registrado, uma mistura aleatória na ordem dos votos é realizada, impossibilitando que alguém identifique o voto pela ordem que estão salvos.

2.2 Não Permitir Alteração de um Voto

Toda eleição criada no SIGEleição deve possuir uma comissão eleitoral, cujo presidente tem como principal função gerar e guardar sigilosamente uma chave de segurança para a eleição.

A chave de segurança é uma sequência de 64 caracteres gerados aleatoriamente pelo sistema. O ponto primordial da segurança do SIGEleição é que essa chave de segurança não é persistida. Ela fica apenas na memória do servidor que executa o SIGEleição. Ninguém que gerencia o sistema tem acesso à chave de segurança, mesmo que se possua acesso ao banco de dados.

Com a chave de segurança carregada na memória do servidor, ela é utilizada para gerar vários *hashes* [GAT UFRJ, 2017] que permitem ao sistema identificar se alguma alteração foi realizada nas tabelas auditadas.

A Figura 1 mostra o esquema de geração do hash da tabela voto.

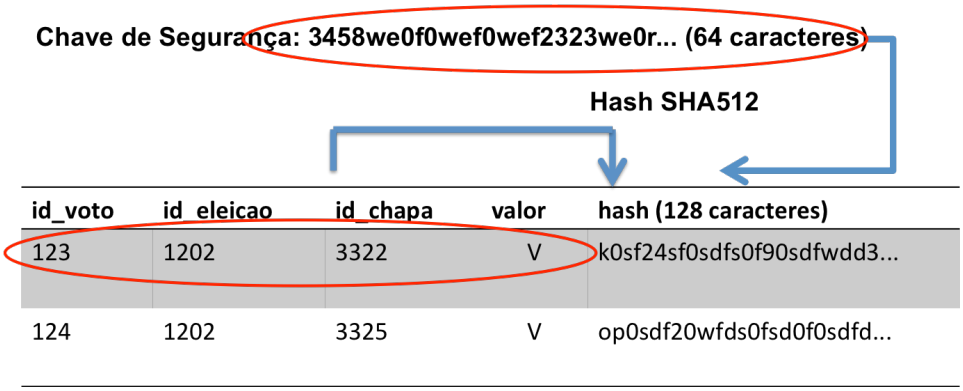

Figura 1. Esquema de Criação do Hash dos Votos

Para cada voto registrado, os dados da linha são concatenados juntos com a chave de segurança da eleição. Com o resultado dessa concatenação é então gerado um hash SHA512 de 128 caracteres para esse voto.

Como não se tem acesso à chave de segurança, não é possível calcular um hash válido. Com isso, garante-se que ninguém pode registrar um novo voto válido na base de dados do sistema. Também não é possível alterar um voto registrado, pois outra propriedade das funções de hashing é que se houver qualquer modificação de parte da informação usada na geração do hash, o hash obrigatoriamente também muda.

Por último, para garantir que um voto não seja apagado da base de dados, o SIGEleição além de gerar um hash para cada voto registrado no sistema, gera um hash geral para a eleição, que fica armazenado na tabela "eleicao". Esse hash é gerado a partir da quantidade de votos registrados até o momento na eleição.

Ao término da eleição, para homologar os resultados, o presidente deve informar novamente a chave de segurança ao sistema, que então utiliza a chave informada para verificar se todos os votos registrados são válidos.

2.3 Autenticação dos Eleitores

Outra propriedade do SIGEleição é assegurar a autenticidade do eleitor, para isso foram implementados alguns esquemas de autenticação dos usuários do SIGEleição.

O modo padrão de autenticação do SIGEleição é a utilização de *login* e senha. Todo eleitor para entrar no sistema deve informar pelo menos um *login* e uma senha que são pessoais e intransferíveis. A segurança desse método de autenticação está na segurança da senha do eleitor.

Além do *login* e senha, o SIGEleição se configurado pode solicitar que o eleitor responda uma pergunta de segurança, selecionada aleatoriamente do banco de dados. Essas perguntas de segurança tem por objetivo dificultar que usuários não humanos tentem acessar o sistema.

Outra estratégia opcional e complementar ao modo de autenticação por *login* e senha é exibir um campo de captcha [CAPTCHA 2017] junto ao campo de *login* e senha para impedir que usuários não humanos tentem acessar o sistema. Esse modo de autenticação é alternativo as perguntas de segurança.

Outro mecanismo de autenticação é a autenticação em duas etapas. Se ativado, após autenticação com *login* e senha, e algum dos outros métodos de autenticação que também estejam ativados, o sistema gerará aleatoriamente uma segunda senha para o eleitor. Essa segunda senha é então enviada para o e-mail do eleitor registrado no sistema. Para conseguir se *logar* no sistema o eleitor terá que acessar o seu e-mail, verificar a senha gerada e informá-la ao sistema em uma segunda tela de autenticação.

Após passar por todos os mecanismos de autenticação do sistema ainda é possível configurar o sistema para solicitar ao eleitor na tela de votação perguntas pessoais para confirmação do voto. Caso o eleitor erre essas perguntas pessoais, ele ficará bloqueado não podendo registrar o seu voto.

2.4. Disponibilidade

Outra propriedade desejada em um sistema de votação é que ele esteja disponível durante todo o período de votação. Isso garante que quem queira votar possa utilizar o sistema.

Como mencionado, toda eleição possui uma chave de segurança e essa chave é carregada apenas na memória do servidor. Para garantir uma maior disponibilidade do sistema ele pode executar em mais de um servidor. Para compartilhar a chave de segurança entre todas as instâncias do sistema sem persisti-la e sem comprometer a segurança do sistema, foi implementado um esquema de cache distribuído exemplificado na Figura 2 utilizando SSLSocket [SSLSocket 2017].

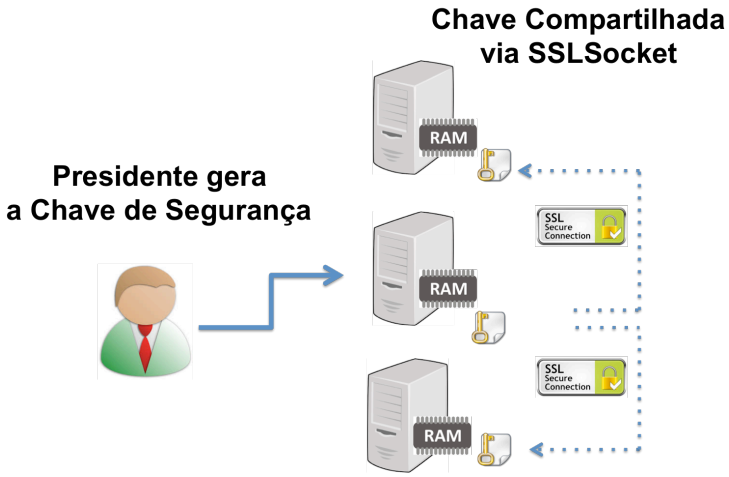

Figura 2. Compartilhamento da chave de segurança

3. Resultados

Já ocorreram mais 800 eleições, com 100.000 votos registrados, mais de 35.000 eleitores diferentes já acessaram o sistema e registraram os seus votos, em mais 1200 chapas utilizando o SIGEleição com os mecanismos de segurança descritos neste artigo.

4. Conclusões

O SIGEleição conseguiu atender aos critérios de confiabilidade e segurança para ser utilizado por uma instituição de ensino superior como a UFRN no pleito para a escolha dos representantes de diversos órgãos da universidade.

Vários grupos de interesse têm se formado para debater o tema. Os proponentes do voto *on-line* acreditam que a nova tecnologia aumentará a participação dos eleitores, permitindo que o eleitorado obtenha maior eficiência e agilidade no pleito. Assim, torna-se mais disponível o acesso ao processo democrático de escolha dos representantes.

Referências

CAPTCHA. Completely Automated Public Turing Test To Tell Computers and Humans Apart. Disponível em: http://www.captcha.net/ Último acesso em 29/03/2017

SSLSocket. Disponível em: https://docs.oracle.com/javase/7/docs/api/javax/net/ssl/SSLSocket.html. Último acesso em 29/03/2017

GAT UFRJ. Função Hashing. Disponível em: http://www.gta.ufrj.br/grad/09_1/versao-final/assinatura/hash.htm. Último acesso em 29/03/2017