Pequenos Passos em Direção a um Sistema Prático de Registro de Votantes

Alberto Sobrinho[1], Roberto Samarone Araujo[1], Juliana dos Santos[1], Matheus Castro[1], Jacques Traoré[2]

[1]Laboratório de Segurança e Criptografia Aplicada (LabSC)
Universidade Federal do Pará (UFPA)
Belém – PA – Brasil

[2]Orange Labs
Caen Cedex, France

Resumo. *Votações via Internet tornaram-se fundamentais em tempos de pandemia. Por meio delas pode-se evitar aglomerações tão comuns em eleições presenciais. Todavia, a comodidade trazida por esse tipo de votação reflete-se na facilidade de realização de ataques coercivos. As diversas soluções propostas para esse cenário possibilitam mitigar tais ataques, mas muitos fatores ainda dificultam o emprego prático delas como o registro presencial das credenciais de votação. Uma dessas soluções foi implementada por meio do sistema de votação CIVIS. Embora as primeiras versões desse sistema considerassem suposições irreais na fase de registro, a introdução de um novo protocolo de registro o tornou mais prático. Neste contexto, este trabalho complementa o trabalho anterior por meio da especificação do novo registro de credenciais. Adicionalmente, ele introduz melhorias a esse registro e apresenta os resultados dos primeiros testes a fim de verificar a sua eficácia.*

Abstract. *Internet voting became fundamental in the pandemic time. By using it, one can avoid agglomerations so common in on-site votings. However, the convenience of these votings make easy to perform coercive attacks. A number of solutions for this scenario aim at mitigating such attacks, but many factors hamper its use as the on-site registration. One of these solutions was implemented by means of the CIVIS voting system. Although the first versions of this system considered irrealistic assumptions in the registration phase, the introduction of a new registration phase protocol made it more practical. In this context, this work complements the former. It specifies the new credencial registration. In addition, it introduces improvements to the registration and shows the first effectiveness test results.*

1. Introdução

Sistemas para eleições via Internet têm recebido cada vez mais atenção principalmente devido ao cenário atual de pandemia. A necessidade de evitar aglomerações e assim conter o vírus da COVID-19 levou muitas entidades (públicas e privadas) a migrarem suas eleições presenciais para aquelas via Internet. Assim, tais sistemas tornaram-se fundamentais no atual momento. A utilização desses sistemas e sua praticidade, no entanto,

levaram muitas dessas entidades a ignorarem o problema da coação. Como eleitores podem votar a partir de qualquer dispositivo conectado à Internet (e.g. *smartphones*), eles são alvos fáceis de terceiros motivados a alterar a vontade genuína de suas vítimas. Além disso, a possibilidade de venda de votos é um problema igualmente relevante.

Em 2005, JCJ [Juels et al. 2005] introduziram a noção de resistência à coação (*coercion-resistance*). Tal noção deixa claro o que um poderoso adversário não pode ser capaz de realizar para que um protocolo criptográfico (e consequentemente o sistema de votação que o implementa) seja resistente à coação. Desde então, diversos protocolos criptográficos foram propostos visando satisfazer essa noção.

De forma a atender a noção de JCJ, esses protocolos utilizam-se da seguinte ideia. Cada votante elegível recebe uma credencial legítima de votação (e.g. um número aleatório grande, 160 *bits*), em uma etapa preliminar. Essa credencial identifica um voto válido na apuração e é entregue de forma segura ao votante. Durante a votação, o votante utiliza essa credencial para votar. Em caso de coação, o votante deve ser capaz de gerar uma credencial falsa (e.g. um outro número aleatório diferente do recebido anteriormente) e entregá-lo ao adversário. O adversário não tem como distinguir entre credenciais verdadeiras e falsas. Na apuração, as credenciais falsas são identificadas e removidas, restando apenas as credenciais legítimas que identificam os votos a serem contados. Isso é realizado sem que nenhum *bit* das credenciais seja revelado.

Um dos sistemas de votação que implementam as ideias de JCJ é o CIVIS [Araujo et al. 2018]. Até recentemente, no entanto, ele considerava credenciais que inviabilizavam o seu uso em cenários práticos. Como nesse sistema uma credencial era composta por uma tupla contendo números aleatórios grandes, era necessário armazená-la, o que facilitava ataques coercivos. De forma a viabilizar o uso prático do CIVIS, SAST [de Sá et al. 2020b] introduziram um protocolo de registro prático de credenciais que utiliza a ideia de senhas coloridas proposta por [de Sá et al. 2020]. Tais credenciais possuem uma parte pública e uma privada. Enquanto a parte pública pode ser armazenada livremente, a parte privada é formada por uma senha que deve ser mantida em segredo. Essa proposta evita que um registrador malicioso obtenha a senha do votante durante o registro e assim possa votar em seu lugar.

Além do protocolo de registro proposto por SAST, o trabalho anterior apresentou uma implementação preliminar do sistema de registro. Ele, no entanto, não incluiu detalhes importantes da implementação como a sua arquitetura. Ademais, não foram apresentados testes que pudessem comprovar ou não a sua eficácia.

O trabalho introduzido aqui primeiramente complementa o trabalho anterior por meio da especificação mais detalhada do sistema de registro seguro. Adicionalmente, ele introduz aprimoramentos nesse sistema e apresenta os primeiros resultados dos testes realizados por intermédio dele. Esses testes objetivaram verificar a eficácia do sistema durante o registro de credenciais legítimas. Consequentemente, eles validam o protocolo implementado pelo sistema. Por fim, o trabalho discute alguns aspectos relacionados as soluções apresentadas.

O trabalho está organizado da seguinte forma. A Seção 2 recapitula o sistema CIVIS bem como o protocolo de registro de senhas de SAST. A Seção 3 detalha a implementação do sistema de registro e sua integração ao CIVIS. Essa seção também

apresenta as novas melhorias introduzidas ao sistema e os resultados dos testes de efetividade realizados. Por fim, a Seção 5 conclui o trabalho e apresenta os trabalhos futuros.

1.1. Trabalhos Relacionados

A introdução do protocolo de registro prático de SAST [de Sá et al. 2020b] tornou prático o registro de votantes originalmente proposto por ABRTY. Todavia, existem outras propostas que objetivam facilitar o registro de votantes e o emprego das credenciais de votação em protocolos resistentes à coerção. [Neumann and Volkamer 2012] proporam um esquema onde a credencial legítima é armazenada em um *smart card* e o votante define um PIN para acessá-la. Apesar de tentativas de melhorá-lo, infelizmente a utilização de *smart cards* em protocolos resistentes à coação tem um problema inerente. Um adversário poderia forçar votantes a entregarem seus *smart cards* e assim impedi-los de votar. [Estaji et al. 2020] apontou problemas nesse protocolo (e em suas variantes) e propôs novas ideias que mitigam problemas anteriores. Tais ideias também possibilitam corrigir PINs incorretamente informados por erros de digitação e podem ou não empregar *smart cards*. Infelizmente a eficácia de tais propostas ainda não foram comprovadas em cenários práticos. O trabalho apresentado aqui não utiliza PINs e nem requer *smart cards*. Ao invés disso, ele utiliza o mecanismo de senhas coloridas proposto por SAST.

2. O Sistema de Votação CIVIS e o Protocolo de Registro de Senhas

A versão atual do sistema foi puramente concebida para o ambiente *Web*. Ele foi desenvolvido na linguagem de programação [Python 2022], com auxílio do *framework* [Django 2022]. Além disso, o sistema utiliza a linguagem Javascript [Mozilla 2022] para realização de operações criptográficas localmente no computador do usuário (cliente). A manipulação dos elementos na página *Web* também ocorre via linguagem Javascript (biblioteca jQuery [OpenJS 2022]). Ademais, o sistema utiliza o formato JSON para disponibilização das informações públicas e para a troca de mensagens entre o cliente (votante) e o servidor da aplicação.

Embora o protocolo de ABRTY considere conjuntos formados por mais de uma autoridade, considera-se aqui apenas três autoridades (uma de cada tipo) para simplificação. A autoridade da eleição (AE) é responsável por gerar os parâmetros da votação além de definir informações tais como nome da eleição, disputas, período de votação, etc. A autoridade de registro (registrador) é responsável pela geração das credenciais válidas e também participa da identificação destas durante a apuração. Por fim, a autoridade de apuração (apurador) é responsável pela apuração de votos válidos e pela publicação dos resultados finais.

Uma eleição no CIVIS possui quatro fases, seguindo o protocolo de ABRTY. Na fase de configuração todo o material criptográfico necessário para garantir a segurança do sistema é gerado. Nessa fase, é definido um grupo cíclico de ordem prima, onde o problema de decisão de Diffie-Hellman é difícil. Além disso, o registrador e o apurador geram seus pares de chaves. Mais especificamente, a AE define um grupo cíclico G de ordem p, os geradores do grupo $g_1, g_3, o \in G$, e as demais informações pertinentes a eleição como título, lista de eleitores, disputas e etc. O apurador gera um par de chaves El Gamal $(sk_A, pk_A = g_1^{sk_A})$, onde sk_A é a chave secreta e pk_{Ai} a chave pública. De forma semelhante, o registador gera seu par de chaves El Gamal $(sk_R, pk_R = g_1^{sk_R})$, onde sk_R é a chave secreta e pk_R a chave pública.

A fase de registro é onde os votantes recebem suas credenciais de votação. Na versão original do sistema, a credencial era gerada pelo registrador e entregue diretamente ao votante. A introdução do protocolo de registro prático SAST possibilitou a geração mais segura da credencial (ver abaixo). Nesse protocolo, o votante interage com o registrador para emissão de sua credencial. Ao fim dessa interação, apenas o votante conhece a parte privada de sua credencial (i.e. a senha de votação). Assim, como a senha é gerada sem que o registrador tenha acesso a ela, ele não consegue votar pelo votante.

Na fase de votação, após selecionar seus candidatos, o votante precisa informar a sua senha de votação (i.e. a parte privada da credencial) e também os valores (A, r) representando a parte pública da credencial. A partir dos valores informados, o sistema gera uma tupla contendo o voto e outros dados criptografados, bem como provas de conhecimento zero. Então, essa tupla é publicada em um quadro público representado um voto submetido. Na fase de apuração, o apurador e o registrador utilizam suas chaves secretas para identificar as credenciais verdadeiras, removendo as falsas. Esse processo é realizado sem revelar qualquer *bit* sobre a parte privada da credencial. Por fim, o apurador decifra os votos cujas credenciais foram identificadas como verdadeiras e em seguida apresenta os resultados da eleição.

O Protocolo de Registro de Senhas

Como descrito, o sistema CIVIS utiliza o protocolo de registro prático proposto por SAST [de Sá et al. 2020b]. O protocolo requer primitivas criptográficas como provas de conhecimento zero de conhecimento não interativas (NIZKP). Além disso, ele requer uma função de derivação de chave (PBKDF). O protocolo possui duas fases (configuração e registro) descritas a seguir.

Fase de Configuração. Considerando os parâmetros definidos anteriormente como o grupo cíclico G e os geradores, AE define e publica no quadro público o dicionário de palavras δ. O registrador gera seu par de chaves tal que a chave privada $sk_R = y$ correspondente a chave pública $pk_R = g^y$.

Fase de Registro. Cada votante interage com o registrador a fim de gerar sua credencial legítima de votação. Para isso, o protocolo de registro de credenciais é executado da seguinte forma:

1. O votante seleciona um conjunto de palavras aleatórias $\omega \in \delta$. Então, ele utiliza uma função de derivação de chaves para calcular a parte secreta x de sua credencial, tal que $x = PBKDF(\omega) \mid x \in Z_p$.

2. O votante calcula o valor C_1 tal que $C_1 = g_1 g_3^x$ e NIZKP1 relacionada à C_1. A tupla $(C_1, \text{NIZKP1})$ é enviada ao registrador;

3. O registrador verifica a validade da prova NIZKP1. Caso ela seja inválida, o processo é cancelado. Caso contrário, o processo segue.

4. O registrador gera o número aleatório $r \in Z_p^*$ e calcula o expoente $\frac{1}{y+r}$, utilizando de sua chave privada $sk_R = y$. Ele calcula A tal que $A = C_1{}^{\frac{1}{y+r}}$ e a prova de conhecimento-zero não-interativa $NIZKP2$, relacionada ao cálculo de A. A tupla $(A, r, \text{NIZKP2})$ é enviada ao votante.

5. O votante verifica a validade da prova NIZKP2. Caso seja inválida, o processo é cancelado. Caso contrário, o votante aceita a credencial de votação.

3. A Implementação do Sistema de Registro de Senhas

O sistema de registro de senhas implementa o protocolo de SAST. Ele utiliza as mesmas tecnologias do sistema de votação CIVIS. No entanto, ele foi implementado como um sistema independente do sistema de votação. Dessa forma, em votações que requeiram maiores garantias de segurança, pode-se separar a fase de registro de votantes das outras fases do sistema. A seguir são apresentados a arquitetura do sistema de registro, os aprimoramentos introduzidos a ele e os resultados dos testes de eficácia realizados.

3.1. Arquitetura

O sistema de registro é composto por três módulos: fase de registro, registro de senhas e usuário. O módulo fase de registro é responsável pela configuração, início e encerramento de uma fase de registro. Por sua vez, o módulo registro de senhas é responsável pela execução de uma fase de registro, ou seja, pelo registro de senhas em si. Por fim, o módulo usuário é responsável pelos tipos de usuários presentes no sistema. Esses módulos são apresentados no diagrama da Figura 1. Essa figura também apresenta as entidades existentes no sistema (relativas ao banco de dados) e o relacionamento entre elas.

A entidade *User* é uma classe padrão própria para usuários disponibilizada pelo *framework* Django. Ela é a única entidade presente no módulo Usuário. Destaca-se que tanto o registrador quanto os votantes utilizam da mesma entidade usuário. O sistema diferencia os papeis de usuários em tempo de execução.

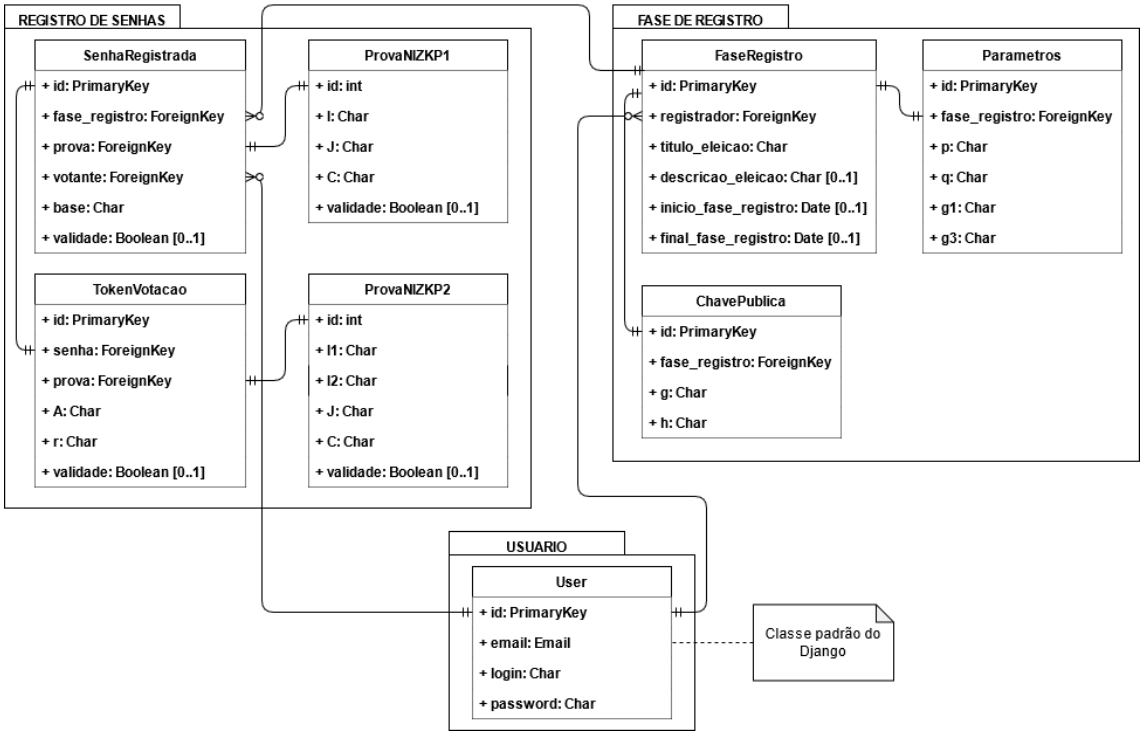

Figura 1. Diagrama de classes das entidades do banco de dados.

O módulo fase de registro possui três entidades: a entidade FaseRegistro, que armazena informações relacionadas à fase de registro; a entidade parâmetros, a qual armazena o conjunto de parâmetros necessários relacionados com a fase de configuração do Protocolo de Registro de Senhas (ver Seção 2); e a entidade ChavePublica, que armazena os valores da chave pública do registrador responsável. Uma fase de registro (FaseRegistro) possui somente um registrador responsável (User), um conjunto de parâmetros (Parametros) e uma chave pública (ChavePublica). Um conjunto de parâmetros (Parametros) e uma chave pública (ChavePublica) são exclusivos de uma única fase de registro (FaseRegistro). Um registrador (User) pode ser responsável por mais de uma fase de registro (FaseRegistro).

No módulo Registro de Senhas existem quatro entidades. A entidade SenhaRegistrada armazena informações a respeito da senha definida pelo votante. A NIZKP relacionada a esta senha é representada na entidade ProvaNIZKP1. A entidade TokenVotacao armazena as informações da tupla (A, r) gerada pelo registrador. O valores (A, r) são públicos. A NIZPK relacionada a este *token* é representada na entidade ProvaNIZKP2. Uma senha registrada (SenhaRegistrada) pertence a somente um votante (User), mas um votante pode ter mais de uma senha registrada. A senha registrada (SenhaRegistrada) possui somente uma NIZPK (ProvaNIZKP1) e gera somente um token de votação (TokenVotacao). Este, por sua vez, possui somente uma NIZPK (ProvaNIZKP2). As provas (ProvaNIZKP1 e ProvaNIZKP2) são exclusivas da senha registrada (SenhaRegistrada) e do *token* de votação (TokenVotacao), respectivamente.

A Fase de Registro

A fase de registro é conduzida pelo registrador. Para isso, ele precisa configurá-la definindo o título da eleição a qual a fase de registro faz parte e, opcionalmente, a descrição da eleição. O título é utilizado como identificador e, portanto, deve ser único entre as demais fases de registro. Após essa definição inicial, a fase de registro é criada, porém ainda não pode ser iniciada.

Para iniciar a fase de registro são necessárias algumas informações que foram geradas previamente durante a fase de configuração do CIVIS, como apresentado na Seção 2. Em particular, os valores (p, q, g_1, o, g_3). Esses valores foram codificados em um arquivo em formato JSON (e.g. informações gerais da eleição). Além disso, é necessário o arquivo em formato JSON contendo a chave pública do registrador. Após a adição desses dois arquivos ao sistema, a fase de registro está pronta para ser iniciada.

Com todas as informações requeridas definidas, o registrador pode programar uma data de início automático para que os votantes possam registrar suas senhas. Todas as informações públicas definidas na fase de registro ficam disponíveis no quadro público. Iniciado o registro de votantes, somente é possível finalizá-lo quando todos os registros em progresso forem finalizados. Isso ocorre tanto pela anulação do registro, quanto pela aceitação da credencial gerada. Não é necessário que todos os votantes iniciem um registro de senha para que a fase seja encerrada.

O Registro de uma Senha

Após a configuração da fase de registro e sua inicialização, os votantes podem registrar-se a fim de obterem suas credenciais de votação. Cada votante gera, em conjunto com o

registrador, uma única e exclusiva senha (a parte privada da credencial) e sua respectiva parte pública (o *token* de votação). Para isso, um processo de registro é estabelecido para cada votante. No sistema, esse processo é dividido em 5 etapas, definidas conforme o protocolo de registro de senhas apresentado na Seção 2. O diagrama de atividades do registro de senhas apresentado na Figura 2 resume estas etapas.

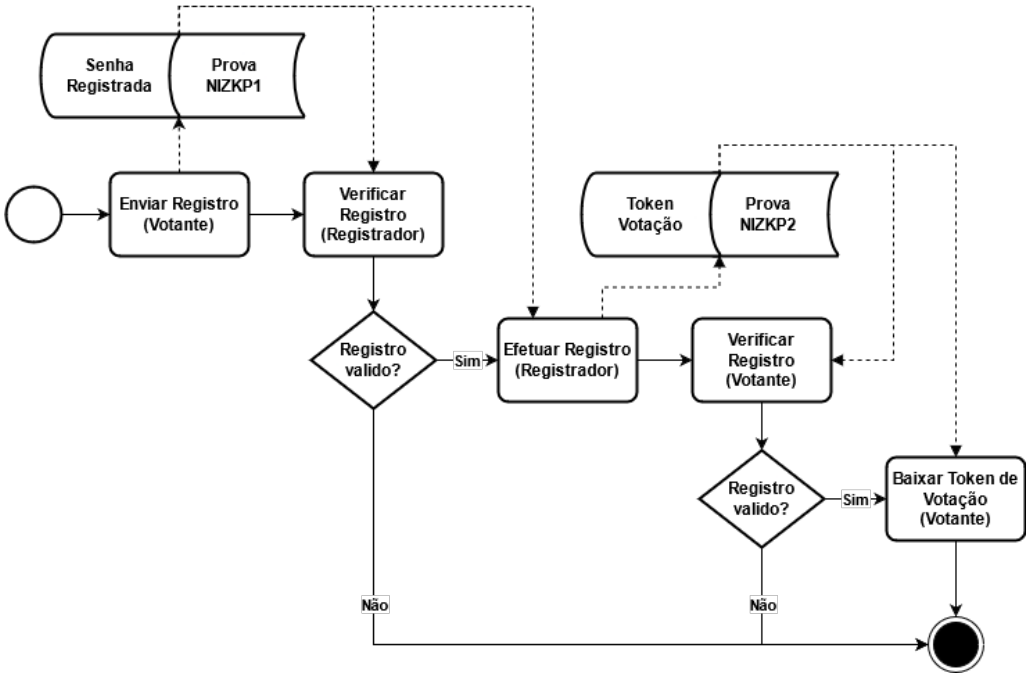

Figura 2. Diagrama de atividades. As linhas contínuas apresentam a sequência de atividades no registro de uma senha. As linhas tracejadas apresentam quais objetos são criados e em quais etapas esses objetos são utilizados.

O votante inicia o registro de sua senha na Etapa **Enviar Registro (Votante)**. Para isso, ele seleciona um conjunto de palavras a partir de um dicionário de palavras dispostas de forma aleatória na página *Web*. O votante obrigatoriamente deve escolher cinco palavras e uma cor para cada palavra. A Figura 3 ilustra a visão do votante ao registrar sua senha.

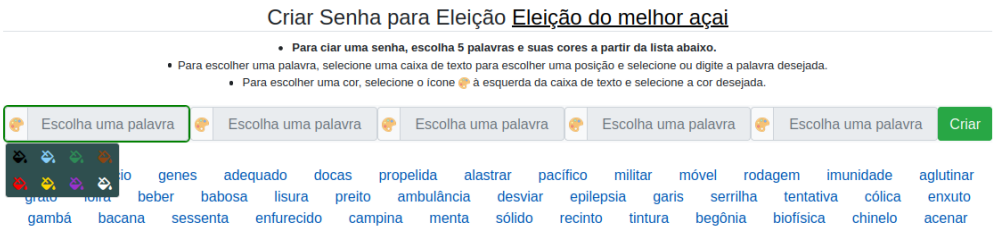

Figura 3. A criação de uma senha.

Como definido no protocolo de registro de senhas, o algoritmo PBKDF recebe como entrada a senha definida pelo votante. Essa senha é concatenada da seguinte forma: palavra1||cor1||palavra2||cor2||...||palavra5||cor5. Em seguida, o computador do votante calcula C_1 e a prova NIZKP1 via JavaScript, codifica esses valores em um arquivo JSON e retorna esse arquivo ao sistema (registrador).

Na etapa **Verificar Registro (Registrador)**, o registrador obtém o arquivo JSON enviado pelo votante e verifica a prova NIZKP1. Caso a prova seja verdadeira, o processo avança para a próxima etapa. Caso contrário, o registro é anulado e o votante precisa iniciar um novo processo de registro. Dando prosseguimento ao registro da senha, o registrador executa a etapa **Efetuar Registro (Registrador)**. Nessa etapa, ele calcula a parte pública da credencial, chamada de *token* de votação. Como resultado obtém-se a tupla $(A, r, \text{NIZKP2})$ que é codificada em um arquivo JSON e enviada ao votante.

Em seguida, o votante executa a etapa **Verificar Registro (Votante)**. Nesta etapa, o votante verifica a validade da prova NIZKP2. Caso essa prova seja verdadeira, ele aceita o registro e o *token* de votação gerado pelo registrador. Caso contrário, o processo de registro é anulado e o votante precisa iniciar um novo processo. Por fim, na etapa **Baixar Token de Votação (Votante)**, o votante obtém o *token* de votação que contém os valores (A, r). Esse *token* representa a parte pública da credencial e é necessário para emissão do voto durante a fase de votação.

O Encerramento da Fase de Registro

Ao final da fase de registro, o registrador deve encerrá-la. Para isso, é necessário que todos os registros em progresso estejam finalizados. A fase de registro pode ser encerrada mesmo que nem todos os votantes autorizados tenham iniciado os seus registros. O encerramento é imediato e, a partir dele, não é permitido a nenhum votante iniciar um novo registro de senha. Com a finalização da fase de registro, o sistema gera um arquivo JSON com informações sobre os registros realizados. Esse arquivo contém todos os *tokens* de votação válidos que foram gerados durante o período de registro.

As Modificações do Sistema CIVIS

Embora o sistema de registro de senhas seja independente do restante do sistema CIVIS, ele foi concebido para ser utilizado em conjunto com esse sistema. Para funcionar em conjunto com o novo registro, o CIVIS recebeu modificações em suas fases de registro e de votação como descrito a seguir.

Ao final da fase de registro, os votantes estão registrados e possuem suas credenciais de votação. Os *tokens* de votação gerados devem ser publicados no quadro público da eleição para fins de auditoria. Além disso, caso algum votante perca o seu *token*, ele poderá obtê-lo a partir do quadro público. A fim de publicar essas informações, o CIVIS recebe o arquivo JSON gerado ao final da fase de registro de votantes. Esse arquivo contém os *tokens* de votação dos votantes registrados.

Além das modificações necessárias para publicar os *tokens* de votação, o novo estilo de credencial resultou em modificações na fase de votação do sistema. Cada votante registra sua senha de votação e recebe um *token*. Ambos devem ser utilizados ao votar. Dessa forma, durante a fase de votação, o votante realiza o seguinte: ele informa sua opção de voto, a sua senha (composta por cores e palavras) e por último insere o arquivo contendo o *token* de votação.

Limitações

O sistema introduzido aqui abstrai mecanismos de segurança necessários em cenários reais de votação. Por exemplo, o uso de mecanismos para autenticação do código das

páginas *Web*. Mecanismo desse tipo são importantes para garantir que o código executado no sistema é o mesmo disponibilizado pela comissão eleitoral. Do contrário, não há como garantir a autenticidade do código carregado no navegador do votante já que o mesmo pode ter sido substituído terceiros.

Uma outra limitação do sistema está relacionada a resistência a computadores quânticos. Assim como o CIVIS, o sistema de registro tem como base um protocolo criptográfico para esse fim. Esse protocolo utiliza primitivas criptográficas concebidas a partir de problemas computacionalmente seguros como o problema do logaritmo discreto. Dessa forma, ambos os sistemas não oferecem resistência a computadores quânticos.

3.2. Outros Aprimoramentos

O sistema CIVIS foi concebido considerando uma fase de registro restrita e livre de adversários. Ele segue a suposição introduzida por JCJ e também seguida pelo protocolo de ABRTY. Ou seja, adversários podem coagir votantes antes do registro, mas não durante esse processo. Para satisfazer essa suposição, é necessário que cada votante receba a sua credencial de votação presencialmente e em um local restrito, como uma cabine protegida de terceiros. Além disso, não deve ser possível salvar qualquer dado que possa comprovar a credencial legítima.

Nas primeiras versões do CIVIS, tal como a proposta de JCJ, o registrador gerava a credencial e a entregava diretamente ao votante. Dessa forma, o registrador precisava ser confiável de forma a não revelar qualquer informação sobre as credenciais geradas. Para reduzir a confiança no registrador, SAST [de Sá et al. 2020b] introduziu o protocolo de registro de senhas. Ou seja, o registrador gera a credencial em conjunto com o votante. A credencial é composta pelo *token* (i.e. parte pública) e pela senha (i.e. parte privada), mas a senha é conhecida exclusivamente pelo votante. Conforme apresentado, tal protocolo possibilitou a adição de melhorias ao CIVIS relativas ao registro de credenciais e a fase de votação. No entanto, a propriedade de resistência à coação ainda depende da emissão das credenciais presencialmente. Em termos práticos, a visita a um local apropriado para isso limita a utilização do sistema.

Visando ampliar o uso do sistema, até então limitado pelo registro presencial das credenciais de votação, possibilitou-se a realização do registro remoto de credenciais. No entanto, esse registro facilita a atuação de adversários, comprometendo a resistência à coação. Credenciais legítimas (i.e. senhas) podem ser facilmente obtidas, por exemplo, observando votantes durante o processo de registro. Esse é um problema comum e inerente a sistemas que não possuem essa propriedade (i.e. resistência à coação) como o Helios [Adida 2008] ou que permitam o envio de senhas por e-mail.

Ao relaxar a propriedade de resistência à coação possibilitando o registro remoto de credenciais, o sistema torna-se mais prático. Uma das melhorias introduzidas para isso é a autenticação prévia de votantes aptos a se registrarem. Ela ocorre antes dos votantes emitirem suas credencias. Dessa forma, após se autenticarem, os votantes têm acesso ao sistema de registro e podem emitir suas credenciais como descrito na Seção 3.1. Essa autenticação pode ser realizada a partir de um cadastro prévio de votantes onde a senha de acesso ao sistema é enviada por e-mail. Também é possível utilizar um serviço de gestão de identidades, como o CAFe da RNP [RNP 2021].

Um outro aprimoramento adicionado ao CIVIS foi a possibilidade de utilizá-lo

por meio de um aplicativo para dispositivos móveis. O sistema anterior permitia apenas o acesso via navegadores *Web*. Isso o tornava mais suscetível a ataques inerentes a esse ambiente, como ataques de phishing. Para minimizar tais riscos e também oferecer mais comodidade aos votantes, o uso de um aplicativo móvel é recomendado. Dessa forma, o CIVIS foi incrementado com um aplicativo que possibilita votar e registrar a credencial de votação. Tal aplicativo foi concebido por meio da plataforma Apache Cordova. Essa plataforma possibilita a criação aplicativos para dispositivos móveis a partir aplicações baseadas em tecnologias *Web* como HTML e Javascript.

A adição do aplicativo para dispositivos móveis ao CIVIS possibilitou a introdução de outras ideias ao sistema. A fim de facilitar a geração de credenciais remotamente, a fase de registro foi adaptada para possibilitar a utilização de dois dispositivos: disp1 e disp2. Um deles é utilizado para acessar o sistema via *Web* (disp1) e o outro executa o aplicativo móvel (disp2). Dessa forma, para registrar sua credencial, o votante realiza os seguintes passos:

1. O votante acessa o sistema *Web* via disp1;
2. O votante define sua senha (correspondente ao valor x da credencial) e o registrador gera os valores A, r a partir dela;
3. O registrador codifica o arquivo JSON contendo os valores A, r em *QR-Code* e apresenta ao votante por meio de uma página *Web*;
4. Utilizando o aplicativo instalado previamente no disp2, o votante realiza a leitura do *QR-Code*;
5. O disp2 armazena o arquivo JSON (i.e. a parte pública da credencial) obtido via *QR-Code*.

Após o registro de sua credencial utilizando os dois dispositivos, o votante utiliza apenas o disp2 (i.e. o dispositivo móvel que contém o aplicativo e o arquivo JSON) para votar na fase de votação. Para isso, o votante realiza os seguintes passos:

1. O votante seleciona o seu candidato através do aplicativo;
2. O votante informa a sua senha;
3. A partir do arquivo JSON armazenado e relativo a senha, o aplicativo prepara a tupla contendo o voto encriptado;
4. O votante confirma seu voto;
5. O aplicativo envia a tupla correspondente para o quadro público.

A Figura 4 ilustra as fases de registro e votação utilizando os dispositivos.

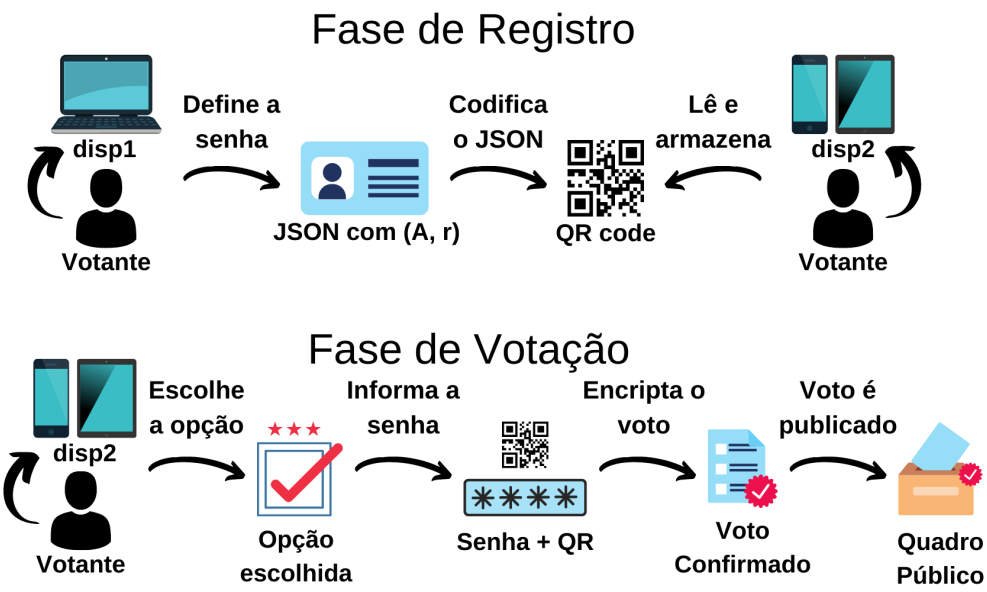

Figura 4. Ilustração do registro de votantes e da fase de votação via dispositivos.

3.3. Verificando a Eficácia do Sistema de Registro

De forma a verificar a eficácia do sistema registro de credenciais, foram realizados alguns testes qualitativos a partir experiência do usuário. Esses testes visaram verificar a facilidade de uso do sistema para a emissão das senhas. Devido a limitação de espaço, a seguir são apresentados apenas os resultados relativos ao tempo de conclusão do registro, a utilização de critérios para escolha da senha e a memorização da senha registrada.

A metodologia utilizada nos testes baseou-se na observação e coleta de dados durante a interação dos participantes com o sistema de registro. Para isso, utilizou-se métricas de usabilidade estabelecidas na ISO/IEC$9126 - 4$ tais como efetividade, eficiência e satisfação. A efetividade refere-se a acurácia e completude com que os usuários atingem os objetivos. A eficiência refere-se aos recursos despendidos em relação à acurácia e completude com que os usuários atingem os objetivos. A satisfação refere-se ao conforto e a aceitabilidade de uso. A coleta de dados ocorreu por meio do questionário pré-teste, da sessão de observação e do questionário pós-teste.

De forma a coletar dados mais precisos, optou-se pela realização dos testes presencialmente. Para isso, foi disponibilizado um computador com acesso ao sistema de registro. Os testes consistiram em utilizar o sistema de registro para emissão de uma credencial legítima, ou seja, uma senha colorida e sua parte pública correspondente. Os participantes foram orientados a utilizar o sistema para criar uma senha colorida composta por 5 palavras e 5 cores. A senha deveria ser memorizada. Cada participante foi orientado a realizar a tarefa proposta de forma independente, mas sendo possível emitir opiniões ou consultar o moderador para sanar eventuais dúvidas.

Os testes foram realizados no ambiente acadêmico e tiveram a participação de 15 voluntários. Eles foram selecionados aleatoriamente e possuíam diferentes áreas de atuação. O único critério de exclusão adotado para seleção foi a idade que deveria ser

maior de 16 anos. Essa é a idade mínima exigida pelo processo eleitoral brasileiro. Dos participantes selecionados, $93,3\%$ eram graduandos e $6,7\%$ professores. Destes, $66,7\%$ declararam ter um bom ou muito bom conhecimento tecnológico, enquanto que $33,3\%$ declararam ter um conhecimento tecnológico médio ou ruim. Em relação à idade, $26,7\%$ estão entre 16 e 19 anos, 60% entre 20 anos e 29 anos e o restante entre 30 e 39 anos.

Considerando o tempo de conclusão do registro, os participantes levaram $4,6$ minutos em média para concluírem o processo de registro, sendo que o desvio padrão foi de $1,67$ minutos. O menor tempo de conclusão foi de 2 minutos e o maior foi de 8 minutos. Considera-se esse tempo satisfatório tendo em vista que são necessários 5 etapas para efetuar o registro (ver Seções 2 e 3.1). Além disso, ressalta-se que na etapa *Verificar Registro* os votantes devem aguardar a verificação da prova pelo registrador para então prosseguirem. Após registrarem suas senhas, os participantes foram questionados sobre a utilização ou não de critérios próprios para seleção de suas senhas. 4 participantes informaram que adotaram palavras que lhes eram cotidianas ou formaram um padrão para relacionar as palavras e cores. Os outros participantes escolheram palavras e cores aleatórias sem se preocuparem com a necessidade de relembrá-las adiante.

Um outro questionamento adotado foi relativo a recordação da senha registrada. Tal recordação é importante pois a utilização de uma senha incorreta resulta na anulação do voto na apuração. Dentre todos os participantes, 4 conseguiram relembrar suas senhas com 100% de acurácia, 2 participantes conseguiram relembrar entre 75% e 90% de suas senhas, 3 conseguiram relembrar entre 50% e 75% de suas senhas e 6 participantes conseguiram relembrar até 25% de suas senhas. O número baixo de acurácia provavelmente decorreu do fato de alguns votantes utilizarem senhas sem nenhum critério de escolha. Apenas os participantes que consideraram critérios próprios conseguiram relembrar suas senhas. Com relação a facilidade de memorização da senhas, 9 participantes declaram que elas são de fácil memorização, 4 declararam que o processo como confuso, complicado e complexo, e os outros não responderam.

4. Discussão

Uma das propostas aqui apresentadas considera um cenário onde os votantes podem emitir suas credenciais de qualquer lugar conectado à Internet. Consequentemente, não há como eles resistirem a ataques coercivos se esse processo for acompanhado por adversários. Embora isso resulta no relaxamento da propriedade de resistência à coação, a manutenção do processo de registro tal como proposto facilita o seu uso em diferentes cenários. Ou seja, como o processo é o mesmo para votações que exigem ou não a propriedade de resistência à coação, não é necessário adaptar o sistema e treinar votantes para utilizar tais adaptações. O mesmo sistema é utilizado em ambos os cenários, optando-se apenas pelo registro remoto ou presencial. Além disso, possibilitar o uso do sistema em votações mais simples implica em usuários melhor preparados para utilizá-lo em votações que exigem maiores garantias de segurança.

As fases de registro e votação podem ser ainda mais simplificadas. Por exemplo, a codificação da senha (secreta) diretamente no *QR-Code* relativo a parte pública da credencial. Dessa forma, ao votar, o votante informa somente o *QR-Code* e o sistema extrai ambas as partes da credencial e realiza o restante do processo. Todavia, tal mudança altera o sistema proposto, o que pretende-se evitar para manter uniforme o uso em diferentes

cenários. As senhas utilizadas no CIVIS são um outro aspecto que merece atenção. No sistema, o usuário define sua senha de votação e a parte pública da credencial é calculada a partir dela. A definição da senha pelo votante possibilita que ele escolha senhas que possam ser lembradas durante a votação. Todavia, é necessário impedir o uso de senhas triviais como palavras que nomeiam as cores escolhidas.

O mecanismo de senhas utilizado torna o sistema mais prático, mas ele possui uma desvantagem inerente. Caso o votante informe sua senha válida incorretamente (e.g. por engano ou desatenção), o voto correspondente será considerado falso e assim ele será excluído dos resultados finais. O CIVIS não impede totalmente esse problema. No entanto, ele dispõe de mecanismos para reduzir erros desse tipo. A senha é selecionada a partir de um dicionário de palavras e outro de cores tal como proposto por [de Sá et al. 2020a]. Apenas palavras e cores definidas nesses dicionários são aceitas como válidas. Ao informar uma senha que não esteja nesses dicionários, ela é desconsiderada e o votante deve informar uma nova senha. Essa limitação de escolha por meio dos dicionários impede o uso de qualquer palavra ou cor. Além disso, o sistema também apresenta a lista de palavras correspondentes enquanto o votante informa a sequência de letras que formam a palavra. Assim, ao invés de digitar a palavra por completo, apenas as iniciais podem ser escritas e a palavra selecionada.

Como descrito, o sistema abstrai o uso de um mecanismo para autenticação do código da página *Web*. Mecanismos para esse fim podem ser adicionados como assinatura de código. O uso desse mecanismo, todavia, não impede totalmente ataques em que o código do sistema (e.g. o código que criptografa as opções de voto do votantes) é substituído maliciosamente. Como a maioria dos votantes (principalmente os leigos) certamente desconhecem procedimentos necessários para correta verificação do código utilizado, códigos maliciosos podem ser adicionados sem que sejam identificados por esses usuários. Infelizmente, garantir a autenticidade de código de forma fácil para usuários leigos ainda é um problema em aberto em qualquer aplicação.

5. Conclusão e Trabalhos Futuros

Este trabalho detalhou a implementação de um sistema de registro seguro que não foi considerada em um trabalho anterior. Além disso, ele introduziu aprimoramentos a esse sistema e apresentou os resultados dos primeiros testes de avaliação de eficácia. Adicionalmente, ele discutiu alguns aspectos relativos as propostas apresentadas.

O sistema de registro visa tornar prático o uso do CIVIS em eleições reais. O registro presencial impediria a utilização do CIVIS em cenários como o da pandemia atual. Dessa forma, a fim tornar possível a utilização do sistema em cenários desse tipo, foram propostas melhorias que permitem realizar o registro remoto de votantes. Todavia, nesse caso, não há como garantir a propriedade de resistência à coação.

Os testes realizados avaliaram a efetividade do sistema de registro. Embora o tempo de registro de senhas tenha sido satisfatório, infelizmente apenas alguns votantes conseguiram relembrar totalmente suas senhas. Esse fato requer uma investigação mais detalhada e é deixado como trabalho futuro. Uma abordagem que poderia ser utilizada em testes futuros é instruir previamente os participantes a definirem critérios que facilitem a recordação de suas senhas.

Referências

[Adida 2008] Adida, B. (2008). Helios: Web-based open-audit voting. In van Oorschot, P. C., editor, *Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA*, pages 335–348. USENIX Association.

[Araujo et al. 2018] Araujo, R., Neto, A., and Traoré, J. (2018). Civis-a coercion-resistant election system. In *Anais do XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 29–42. SBC.

[de Sá et al. 2020a] de Sá, M. O., Araujo, R., Sobrinho, A. C. L., Neto, A. S., Maximino, G. S., and Traoré, J. (2020a). How colored passwords can improve the usability of coercion-resistant internet voting systems. In *Proceedings of the 19th Brazilian Symposium on Human Factors in Computing Systems*, pages 1–6.

[de Sá et al. 2020b] de Sá, M. O., Araujo, R., Sobrinho, A. C. L., and Traoré, J. (2020b). Registro prático aplicado a um sistema de votação resistente à coerção. In *SBSeg-Main Track*. SBC.

[de Sá et al. 2020] de Sá, M. O. L., Araújo, R., Sobrinho, A. C. L., Neto, A. S., Maximino, G. S., and Traoré, J. (2020). How colored passwords can improve the usability of coercion-resistant internet voting systems. In Santos, C. Q., Villela, M. L. B., Gasparini, I., and Conte, T. U., editors, *IHC '20: XIX Brazilian Symposium on Human Factors in Computing Systems, Online Event / Diamantina, Brazil, October 26-30, 2020*, pages 49:1–49:6. ACM.

[Django 2022] Django, D. S. F. (2022). Django - the web framework for perfectionists with deadlines. `https://www.djangoproject.com/`. Acessado em: Junho/2022.

[Estaji et al. 2020] Estaji, E., Haines, T., Gjøsteen, K., Rønne, P. B., Ryan, P. Y. A., and Soroush, N. (2020). Revisiting practical and usable coercion-resistant remote e-voting. In Krimmer, R., Volkamer, M., Beckert, B., Küsters, R., Kulyk, O., Duenas-Cid, D., and Solvak, M., editors, *Electronic Voting - 5th International Joint Conference, E-Vote-ID 2020, Bregenz, Austria, October 6-9, 2020, Proceedings*, volume 12455 of *Lecture Notes in Computer Science*, pages 50–66. Springer.

[Juels et al. 2005] Juels, A., Catalano, D., and Jakobsson, M. (2005). Coercion-resistant electronic elections. In Atluri, V., di Vimercati, S. D. C., and Dingledine, R., editors, *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, WPES 2005, Alexandria, VA, USA, November 7, 2005*, pages 61–70. ACM.

[Mozilla 2022] Mozilla (2022). Mdn web docs - javascript. `https://developer.mozilla.org/en-US/docs/Web/JavaScript`. Acessado em: Junho/2022.

[Neumann and Volkamer 2012] Neumann, S. and Volkamer, M. (2012). Civitas and the real world: Problems and solutions from a practical point of view. In *Seventh International Conference on Availability, Reliability and Security, Prague, ARES 2012, Czech Republic, August 20-24, 2012*, pages 180–185. IEEE Computer Society.

[OpenJS 2022] OpenJS, O. F. (2022). jQuery - write less, do more. `https://jquery.com/`. Acessado em: Junho/2022.

[Python 2022] Python, P. S. F. (2022). Python language reference. `https://www.python.org/`. Acessado em: Junho/2022.

[RNP 2021] RNP (2021). Federação CAFe. `https://www.rnp.br/servicos/alunos-e-professores/identidade-e-seguranca/cafe`. Acessado em: Julho/2021.