Aprimorando a Segurança do Sistema de Votação CIVIS através da Geração Distribuída de Credenciais

Alberto Sobrinho[1], **Roberto Araújo**[1]

[1]Faculdade de Computação – Universidade Federal do Pará (UFPA)
Belém – PA – Brasil

alberto.sobrinho@icen.ufpa.br, rsa@ufpa.br

Abstract. *The CIVIS Internet voting system enables voters to react to coercive attacks. Voters receive legitimate voting credentials and have to generate false credentials when coerced. The current version of the system relies on a single authority responsible for generating and delivering legitimate credentials. As a result, the system requires a trusted authority to ensure security. In order to improve the security of the system, this work proposes modifications to the CIVIS system in order to allow the distributed generation of voting credentials.*

Resumo. *O sistema de votação via Internet CIVIS possibilita aos votantes reagirem a ataque coercivos. Votantes recebem credenciais de votação legítimas e devem gerar credenciais falsas quando coagidos. A versão atual do sistema possui uma única autoridade responsável por gerar e entregar credenciais legítimas aos votantes. Como resultado, o sistema requer uma autoridade confiável para garantir a segurança do processo. A fim de aprimorar a segurança do sistema, este trabalho propõem modificações no sistema CIVIS a fim de possibilitar a geração distribuída de credenciais de votação.*

1. Introdução

Modernos protocolos de votação via *Internet* mitigam ataques coercivos através do uso de credenciais de votação. Em outras palavras, o votante recebe uma credencial legítima em segredo e a utiliza para votar posteriormente. Ao ser coagido, o votante deve utilizar uma credencial falsa. O sistema de votação via *Internet* CIVIS [Araujo et al. 2018] tem como base um protocolo resistente à ataques coercivos que utiliza essa ideia. Na versão atual do sistema, no entanto, essa credencial é emitida por uma única autoridade, diferindo do proposto no protocolo. Como resultado, essa autoridade deve ser confiável. A fim de se adequar ao protocolo e aprimorar a segurança do sistema, este trabalho apresenta modificações no sistema CIVIS as quais possibilitam a geração distribuída de credenciais.

2. O Sistema de Votação via *Internet* CIVIS

O CIVIS é um sistema de votação via *Internet* resistente à coerção, o qual implementa o protocolo criptográfico para eleições via *Internet* proposto por [Araújo and Traoré 2013]. Ele foi desenvolvido na linguagem Python [Van Rossum and Drake 2003], com auxílio do framework *web* Django [Holovaty and Kaplan-Moss 2009] e com ferramentas criptográficos implementados na linguagem JavaScript [Flanagan 2006]. Uma eleição no sistema possui as seguintes fases: configuração, onde ocorre a definição do material criptográfico e de outros parâmetros iniciais da eleição; registro, onde são geradas e entregues

aos votantes as credenciais de votação; votação, onde os votos são emitidos utilizando as credenciais; e apuração, onde os votos legítimos são identificados e apurados sem revelar qualquer bit sobre o mesmo. Na versão atual do sistema, a geração e envio de credenciais é realizada por uma única autoridade. A credencial no CIVIS possui uma estrutura composta por $\left(A = (g_1 g_3^x)^{\frac{1}{y+r}}, r, x\right)$, onde: $g_1, g_3 \in Z_p^*$ são geradores aleatórios provenientes dos parâmetros iniciais da votação; $r, x \in Z_q^*$ são números gerados aleatoriamente; e y é a chave privada da autoridade responsável pela geração das credenciais. Diferente de outras soluções da literatura, onde as credenciais são números aleatórios, as credenciais utilizadas pelo protocolo de Araújo et al. possuem uma estrutura matemática. Dessa forma, sua verificação na fase de apuração se torna mais eficiente (linear *versus* quadrática). Porém, a comparação de geração de credenciais com estruturas diferentes torna-se difícil.

3. O Protocolo para Geração Distribuída de Credenciais

É necessário um protocolo que garanta a segurança de todo o processo de geração distribuída de credenciais no CIVIS. O protocolo de assinaturas digitais curtas limiar proposto por [Wang et al. 2005] pode ser adaptado para geração dessas credenciais. O protocolo possui três fases: geração distribuída do par de chaves de comprometimento, onde os participantes geram um par de chaves de comprometimento, sendo h_2 a chave pública; a geração distribuída do par de chaves de assinatura, onde são gerados os dois pares de chaves da assinatura, sendo x e y os segredos compartilhados; e geração da assinatura digital limiar, onde são gerados de forma distribuída o segredo aleatório r e o valor aleatório a, e calculados os valores $b = x + m + ry \ (mod\ q)$, onde m é uma mensagem, e $c = a \cdot b \ (mod\ q)$. A assinatura gerada é estruturada como: $\sigma = \left((g^a)^{c^{-1}}, r\right)$.

De forma a utilizar o protocolo de [Wang et al. 2005] para gerar credenciais no CIVIS, uma adaptação desse protocolo é proposta por [Sá 2018]. Nessa adaptação, a fase de geração de assinatura digital limiar corresponde a geração distribuída de credencial e o protocolo passa a considerar um grupo de inteiros, diferente do grupo bilinear proposto por [Wang et al. 2005]. A chave privada de assinatura x passa a ser um segredo aleatório gerado de forma distribuída na fase de geração distribuída de credencial. O valor b é calculado tal que $b = r + y \ (mod\ q)$ e o valor $g_1 g_3^x$ é utilizado como base durante a geração distribuída do valor aleatório a. A credencial gerada ao final possui a seguinte estrutura: $\left(A = (g_1 g_3^x)^{ac^{-1}} = (g_1 g_3^x)^{\frac{1}{y+r}}, r, x\right)$.

4. A Geração Distribuída de Credenciais no Sistema CIVIS

As modificações desenvolvidas tem por base funcionalidades e estruturas implementadas no protótipo proposto por [Silva Neto and Araújo 2017], o qual utiliza uma versão limiar do algoritmo de criptografia assimétrica El Gamal. Cada autoridade de apuração gera um par chaves assimétrica para comunicação entre elas. O grupo limiar também gera a chave de comprometimento necessária para realizarem comprometimentos de Pedersen. Nas alterações aqui propostas, considera-se que as autoridades de registro utilizam desse mesmo material criptográfico necessário ao comprometimento. Dessa forma, não é preciso gerar a chave de comprometimento necessária ao protocolo de [Wang et al. 2005].

As fases restantes do protocolo foram divididas em seis etapas: geração distribuída do par de chaves das autoridades de registro, onde y é um segredo compartilhado entre es-

sas autoridades, representando a chave privada; geração distribuída do segredo aleatório r; geração distribuída do segredo aleatório x; geração distribuída do valor aleatório a; cálculo do valor b; e cálculo do valor c. Como apresentado no diagrama de atividades da Figura 1, cada etapa tem como resultado um valor conhecido apenas em parte por cada autoridade. Por exemplo, cada autoridade conhece apenas sua parte do segredo y. As autoridades utilizam suas partes dos segredos no decorrer processo. Ademais, são gerados polinômios de comprometimento em todas as etapas de geração dos valores. Estruturas já existentes foram adaptadas e novas estruturas criadas no banco de dados de modo a armazenar todas as informações geradas, distinguindo-se as etapas. Por exemplo, a estrutura da autoridade de registro foi alterada para armazenar os polinômios de comprometimento gerados durante o processo, bem como em qual etapa da geração a autoridade se encontra.

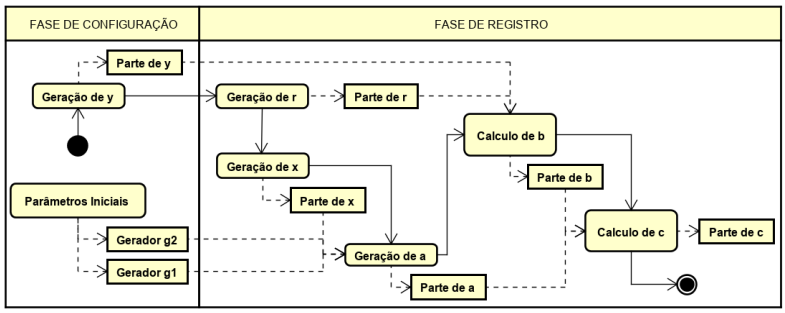

Figura 1. Diagrama de atividade para geração distribuída de credencial. Etapas de geração são distribuídas e etapas de cálculo são individuais.

Para acomodar as etapas descritas acima, também foram necessárias alterações nas páginas *web* existentes. A Figura 2 apresenta os passos exibidos durante cada etapa de geração. Conforme a figura, no primeiro passo ocorre a geração dos pares de chaves criptográficos, as quais são utilizadas apenas para comunicação entre as autoridades e cada uma delas possui um único par. No segundo passo, cada autoridade gera os segredos $s, r \in Z_q^*$ aleatórios e os compartilha na forma de frações de segredo, criptografadas com a chave pública da autoridade de destino. Durante esse passo, cada autoridade também calcula seu polinômio de comprometimento e polinômio público.

Tabela de Autoridades

Autoridade	Chave Pública	Comprometimento / Pol. Público	Comprometimento Verificado	Parte da Chave Pública	Pol. Público Verificado
Autoridade 1	JSON	-	Não	-	Não
Autoridade 2	JSON	-	Não	-	Não

Figura 2. Visualização no sistema da sequência de passos e tabela contendo informações públicas sobre a geração distribuída de credencial.

No terceiro passo, cada autoridade decripta e verifica as frações recebidas com base no polinômio de comprometimento da autoridade remetente, publicando o resultado. Logo após, no quarto passo, as autoridades aprovadas na verificação anterior decriptam

as frações de segredo recebidas e calculam suas duas partes de segredo, respectivas aos segredos s e r. Nesse passo, também é calculada e publicada, por cada autoridade, uma informação para verificação do polinômio de comprometimento do grupo. Por fim, no quinto passo, cada autoridade decripta as frações do segredo s recebidas e as verifica com base no polinômio público do remetente. Durante esse passo, é calculado e publicado, por cada autoridade, uma informação de verificação do polinômio público do grupo.

Ao término das etapas de geração, cada autoridade utiliza suas partes de segredo obtidas nas etapas anteriores para cálculo das partes dos valores b e c. No cálculo da parte do valor b, cada autoridade insere no sistema sua parte do segredo compartilhado y e parte do segredo aleatório r. No cálculo da parte do valor c, cada autoridade insere no sistema sua parte do valor b e sua parte do valor aleatório a. As autoridades que desejam participar da geração distribuída das credenciais inserem no sistema suas partes do valor c. Após uma quantidade mínima de autoridades participarem, o valor c é recuperado e a credencial é gerada. Todas as informações públicas do processo de geração de credenciais são publicadas no Quadro Público da eleição, permitindo posterior verificação do processo.

5. Considerações Finais

As modificações do sistema CIVIS apresentadas neste trabalho tiveram como objetivo adequar o CIVIS ao protocolo criptográfico para eleições via *Internet* proposto por Araujo et al. Portanto, elas possibilitam a geração distribuída de credenciais de votação. Como este é um trabalho em andamento, os próximos passos objetivam implementar a fase do protocolo de Wang et al. em que ocorre o *back-up* das partes dos valores *a*, *b* e *c* e desenvolver e integrar a identificação das credenciais de votação durante a fase de apuração. Como as modificações aqui propostas fazem parte do sistema CIVIS, ela será disponibilizada ao público juntamente com o sistema na forma de software livre em breve.

Referências

Araujo, R., Silva Neto, A., and Traoré, J. (2018). CIVIS-A coercion-resistant election system. In *SBSeg 2018*, pages 29–42. SBC.

Araújo, R. and Traoré, J. (2013). A practical coercion resistant voting scheme revisited. In *International Conference on E-Voting and Identity*, pages 193–209. Springer.

Flanagan, D. (2006). *JavaScript: the definitive guide*. "O'Reilly Media, Inc.".

Holovaty, A. and Kaplan-Moss, J. (2009). *The definitive guide to Django: Web development done right*. Apress.

Silva Neto, A. A. and Araújo, R. (2017). A integração do criptossistema el gamal limiar ao sistema de votação via internet CIVIS. In *SBSeg-WTICG*, pages 697–706. SBC.

Sá, M. O. L. (2018). A implementação de um protocolo criptográfico para geração distribuída de credenciais no sistema Civis. Monografia de Trabalho de Conclusão de Curso em Ciência da Computação, Universidade Federal do Pará, Belém, Brazil.

Van Rossum, G. and Drake, F. L. (2003). *Python language reference manual*. Network Theory United Kingdom.

Wang, H., Zhang, Y., and Feng, D. (2005). Short threshold signature schemes without random oracles. In *International Conference on Cryptology in India*, pages 297–310. Springer.