SOUTH AMERICAN JOURNAL
of Basic Education, Technical and Technological

SAJEBTT, Rio Branco, UFAC
v.8 n.2 (2021): Edição jan/abr.
ISSN: 2446-4821

(IN)SEGURANÇA DO SISTEMA DE VOTAÇÃO ELETRÔNICA IMPLANTADO NO INSTITUTO FEDERAL DE RONDÔNIA

(IN)SECURITY OF THE ELECTRONIC VOTING SYSTEM IMPLEMENTED AT FEDERAL INSTITUTE OF RONDONIA

Ewerton Rodrigues Andrade [1*]
1. Departamento Acadêmico de Ciência da Computação
Fundação Universidade Federal de Rondônia

* Autor correspondente: e-mail ewerton.andrade@unir.br

RESUMO

Este trabalho apresenta uma análise de segurança do sistema de votação implantado no Instituto Federal de Educação, Ciência e Tecnologia de Rondônia, realizada de maneira independente e somente com motivação acadêmica. Durante esta análise, foram detectadas vulnerabilidades e fragilidades no sistema de votação e no projeto de implantação do sistema. Em razão disto, este trabalho apresenta cenários onde estas vulnerabilidades e fragilidades podem ser exploradas com o intuito de promover a fraude eleitoral ou, eventualmente, outros crimes de responsabilidade. Além disso, são apontadas fragilidades no projeto de implantação do sistema que também comprometem a segurança do processo eleitoral como um todo. Em particular, os principais problemas de segurança encontrados foram: Autenticação insegura, Falha na verificabilidade do voto, Utilização de algoritmos obsoletos e inseguros, Inverificabilidade do código-fonte em produção, Formulação equivocada do modelo de atacante, Possibilidade de ataques utilizando engenharia social, e Proteção inadequada do sigilo do voto.
Palavras-chave: Votação eletrônica; análise de segurança; IFRO.

ABSTRACT

In this work we present an independent security analysis of the voting system implemented at Federal Institute of Rondonia. During our analysis, vulnerabilities and flaws were detected in the voting software and system deployment. As a result, this work presents scenarios where these problems can be explored in order to promote electoral fraud or, possibly, other responsibility crimes. Additionally, implementation flaws are identified because they also compromise the security of the electoral process. In particular, the main design and/or implementation problems detected in the security mechanisms of the voting software were: Unsafe authentication, Unsafe verifiability of the ballot, Obsolete cryptographic algorithms, Unverifiability of source code in production, Inappropriate attacker model, The possibility of attacks using social engineering, and Inadequate protection of ballot secrecy.
Key words: Electronic voting; security analysis; IFRO.

SAJEBTT, Rio Branco, UFAC
v.8 n.2 (2021): Edição jan/abr.
ISSN: 2446-4821

1 INTRODUÇÃO

Nos últimos anos, o Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO) intensificou sua política de informatização dos processos institucionais. Como exemplos desta informatização, pode-se citar a adoção do SEI (Sistema Eletrônico de Informações) para controle de processos e publicações eletrônicas (TRF4, 2018), também vale mencionar a utilização do Moodle (*Modular Object-Oriented Dynamic Learning Environment*) para apoio à aprendizagem em ambiente virtual (MOODLE, 2018), e, ainda, destaca-se a efetivação do SUAP (Sistema Unificado de Administração Pública) como ferramenta unificada de apoio à gestão (IFRN, 2018). Contudo, tem-se que a organização de eleições realizadas pela Internet seja um verdadeiro marco neste processo de informatização (IFRO, 2018b).

Ao se estabelecer os componentes básicos do sistema eletrônico de votação e procedimentos relacionados, entende-se que a preocupação direta deve ser focada no incremento da segurança para que seja possível executar eleições confiáveis que conservem absolutamente o sigilo e a integridade das escolhas definidas pelo eleitor (ARANHA *et al.*, 2013).

De fato, estas primitivas de segurança são esperadas em todo e qualquer processo de votação democrático, e vêm sendo discutidas em diversas comunicações científicas especializadas, como, por exemplo, em Aranha *et al.* (2013), Silva (2002), Gritzalis (2012), Krimmer *et al.* (2017), Hao e Ryan (2016), entre outros.

Todavia, esta observância aos requisitos de segurança não foi a tônica do último pleito eleitoral ocorrido no Instituto Federal de Educação, Ciência e Tecnologia de Rondônia, conforme será discutido nas próximas seções deste trabalho.

1.1 OBJETIVO

O objetivo geral deste trabalho é formalizar as observações realizadas pelo autor desde o dia 28 de Maio de 2018 – data do anúncio do sistema de votação a ser adotado nas eleições de Reitor e Diretores Gerais dos *campi* do IFRO (IFRO, 2018e) –.

Mais especificamente, destaca-se que este trabalho apresenta uma análise técnico-científica das primitivas criptográficas do sistema de votação adotado, bem como discute a (in)segurança das práticas e processos do último pleito eleitoral do Instituto Federal de Rondônia.

SAJEBTT, Rio Branco, UFAC
v.8 n.2 (2021): Edição jan/abr.
ISSN: 2446-4821

Além disso, este trabalho também apresenta cenários onde estas vulnerabilidades e fragilidades podem ser exploradas com o intuito de promover a fraude eleitoral ou, eventualmente, outros crimes de responsabilidade.

Contudo, é importante salientar que o conteúdo e as conclusões aqui apresentados são de inteira responsabilidade do autor e não representam de forma alguma a opinião do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia, Universidade Federal de Rondônia ou quaisquer outros órgãos e setores aos quais eventualmente o autor prestou ou venha a prestar serviço. Além disso, destaca-se que este trabalho não possui nenhuma motivação política, se tratando puramente de um estudo acadêmico.

1.2 ORGANIZAÇÃO DO TRABALHO

Este trabalho obedece a estrutura a seguir. A Seção 2 discute o método adotado durante o desenvolvimento deste estudo e, também, apresenta as principais características do Instituto Federal de Rondônia, descreve brevemente o sistema de votação *online* adotado pelo instituto, e ainda traz um resumo dos acontecimentos do último pleito eleitoral. Já as Seções 3 e 4 expõem o conjunto de vulnerabilidades e fragilidades encontradas no processo eleitoral como um todo. Por fim, a Seções 5 e 6 apresentam algumas considerações acerca da possível abrangência deste estudo, bem como traz as conclusões e sugestões para que se incrementem a segurança, transparência e auditabilidade do sistema eletrônico de votação do Instituto Federal de Rondônia.

2 DESCRIÇÃO DO PLEITO ELEITORAL E DOS MÉTODOS

2.1 MÉTODO CIENTÍFICO

O método adotado durante o desenvolvimento deste estudo foi o da pesquisa exploratória (WAZLAWICK, 2020), uma vez que o autor não tinha necessariamente uma noção de todos os problemas de segurança que encontraria. Assim, conforme o autor foi tomando contato com o sistema de votação eletrônica sob análise, bem como as técnicas utilizadas durante a sua implantação, o autor foi, então, desenvolvendo estratégias de pesquisa e coletando informações sobre vulnerabilidade e fragilidades já conhecidas.

Vale ressaltar que o autor não obteve acesso ao código fonte em produção. Desta forma, o processo de análise e discussão de estratégias de ataques foram realizadas a partir de dados e sistemas públicos, referências bibliográficas, e implementações de ataques conhecidos.

SAJEBTT, Rio Branco, UFAC
v.8 n.2 (2021): Edição jan/abr.
ISSN: 2446-4821

2.2 APRESENTAÇÃO – IFRO

O Instituto Federal de Educação, Ciência e Tecnologia de Rondônia, autarquia federal vinculada ao Ministério da Educação (MEC), foi criado juntamente com todos os demais Institutos Federais através da Lei N.º 11.892 de 29 de dezembro de 2008 (BRASIL, 2008). O IFRO é uma instituição especializada na oferta de educação profissional e tecnológica, atuando também na educação básica e superior, na pesquisa e no desenvolvimento de produtos e serviços, em estreita articulação com a sociedade. Territorialmente, o Instituto Federal de Rondônia está presente em vários municípios do estado de Rondônia, ofertando educação presencial e à distância em 09 (nove) *campi* e mais de 170 polos de Ensino a Distância (IFRO, 2018a).

Desde sua implantação, o IFRO vem apresentando um crescente aumento na sua matriz orçamentária – seja pela implantação de novos *campi*, como pela expansão no número de servidores e alunos –, sendo que para o ano de 2021 existe uma previsão orçamentária de mais de R$ 286 milhões (IFRO, 2018c, p. 237).

Para estabelecer uma relação entre as receitas do IFRO e a média orçamentária estadual, destaca-se que o município de Ji-Paraná, segundo maior município do estado, prevê um orçamento de aproximadamente R$ 300 milhões para o ano de 2021 (JI-PARANÁ, 2020). Ou seja, os gestores do Instituto Federal de Rondônia administram um montante significativo dentro da realidade rondoniense.

2.3 HELIOS, O SISTEMA DE VOTAÇÃO ADOTADO

Helios é um sistema de votação *online* que permite a realização de eleições através da Internet, com auditoria aberta ao público (*End-to-end voter verifiable* - E2E) (IFSC, 2021). Este sistema foi desenvolvido por uma comunidade de software livre, e seu código-fonte pode ser encontrado em Adida, Marneffe e Pereira (2021a) e Adida, Marneffe e Pereira (2021b).

Segundo o Diretor de Gestão de Tecnologia da Informação do IFRO (DGTI-IFRO), todas eleições do Instituto Federal de Rondônia ocorrerão com o suporte do Sistema Helios:

> "O IFRO adaptou uma versão que foi desenvolvida pelo Instituto Federal de Santa Catarina. Trata-se de um sistema seguro e que possui níveis avançados de criptografia para cada voto, que é enviado de forma criptografada para o banco de dados. Também permite a apuração rápida, a partir do momento que foi aberta e os eleitores realizaram a votação, a apuração é feita de forma instantânea. Em questão de minutos já tem o resultado dessa eleição." (IFRO, 2018b)

SAJEBTT, Rio Branco, UFAC
v.8 n.2 (2021): Edição jan/abr.
ISSN: 2446-4821

Todavia, conforme será discutido nas próximas seções, verificou-se que este sistema adotado pelo IFRO não possui todas as primitivas criptográficas necessárias para garantir a segurança de um processo eleitoral.

2.4 ACONTECIMENTOS DO ÚLTIMO PLEITO ELEITORAL

Conforme mencionado anteriormente, o autor deste trabalho vem realizando observações e análises de segurança desde a escolha do sistema de votação a ser utilizado pelo Instituto Federal de Rondônia.

Com intuito de notificar a Comissão Eleitoral e Gabinete da Reitoria sobre as vulnerabilidades e fragilidades do sistema adotado, foi publicada uma versão preliminar deste trabalho, contendo as principais ideias e apontamentos aqui expostos (ANDRADE, 2018).

Após a disseminação deste relatório, a DGTI-IFRO emitiu um "Parecer Técnico" explicando algumas medidas de seguranças implementadas pelo Instituto Federal de Rondônia, sendo elas (SOUZA, 2018): proteção da rede interna através de *firewalls*, implementação de auditoria baseada em LOGs do sistema, e utilização de certificados de segurança SSL (*Secure Socket Layer*) para comunicações externas.

Porém, para amparar a utilização do Sistema Helios, a DGTI-IFRO utilizou a justificativa de que tal sistema vem sendo utilizado em outras instituições sem a ocorrência de incidentes, e por isso está seguro (SOUZA, 2018). Todavia, sabe-se que não é possível garantir a segurança de um sistema só porque ele é amplamente utilizado.

Contudo, mesmo com a incerteza acerca da segurança do sistema escolhido, e, ainda, após pedido formal do candidato Ênio Gomes da Silva para alteração do sistema (SILVA, 2018), o pleito eleitoral para Reitor e Diretores Gerais ocorreu e o resultado final foi homologado (CONSUP-IFRO, 2018).

De todo modo, o autor deste estudo optou por submeter esta análise de segurança a um comitê científico especializado, para que suas observações sejam validadas ou refutadas.

3 VULNERABILIDADE

Nesta seção é descrita uma grave vulnerabilidade encontrada durante esta análise. Tal vulnerabilidade permite que um atacante capture e utilize a identidade de outro usuário.

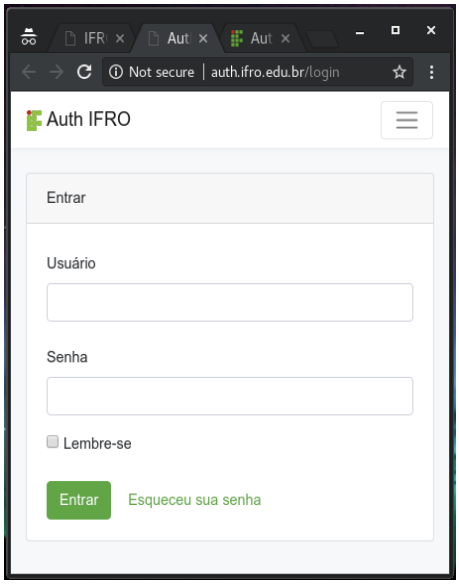
SOUTH AMERICAN JOURNAL
of Basic Education, Technical and Technological
SAJEBTT, Rio Branco, UFAC
v.8 n.2 (2021): Edição jan/abr.
ISSN: 2446-4821

3.1 AUTENTICAÇÃO INSEGURA

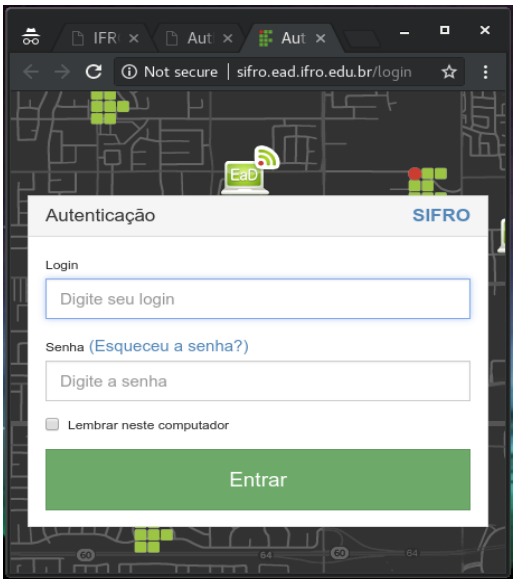
Com a crescente pervasividade de tecnologias computacionais, a autenticação de usuários assume um papel essencial em sistemas modernos para prover segurança no acesso a informações e serviços, garantindo que somente os usuários autorizados obtenham os privilégios necessários.

Apesar deste papel crucial, notou-se que os mantenedores do sistema de votação do Instituto Federal de Rondônia não deram a devida atenção ao mecanismos de autenticação implementado para funcionar juntamente com o sistema de votação Helios[1].

Figura 1 – Telas do autenticador do sistema de votação adotado pelo IFRO.



(a) Website para autenticação de servidores e alunos da modalidade de educação presencial.



(b) Website para autenticação de alunos da modalidade de educação a distância.

Fonte: (IFRO, 2018d).

Conforme pode ser verificado nas Figuras 1(a) e 1(b) (canto superior esquerdo de cada figura), o website utilizado para autenticar os usuários não fornece nenhum mecanismo de segurança para os dados trocados entre o computador do usuário e o mecanismo de autenticação.

Desta forma, um atacante que possua acesso a algum dos dispositivos de rede conectados entre a origem e destino dos dados (computador do usuário e website de autenticação) poderá capturar os dados inseridos no formulário de autenticação e (re)utilizá-

[1] Ou seja, esta é uma vulnerabilidade criada pelos mantenedores do sistema no IFRO. Não podendo ser atribuída ao sistema original.

SAJEBTT, Rio Branco, UFAC
v.8 n.2 (2021): Edição jan/abr.
ISSN: 2446-4821

los como quiser. Podendo, assim, utilizar a identidade do usuário atacado para votar no candidato que desejar.

Um outro desdobramento deste "sequestro" de identidade reside na possibilidade do atacante autenticar-se nos demais sistemas institucionais do IFRO utilizando a identidade do usuário atacado (e.g., Sistema Eletrônico de Informações – SEI, Sistema Unificado de Administração Pública – SUAP, e todos demais sistemas que utilizem as mesmas credenciais de acesso). Assim, o atacante poderá criar documentos ou promover alterações indevidas, podendo, inclusive, cometer delitos utilizando outra identidade.

Outras informações sobre este tipo de ataque podem ser consultadas em: Brown e Stallings (2017), McClure, Scambray e Kurtz (2014).

Atualização pós pleito eleitoral

Em uma atualização ocorrida após as eleições, a Diretoria de Gestão de Tecnologia da Informação do IFRO (DGTI-IFRO) corrigiu algumas configurações que impediam o estabelecimento de uma conexão segura entre o computador do usuário e o mecanismo de autenticação. A solução encontrada foi utilizar o certificado digital ICPEdu, fornecido pela ICP-Brasil (ITI, 2021).

Apesar de ser uma boa solução para a maioria das aplicações web, acredita-se que esta não seja plausível para uma aplicação crítica como a de votação eletrônica.

Isto porque, à princípio, não é possível garantir que o computador do usuário (eleitor) não esteja infectado por alguma aplicação maliciosa como *keylogger*, otimização para mecanismos de busca "envenenado" (HOWARD; KOMILI, 2010), *spyware*, entre tantas outras aplicações que comumente se hospedam nos computadores dos usuários finais com intuito de capturar suas credenciais para fins maliciosos.

Além disso, o mantenedor do sistema não pode garantir que toda rede utilizada para conexão esteja livre de ameaças como SSLStrip (MARLINSPIKE, 2011) e outras aplicações maliciosas que impeçam o estabelecimento de conexões seguras utilizando certificados digital e SSL.

Dessa forma, utilizando o cenário de votação através de qualquer computador conectado a Internet, observa-se que não é possível garantir que um atacante não seja capaz de capturar os dados inseridos no formulário de autenticação e (re)utilizá-los para fins maliciosos.

SAJEBTT, Rio Branco, UFAC
v.8 n.2 (2021): Edição jan/abr.
ISSN: 2446-4821

4 FRAGILIDADES

O exame do código-fonte do Sistema Helios (ADIDA; MARNEFFE; PEREIRA, 2021b) evidenciou um conjunto de fragilidades em componentes críticos do *software*. Além disto, durante a execução do último pleito eleitoral, foi observado que algumas práticas adotadas pela equipe de implantação do sistema adicionaram fragilidades ao processo eleitoral como um todo. Sendo que cada fragilidade apresentada aqui representa uma vulnerabilidade em potencial que permite a um agente externo ou (principalmente) um agente interno formular uma metodologia de ataque.

4.1 FALHA NA VERIFICABILIDADE DO VOTO

A possibilidade de verificar se o voto foi computado corretamente é um dos pontos primordiais em sistemas eleitorais modernos (KUSTERS; TRUDERUNG; VOGT, 2012). Isto porque, esta característica garante a auditabilidade de uma eleição realizada eletronicamente.

Apesar desta funcionalidade ser essencial, não se admite que tal característica gere outra fragilidade. Afinal, em sistemas computacionais seguros, não devemos favorecer uma característica em detrimento de outra.

Contudo, ataques presentes na literatura demonstram que a forma que foi implementada a verificabilidade do voto no sistema Helios possui falhas (KUSTERS; TRUDERUNG; VOGT, 2012; CORTIER; SMYTH, 2013; ESTEHGHARI; DESMEDT, 2010). Sendo que uma destas falhas possibilita que um mesmo recibo de voto atribua votos a diferentes candidatos (KUSTERS; TRUDERUNG; VOGT, 2012).

4.2 UTILIZAÇÃO DE ALGORITMOS OBSOLETOS E INSEGUROS

Alguns algoritmos criptográficos utilizados na implementação do sistema de votação Helios não oferecem a segurança esperada. Nas próximas seções serão apontados quais são estes algoritmos e ainda será discutido o porquê destes algoritmos serem considerados como obsoletos e inseguros.

4.2.1 FONTE INADEQUADA DE ENTROPIA

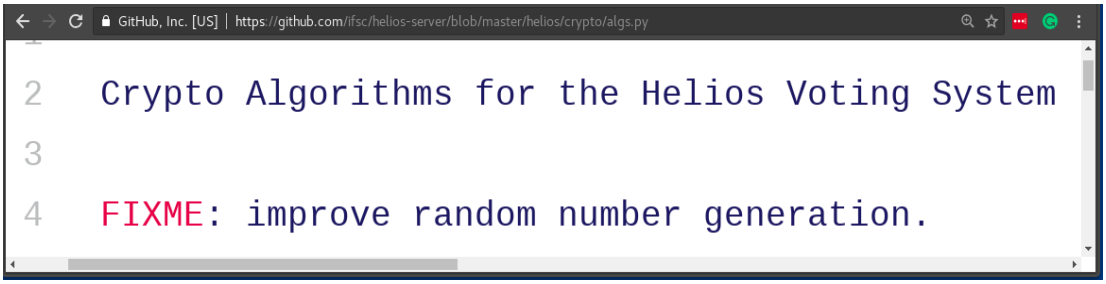
Segundo o primeiro pesquisador que atacou a urna eletrônica brasileira, professor Diego Aranha (2013):

> "entropia tem caráter crítico para várias operações criptográficas que requerem dados aleatórios, como a geração de chaves efêmeras ou a alimentação com semente de geradores pseudo-aleatórios, e em muitos casos é possível contornar completamente a técnica criptográfica com ataques apenas na fonte de entropia" (ARANHA *et al.*, 2013).

SAJEBTT, Rio Branco, UFAC
v.8 n.2 (2021): Edição jan/abr.
ISSN: 2446-4821

Como qualquer aplicação de votação eletrônica necessita de uma fonte adequada de aleatoriedade para assinatura dos votos e geração das chaves, espera-se que o sistema de votação implemente seu gerador de números pseudo-aleatórios de forma extremamente segura, pois a não observância desta primitiva poderá comprometer a segurança de todo o sistema (conforme destacado anteriormente).

Figura 2 – Comentário de correção encontrado no arquivo que contém os arquivos criptográficos utilizados pelo sistema Helios (./helios/crypto/algs.py).



Fonte: (ADIDA; MARNEFFE; PEREIRA, 2021a).

Todavia, isto não é o que ocorre no sistema Helios. Em uma rápida análise no código-fonte desta solução (ADIDA; MARNEFFE; PEREIRA, 2021a; ADIDA; MARNEFFE; PEREIRA, 2021b), observa-se que a semente do gerador de números pseudo-aleatórios é puramente baseado em dados de software. Além disto, no arquivo que contém os arquivos criptográficos utilizados pelo sistema (*./helios/crypto/algs.py*), pode ser encontrado o comentário que diz: "*FIXME: improve random number generation.*" (CORRIJA-ME: aprimorar a geração de números aleatórios, em tradução livre). Ou seja, um problema evidente, assumido inclusive pelos autores do código.

A utilização de fonte inadequada de entropia não é uma vulnerabilidade desconhecida em sistemas de votação ou software comercial (ARANHA *et al.*, 2013). A urna eletrônica utilizada nos Estados Unidos empregava técnicas inseguras (CALANDRINO *et al.*, 2007), obtendo informação a partir do conteúdo da tela e de uma medida de tempo com resolução de milissegundo desde a inicialização do sistema operacional.

Recentemente, a urna eletrônica brasileira sofreu um ataque que possibilita a recuperação da ordem de votação pois seu *software* utilizava apenas a medida do tempo em resolução de segundos como fonte de entropia (ARANHA *et al.*, 2013). Além disso, em 1995, calouros de doutorado da Universidade de Berkeley descobriram sem acesso ao código-fonte que a versão 1.1 do navegador Netscape apresentava exatamente a mesma fragilidade (GOLDBERG; WAGNER, 1996).

SAJEBTT, Rio Branco, UFAC
v.8 n.2 (2021): Edição jan/abr.
ISSN: 2446-4821

4.2.2 ESCOLHA INADEQUADA DE ALGORITMOS

Além da escolha absolutamente inadequada de algoritmo para geração de números pseudoaleatórios, o sistema de votação Helios também utiliza a função de hash (ou de resumo criptográfico, em português livre) SHA-1 (NIST, 2002). Conforme pode ser verificado no código-fonte desta solução (ADIDA; MARNEFFE; PEREIRA, 2021a; ADIDA; MARNEFFE; PEREIRA, 2021b).

Esta função de hash específica tem uso não recomendado desde 2006, quando se verificou que a mesma não fornecia a resistência esperada contra colisões (WANG; YIN; YU, 2005). Uma materialização dessa insegurança pode ser encontrado no projeto SHAttered do Google (STEVENS, 2017), neste trabalho, os pesquisadores encontraram dois arquivos de PDF completamente distintos mas que possuem o mesmo valor de hash, quando utilizado a função SHA1. Desta forma, fica claro que é prudente a migração rápida para funções de hash mais seguras (BURR, 2009).

4.3 INVERIFICABILIDADE DO CÓDIGO-FONTE EM PRODUÇÃO

Apesar da Diretoria de Gestão de Tecnologia da Informação do IFRO afirmar que vem utilizando o sistema de votação *online* Helios (IFRO, 2018b; IFRO, 2018e), não é possível verificar se o código-fonte em produção, disponível no site <http://eleicao.ifro.edu.br/>, é o mesmo código mantido pela comunidade que o desenvolveu (ADIDA; MARNEFFE; PEREIRA, 2021a; ADIDA; MARNEFFE; PEREIRA, 2021b). Uma vez que não é possível auditar publicamente o código-fonte da página em produção, e também não exista nenhum mecanismo para comprovar sua integridade ou similaridade com o código original.

4.4 FORMULAÇÃO EQUIVOCADA DO MODELO DE ATACANTE

Assim como na urna eletrônica brasileira (ARANHA *et al.*, 2013), o projeto de mecanismos de segurança utilizado preocupa-se exageradamente com atacantes externos e ignora o risco de atacantes internos como: funcionários da Diretoria de Gestão de Tecnologia da Informação, Diretores Gerais, Pró-Reitores e Reitores.

Também preocupar-se com estes agentes internos é essencial pois eventualmente eles podem se tornar o tipo de atacante mais perigoso de um sistema de votação: o atacante que dispõe de informação privilegiada.

SAJEBTT, Rio Branco, UFAC
v.8 n.2 (2021): Edição jan/abr.
ISSN: 2446-4821

4.5 POSSIBILIDADE DE ATAQUES UTILIZANDO ENGENHARIA SOCIAL

Durante a execução do último pleito eleitoral, foi observado que os representantes da DGTI-IFRO em cada um dos *campi* estavam conduzindo o pleito eleitoral do corpo discente de forma extremamente insegura. Estes representantes criavam uma senha comum a todos discentes (e.g., "ifro-2018") e os instruíam a não alterá-la, pois alterações poderiam causar inconsistências. Desta forma, o único dado que divergia de um usuário para o outro era o seu identificador, que neste caso era o CPF (Cadastro de Pessoas Físicas) de cada um dos envolvidos.

Como o CPF é um dado que pode ser facilmente encontrado por qualquer atacante, principalmente se este atacante possui proximidade à vítima ou acesso privilegiado a dados escolares da instituição, conjectura-se que usuários mal intencionados tiveram a possibilidade de alterar os votos de parte do corpo discente.

4.6 PROTEÇÃO INADEQUADA DO SIGILO DO VOTO

Conforme evidenciado no vídeo institucional que explica o processo de votação do Instituto Federal de Rondônia (Trecho ilustrado na Figura 3): "o eleitor poderá votar quantas vezes quiser, enquanto a eleição estiver aberta, porém o sistema terá registrado somente o último voto" (IFRO, 2018e). Desta forma, conjectura-se que o sistema é capaz de relacionar um voto a um eleitor de maneira determinística. Ou seja, o sistema possui um banco de dados com os votos de cada um dos eleitores, e os deixa ser alterado até o encerramento do processo eleitoral.

Combinando esta característica com as demais fragilidades apontadas anteriormente, não se torna improvável que um agente interno (um gestor do alto escalão, por exemplo) recupere a lista dos votos com seus respectivos eleitores. Não garantindo, assim, um dos direitos fundamentais de qualquer eleição: o direito ao sigilo/anonimato do voto.

5 ABRANGÊNCIA DESTAS FRAGILIDADES

A existência de problemas de segurança em sistemas de votação eletrônica são por si só um grande motivo de preocupação. Afinal, nenhum usuário deste tipo de sistema deseja ter o sigilo e a integridade de seu voto violados.

Contudo, no caso do sistema adotado pelo Instituto Federal de Rondônia, esta preocupação é ainda maior, uma vez que o Sistema de Votação Helios é utilizado em

SAJEBTT, Rio Branco, UFAC
v.8 n.2 (2021): Edição jan/abr.
ISSN: 2446-4821

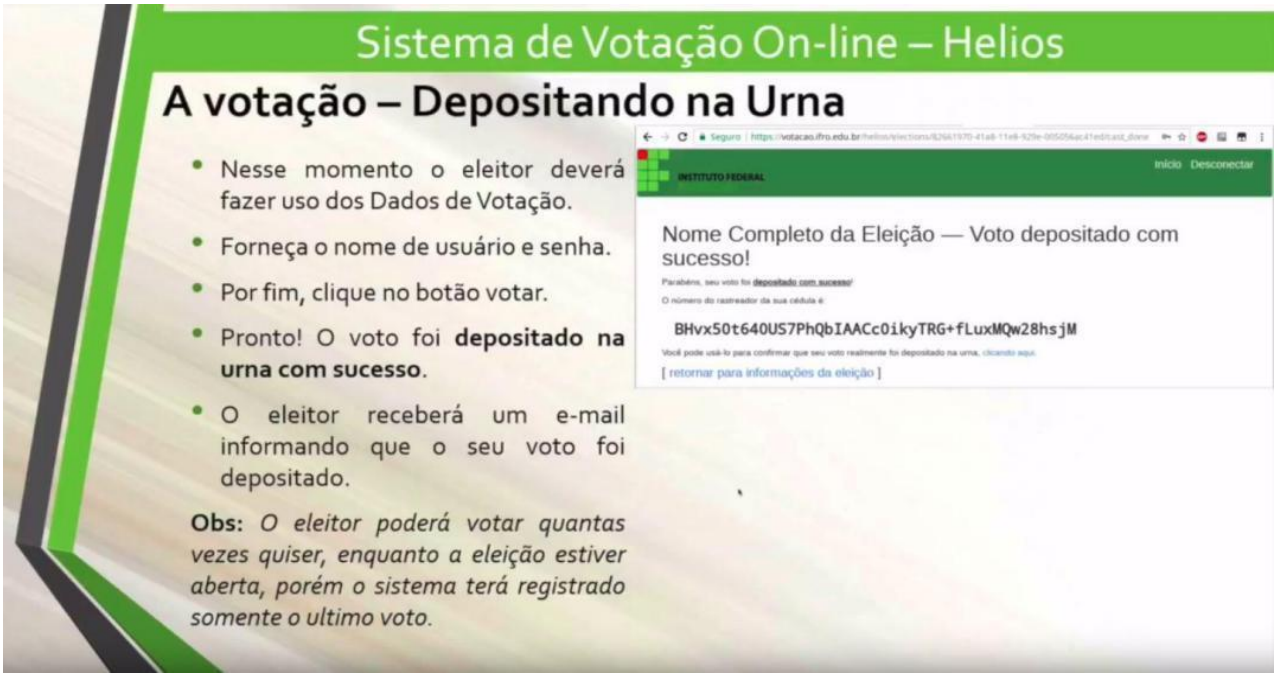
diversas outras instituições. Ou seja, as falhas de segurança levantadas neste estudo também podem ser encontradas (e possivelmente exploradas) em outros cenários.

Em uma busca pela Internet, pode ser verificado que este sistema vem sendo adotado por instituições como Defensoria Pública da União – DPU (UNB, 2016); Instituto Federal Fluminense – IFF (IFF, 2017); Instituto Federal de Goiás – IFG (IFG, 2017; IFG, 2018); Instituto Federal do Pará – IFPA (IFPA, 2016); Instituto Federal de Santa Catarina IFSC (IFSC, 2021; ADIDA; MARNEFFE; PEREIRA, 2021b); Universidade de São Paulo – USP (FMRP-USP, 2018).

Esta preocupação ganhou ainda mais força nas últimas semanas porque, devido às medidas de isolamento social necessárias ao combate à pandemia do novo coronavírus (COVID-19), diversas Instituições Federais de Ensino sinalizaram que utilizarão sistemas de votação *online* em seus processos de consulta à comunidade.

Sendo assim, tem-se que a abrangência desta análise de segurança não se limita ao Instituto Federal de Rondônia. Sendo recomendado que todas instituições que adotam o Sistema Helios ponderem sobre a sua utilização.

Figura 3 – Trecho do vídeo institucional que explica o processo de votação.



Fonte: (IFRO, 2018e).

6 CONCLUSÕES E PERSPECTIVAS

Este trabalho apresentou um conjunto de fragilidades e vulnerabilidades que evidenciam falhas de segurança no sistema eleitoral adotado pelo IFRO (ou sistema de consulta à comunidade, como vem sendo chamado em algumas comunicações oficiais). As consequências dessas falhas foram discutidas ao longo do texto sob um modelo realista de atacante. Em particular, mostrou-se possível que um atacante capture e utilize as credenciais de um usuário legítimo, explorando a vulnerabilidade do sistema de autenticação.

Contudo, além da necessidade das correções das primitivas de segurança, espera-se que a equipe de desenvolvimento do sistema de votação adotado pelo Instituto Federal de Rondônia fique atenta a algumas fragilidades comuns no processo de desenvolvimento de *softwares* destinados à votação. Complexidade acentuada, auditoria externa insuficiente, ausência de análise estática de código, ausência de exercícios interno, falta de treinamento formal, disponibilização de dados críticos aos investigadores, ignorância da literatura relevante, e falsa sensação de segurança são exemplos de erros comuns que levam ao desenvolvimento de soluções frágeis (ARANHA *et al.*, 2013; CALANDRINO *et al.*, 2007).

Além disso, torna-se evidente a necessidade de se utilizar recursos para avaliação científica, independente e contínua das soluções de segurança adotadas pelo Instituto Federal de Educação, Ciência e Tecnologia de Rondônia. Ainda mais havendo ampla disponibilidade de especialistas internos e externos capazes de contribuir na direção do incremento real das propriedades de segurança destas soluções.

REFERÊNCIAS

ADIDA, B.; MARNEFFE, O. de; PEREIRA, O. **Helios Election System**. 2021. Disponível em: <https://github.com/benadida/helios-server>. (Acesso em: 27 de março de 2021).

_____. **Helios Election System – IFSC**. 2021. Disponível em: <https://github.com/ifsc/helios-server>. (Acesso em: 27 de março de 2021).

ANDRADE, E. R. **Breve análise de segurança do sistema de votação eletrônica adotado pelo Instituto Federal de Rondônia.** 2018. Disponível em: <http://ewerton.andrade.pro.br/arquivos/relatorio-urna-ifro-1.0.pdf>. (Acesso em: 27 de março de 2021).

ARANHA, D. F. *et al.* **Vulnerabilidades no software da urna eletrônica brasileira**. 2013. 40 p. Disponível em: <https://sites.google.com/site/dfaranha/projects/relatorio-urna.pdf>. (Acesso em: 27 de março de 2021).

BRASIL. L**ei nº 11.892, de 29 de dezembro de 2008**. 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11892.htm>. (Acesso em: 27 de março de 2021).

SAJEBTT, Rio Branco, UFAC
v.8 n.2 (2021): Edição jan/abr.
ISSN: 2446-4821

BROWN, L.; STALLINGS, W. **Segurança de Computadores: Princípios e Práticas**. Elsevier Editora Ltda, 2017. ISBN 9788535264500.

BURR, W. **NIST Comments on Cryptanalytic Attacks on SHA-1**. 2009.

CALANDRINO, J. A.; FELDMAN, A. J.; HALDERMAN, J. A.; WAGNER, D.; YU, H.; ZELLER, W. P. Source code review of the diebold voting system. 2007.

CONSUP-IFRO. A**ta da 21ª reunião ordinária do Conselho Superior**. 2018. Disponível em: <https://sei.ifro.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0> Código verificador: 0279430 CRC: 62B11A1C. (Acesso em: 27 de março de 2021).

CORTIER, V.; SMYTH, B. Attacking and fixing helios: An analysis of ballot secrecy. **Journal of Computer Security**, IOS Press, v. 21, n. 1, p. 89–148, 2013.

ESTEHGHARI, S.; DESMEDT, Y. Exploiting the client vulnerabilities in internet e-voting systems: Hacking helios 2.0 as an example. **EVT/WOTE**, v. 10, p. 1–9, 2010.

FMRP-USP. **Helios Voting Corporativo – FMRP-USP**. 2018. Disponível em: <http://sti.fmrp.usp.br/helios-voting-corporativo/>. (Acesso em: 27 de março de 2021).

GOLDBERG, I.; WAGNER, D. Randomness and the netscape browser. **Dr Dobb's Journal-Software Tools for the Professional Programmer**, Redwood City, CA: M&T Pub., 1989-, v. 21, n. 1, p. 66–71, 1996.

GRITZALIS, D. **Secure Electronic Voting**. Springer US, 2012. (Advances in Information Security). ISBN 9781461502395.

HAO, F.; RYAN, P. **Real-World Electronic Voting: Design, Analysis and Deployment**. CRC Press, 2016. (Series in Security, Privacy and Trust). ISBN 9781315354118.

HOWARD, F.; KOMILI, O. Poisoned search results: How hackers have automated search engine poisoning attacks to distribute malware. **Sophos Technical Papers**, p. 1–15, 2010.

IFF. **Sistema de votação online do IFF garante rapidez e segurança dos processos eleitorais**. 2017. Disponível em: <http://portal1.iff.edu.br/reitoria/noticias/sistema-de-votacao-online-do-iffluminense-garante-rapidez-e-seguranca-dos-processos-eleitorais>. (Acesso em: 27 de março de 2021).

IFG. **Welcome to IFG E-Voting System**. 2017. Disponível em: <https://votacoes.ifg.edu.br/>. (Acesso em: 27 de março de 2021).

_____. **Catálogo de Sistemas – IFG**. 2018. Disponível em: <https://www.ifg.edu.br/dti/sistemas>. (Acesso em: 27 de março de 2021).

IFPA. **IFPA realizará eleição para o Conselho Superior**. 2016. Disponível em: <https://www.ifpa.edu.br/component/content/article?id=367>. (Acesso em: 27 de março de 2021).

IFRN. **Sistema Unificado de Administração Pública (SUAP) – IFRO**. 2018. Disponível em: <https://suap.ifro.edu.br/>. (Acesso em: 27 de março de 2021).

IFRO. **Apresentação – IFRO**. 2018. Disponível em: <http://portal.ifro.edu.br/apresentacao>. (Acesso em: 27 de março de 2021).

_____. **Eleições para reitor e diretores de campi ocorrem no dia 05**. 2018. Disponível em: <http://portal.ifro.edu.br/component/content/article?id=5301>. (Acesso em: 27 de março de 2021).

_____. **Plano de Desenvolvimento Institucional do IFRO (2018–2022)**. 2018. Disponível em: <https://portal.ifro.edu.br/images/ifro-pdi-interativo-20180209_pagina-simples.pdf>. (Acesso em: 27 de março de 2021).

_____. **Sistema de eleições do IFRO**. 2018. Disponível em: <http://eleicao.ifro.edu. br>. (Acesso em: 27 de março de 2021).

_____. **Tutorial Votação - Processo de Consulta à Comunidade do IFRO 2018**. 2018. Disponível em: <https://www.youtube.com/watch?v=cFR69Ra3yTs>. (Acesso em: 27 de março de 2021).

IFSC. **Sistema de Votação On-line – Helios**. 2021. Disponível em: <https://dtic.ifsc.edu.br/sistema-de-votacao-online-helios/>. (Acesso em: 27 de março de 2021).

ITI. **ICP-Brasil**. 2021. Disponível em: <https://estrutura.iti.gov.br>. (Acesso em: 27 de março de 2021).

JI-PARANÁ. **Lei nº 3330, de 22 de junho de 2020**. 2017. Disponível em: <http://transparencia.ji-parana.ro.gov.br/transparencia/aplicacoes/publicacao/download.php?id_doc=018956&extencao=PDF>. (Acesso em: 27 de março de 2021).

KRIMMER, R.; VOLKAMER, M.; BARRAT, J.; BENALOH, J.; GOODMAN, N.; RYAN, P.; TEAGUE, V. **Electronic Voting: First International Joint Conference, E-Vote-ID 2016, Bregenz, Austria, October 18-21, 2016, Proceedings**. Springer International Publishing, 2017. (Lecture Notes in Computer Science). ISBN 9783319522401.

KUSTERS, R.; TRUDERUNG, T.; VOGT, A. Clash attacks on the verifiability of e-voting systems. In: **2012 IEEE SSP**. 2012. p. 395–409. ISSN 1081-6011.

MARLINSPIKE, M. **Software >> sslstrip**. 2011. Disponível em: <https://github.com/moxie0/sslstrip>. (Acesso em: 27 de março de 2021).

MCCLURE, S.; SCAMBRAY, J.; KURTZ, G. **Hackers Expostos - 7ed: Segredos e Soluções para a Segurança de Redes**. Bookman Editora, 2014. ISBN 9788582601426.

MOODLE. **Ambiente Virtual de Aprendizagem do IFRO – virtual.ifro**. 2018. Disponível em: <https://virtual.ifro.edu.br/>. (Acesso em: 27 de março de 2021).

NIST. **FIPS 180-2: Secure hash standard**. 2002.

SILVA, Ê. G. da. **SISTEMA DE VOTAÇÃO - URGENTE (email)**. 2018. Disponível em: <http://docdro.id/LKnKRWv>. (Acesso em: 27 de março de 2021).

SILVA, M. C. da. **Voto eletrônico: é mais seguro votar assim?** Editora Insular, 2002.

SOUZA, E. F. de. **Parecer Nº 3/2018/REIT - DGTI/REIT - PRODIN/REIT**. 2018. Disponível em: <https://sei.ifro.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_ac

SAJEBTT, Rio Branco, UFAC
v.8 n.2 (2021): Edição jan/abr.
ISSN: 2446-4821

esso_externo=0> Código verificador: 0258108CRC: 5A004472. (Acesso em: 27 de março de 2021).

STEVENS, M. **SHAttered: We have broken SHA-1 in practice**. 2017. Disponível em: <https://shattered.io>. (Acesso em: 27 de março de 2021).

TRF4. **Sistema Eletrônico de Informações (SEI) – IFRO**. 2018. Disponível em: <https://sei.ifro.edu.br/>. (Acesso em: 27 de março de 2021).

UNB. **UnB adapta sistema de voto eletrônico para Defensoria Pública da União**. 2016. Disponível em: <https://www.unbciencia.unb.br/exatas/41-engenharia- eletrica/117-unb-adapta-sistema-de-voto-eletronico-para-defensoria-publica-da-uniao>. (Acesso em: 27 de março de 2021).

WANG, X.; YIN, Y. L.; YU, H. Finding collisions in the full SHA-1. In: **Advances in Cryptology - CRYPTO 2005**. Springer, 2005. v. 3621.

WAZLAWICK, R. S. **Metodologia de pesquisa para ciência da computação**. Rio de Janeiro: Elsevier, 2020. 152 p. ISBN 8595151091.