Breve análise de segurança do sistema de votação eletrônica adotado pelo Instituto Federal de Rondônia

Ewerton R. Andrade[1]

[1]Instituto Federal de Rondônia, *campus* Porto Velho Calama,
<ewerton.andrade@ifro.edu.br>.

04 de Junho de 2018

Versão 1.0 *

*Disponível em: http://ewerton.andrade.pro.br/arquivos/relatorio-urna-ifro-1.0.pdf

"Quem vigia os vigilantes?"

(Juvenal)

Resumo

Este relatório apresenta uma análise de segurança do sistema de votação adotado pelo Instituto Federal de Educação, Ciência e Tecnologia de Rondônia, realizada de maneira independente. Durante esta análise, foram detectadas vulnerabilidades no *software* de votação e também no projeto de implantação do sistema. Em razão disto, este relatório apresenta cenários onde estas vulnerabilidades podem ser exploradas com o intuito de promover a fraude eleitoral ou, eventualmente, outros crimes de responsabilidade. Além disto, também são apontadas fragilidades no projeto de implantação do sistema. Em particular, os principais problemas encontrados foram:

- **Autenticação insegura:** o sistema de autenticação dos usuários não fornece nenhum mecanismo de segurança para os dados trocados entre o computador do usuário e o site de autenticação. Desta forma, um atacante pode capturar os dados inseridos no formulário de autenticação e (re)utilizá-los como quiser.

- **Falha na verificabilidade do voto:** a possibilidade de verificar se o voto foi computado corretamente é um dos pontos primordiais em sistemas eleitorais modernos. Todavia, a forma que foi implementada no sistema analisado possibilita que um mesmo recibo de voto atribua votos a diferentes candidatos.

- **Utilização de algoritmos obsoletos e inseguros:** alguns algoritmos criptográficos utilizados na implementação do sistema de votação não oferecem a segurança esperada. Sendo que alguns deles são considerados inseguros há mais de 10 anos.

- **Formulação equivocada do modelo de atacante:** o projeto é totalmente pensado para defender-se de um atacante externo. Contudo, agentes internos representam um risco significativo a processos eleitorais.

- **Proteção inadequada do sigilo do voto:** a combinação dos problemas acima listados, juntamente com a capacidade de modificar o voto quantas vezes for necessário, apontam para uma possível exposição da identidade do eleitor, caso o administrador do sistema assim deseje.

Mais detalhes a respeito dos problemas acima são fornecidos no decorrer deste relatório. Contudo, nem todos os ataques/problemas contarão com uma explicação extensa, devido a falta de tempo hábil para uma análise mais criteriosa, uma vez que as informações sobre o sistema de votação a ser

adotado nas eleições de Diretores Gerais dos *campi* e Reitor foram publicadas há apenas 7 (sete) dias antes da realização desta análise [1, 2].

Sumário

1 Introdução

O Instituto Federal de Educação, Ciência e Tecnologia de Rondônia vem adotando uma crescente informatização de seus processos. Como marco nesta informatização, podemos citar a organização de eleições realizadas pela Internet [2].

Ao se estabilizar 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 [3, 4].

1.1 Objetivo deste relatório

O objetivo geral deste relatório é formalizar as observações realizadas pelo autor desde o dia 28 de Maio de 2018, data que foi anunciado o sistema eleitoral que seria adotado pelo Instituto Federal de Rondônia [1].

É importante salientar que, devido a falta de tempo hábil, possivelmente o presente relatório não cobrirá todas as vulnerabilidades e fragilidades do sistema eleitoral em análise. No entanto, espera-se que sua importância não seja minimizada.

Frisa-se, ainda, 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 Rondônia ou quaisquer outros órgãos aos quais eventualmente o autor prestou ou venha a prestar serviço.

1.2 Organização do documento

O documento obedece a estrutura a seguir. A Seção 2 descreve brevemente o sistema de votação *online* Helios. Enquanto as Seções 3 e 4 expõem o conjunto de vulnerabilidades e fragilidades encontradas no sistema eleitoral do Instituto Federal de Rondônia. Por fim, a Seção 5 apresenta as conclusões e sugestões para que se incrementem a transparência e auditabilidade do sistema eletrônico de votação do IFRO.

2 Helios

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) [5]. Este sistema foi desenvolvido por uma comunidade de

software livre, e seu código-fonte pode ser encontrado em [6] e [7] (versão adotada pelo IFRO).

Segundo o Diretor de Gestão de Tecnologia da Informação do IFRO, as eleições do Instituto Federal de Rondônia ocorrerão com o suporte do Sistema Helios [2]: "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."

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.

3 Vulnerabilidades

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.

3.1 Autenticação insegura

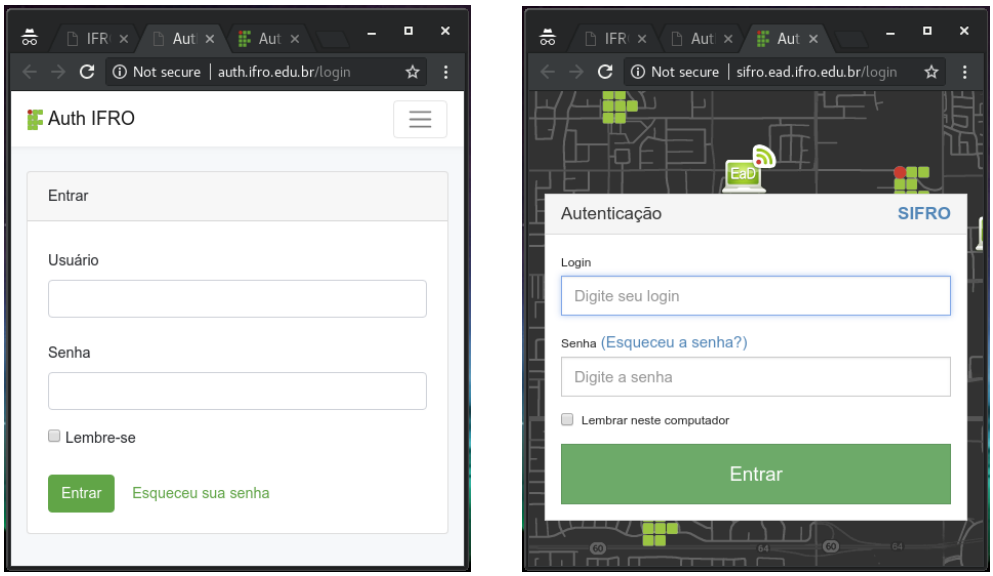
Com a crescente pervasividade de tecnologias computacionais, a autenticação de usuários assume um papel essencial em sistemas modernos para prover segurança no acesso a informações e serviços, garantindo que somente os usuários autorizados obtenham os privilégios necessários.

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[†].

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

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



(a) Website para autenticação de servidores e alunos presenciais.

(b) Website para autenticação de alunos EaD.

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

e website de autenticação) poderá capturar os dados inseridos no formulário de autenticação e (re)utilizá-los como quiser.

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

Um outro desdobramente 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: [8, 9].

4 Fragilidades

O exame do código-fonte do sistema Helios [7] evidenciou um conjunto de fragilidades em componentes críticos do *software*. 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 [10]. 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 [10, 11, 12]. Sendo que uma destas falhas possibilita que um mesmo recibo de voto atribua votos a diferentes candidatos [10].

4.2 Utilização de algoritmos obsoletos e inseguros

Alguns algoritmos criptográficos utilizados na implementação do sistema de votação adotado pelo IFRO 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" [3].

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 no parágrafo anterior).

Todavia, isto não é o que ocorre no sistema Helios. Em uma rápida análise no código-fonte desta solução [6, 7], especificamente 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 [3]. A urna eletrônica utilizada nos Estados Unidos empregava técnicas inseguras [13], 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 [3]. Além disto, 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 vulnerabilidade [14].

4.2.2 Escolha inadequada de algoritmos

Além da escolha absolutamente inadequada de algoritmo para geração de números pseudo-aleatórios, o sistema de votação Helios também utiliza a função de hash (ou de resumo criptográfico, em português livre) SHA-1 [15]. Conforme pode ser verificado no código-fonte desta solução [6, 7].

Esta função de hash específica tem uso não recomendado desde 2006, quando se verificou que a mesma não fornecia a resistência esperada contra colisões [16], ficando recomendada como prudente a migração rápida para funções de resumo mais seguras [17].

4.3 Formulação equivocada do modelo de atacante

Assim como na urna eletrônica brasileira [3], 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.

4.4 Proteção inadequada do sigilo do voto

Conforme evidenciado no vídeo institucional que explica o processo de votação do Instituto Federal de Rondônia, "o eleitor poderá votar quantas vezes qui-

ser, enquanto a eleição estiver aberta, porém o sistema terá registrado somente o último voto" [1]. 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 Conclusões e perspectivas

Este breve relatório 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 destas falhas foram discutidas ao logo 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 IFRO fique atenta a algumas fragilidades comuns no processo de desenvolvimento de *softwares* destinados a 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 [3, 13].

Além disto, torna-se evidente a necessidade de se instalar recursos para avaliação científica, independente e contínua das soluções de segurança adotadas pelo Instituto Federal 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.

Agradecimentos

O autor gostaria de agradecer ao Prof. Dr. Diego F. Aranha da UNICAMP pelas, sempre interessantes, discussões a respeito de criptografia, segurança

da informação e principalmente votações eletrônicas. Também gostaria de agradecer ao Prof. Dr. Jeroen van de Graaf da UFMG pela recente obra que contribuiu e também motivou a execução deste trabalho [4]. E especialmente agradecer ao Prof. Dr. Routo Terada e ao Prof. Dr. Marcos A. Simplicio Jr., ambos da USP, pelas orientações e conversas durante a minha formação acadêmica.

Referências

[1] IFRO, "Tutorial Votação - Processo de Consulta à Comunidade do IFRO 2018." Disponível em: `https://www.youtube.com/watch?v=cFR69Ra3yTs`, 2018.

[2] IFRO, "Eleições para reitor e diretores de campi ocorrem no dia 05." Disponível em: `http://portal.ifro.edu.br/component/content/article?id=5301`, 2018.

[3] D. F. ARANHA *et al.*, "Vulnerabilidades no software da urna eletrônica brasileira." Disponível em: `https://sites.google.com/site/dfaranha/projects/relatorio-urna.pdf?attredirects=0`, 2013.

[4] J. van de Graaf, *O mito da urna: desvendando a (in)segurança da urna eletrônica (Versão 1).* Creative Commons, 2017. url=https://inscrypt.dcc.ufmg.br/wp-content/uploads/2017/11/o-mito-da-urna.pdf.

[5] IFSC, "Sistema de Votação On-line – Helios." Disponível em: `http://dtic.ifsc.edu.br/sistemas/sistema-de-votacao-on-line-helios/`, 2018.

[6] B. Adida, O. de Marneffe, and O. Pereira, "Helios Election System." Disponível em: `https://github.com/benadida/helios-server`, 2018.

[7] B. Adida, O. de Marneffe, and O. Pereira, "Helios Election System – IFSC." Disponível em: `https://github.com/ifsc/helios-server`, 2018.

[8] L. Brown and W. Stallings, *Segurança de Computadores: Princípios e Práticas.* Elsevier Editora Ltda, 2017.

[9] S. McClure, J. Scambray, and G. Kurtz, *Hackers Expostos - 7ed: Segredos e Soluções para a Segurança de Redes.* Bookman Editora, 2014.

[10] R. Kusters, T. Truderung, and A. Vogt, "Clash attacks on the verifiability of e-voting systems," in *2012 IEEE Symposium on Security and Privacy*, pp. 395–409, May 2012.

[11] V. Cortier and B. Smyth, "Attacking and fixing helios: An analysis of ballot secrecy," *Journal of Computer Security*, vol. 21, no. 1, pp. 89–148, 2013.

[12] S. Estehghari and Y. Desmedt, "Exploiting the client vulnerabilities in internet e-voting systems: Hacking helios 2.0 as an example.," *EVT/WOTE*, vol. 10, pp. 1–9, 2010.

[13] J. A. Calandrino, A. J. Feldman, J. A. Halderman, D. Wagner, H. Yu, and W. P. Zeller, "Source code review of the diebold voting system," *University of California, Berkeley under contract to the California Secretary of State*, 2007.

[14] I. Goldberg and D. Wagner, "Randomness and the netscape browser," *Dr Dobb's Journal-Software Tools for the Professional Programmer*, vol. 21, no. 1, pp. 66–71, 1996.

[15] NIST, "FIPS 180-2: Secure hash standard," tech. rep., National Institute of Standards and Technology, NIST, U.S. Department of Commerce, Washington DC. `http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf`, 2002.

[16] X. Wang, Y. L. Yin, and H. Yu, "Finding collisions in the full SHA-1," in *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, vol. 3621 of *Lecture Notes in Computer Science*, pp. 17–36, Springer, 2005.

[17] W. Burr, "Nist comments on cryptanalytic attacks on sha-1." Disponível em: `http://csrc.nist.gov/groups/ST/hash/statement.html`, 2009.