REVISTA DE **EMPREENDEDORISMO, INOVAÇÃO E TECNOLOGIA**

Práticas educacionais no ensino da computação forense: um relato de experiência

Educational practices in teaching computer forensics: an experience report

Ricardo de la Rocha Ladeira(1); Rafael Rodrigues Obelheiro(2)

1 Instituto Federal Catarinense (IFC) - Campus Blumenau – Brasil. E-mail: ricardo.ladeira@ifc.edu.br.
2 Universidade do Estado de Santa Catarina (UDESC) – Brasil. E-mail: rafael.obelheiro@udesc.br

Revista de Empreendedorismo, Inovação e Tecnologia, Passo Fundo, vol. 4, n. 1 p. 110-120, Jan.-Jun. 2017 - ISSN 2359-3539

DOI: https://doi.org/10.18256/2359-3539/reit-imed.v4n1p110-120

Endereço correspondente / Correspondence address
Ricardo de la Rocha Ladeira
Rua Bernardino José de Oliveira, nº 81 - Blumenau – SC.
CEP: 89070-270

Como citar este artigo / How to cite item: clique aqui!/click here!

Resumo

Segurança Computacional e suas subáreas, tais como Computação Forense e Criptografia, são tópicos ainda pouco explorados no ensino formal. A desatualização dos currículos, o pouco espaço dedicado a estas áreas, a falta de abordagens pedagógicas específicas e de preparo de profissionais são alguns fatores que contribuem para este cenário. Como consequência, é pequeno o interesse dos estudantes por Segurança Computacional, ao passo que cresce a necessidade por profissionais com este conhecimento. Com o objetivo de diminuir esta lacuna, este artigo descreve um desafio forense proposto e aplicado no contexto de uma disciplina de Segurança Computacional em nível de graduação. Exigiu-se o uso da técnica Esteganografia para a conclusão do desafio, sem que qualquer instrução anterior sobre este tópico fosse fornecida. visando a observar se os estudantes conseguiriam avançar etapas de forma autônoma e sentir-se-iam entusiasmados com o trabalho proposto. A satisfação dos estudantes foi coletada após a realização da atividade, e o resultado sugere que a forma de ensino aplicada se mostrou motivadora e eficaz.

Palavras-chave: Computação Forense, Esteganografia, Ensino

Abstract

Cybersecurity and its subareas such as Forensic Computing and Cryptography are topics still poorly explored in formal education. Outdated curricula, lack of space dedicated to these areas, lack of specific pedagogical approaches and professional training are some factors that contribute to this scenario. As a consequence, students' interest in Cybersecurity is small while the need for professionals with this knowledge grows. In order to reduce this gap, this paper describes a forensic challenge proposed and applied in the context of a Computer Security course at the undergraduate level. Steganography technique was required to complete the challenge without previous instruction on these topic being provided, in order to see if students could progress independently and would be enthusiastic about the proposed work. After completing the activity, student satisfaction was collected, and the result suggests that the form of teaching applied was motivating and effective.

Keywords: Computer Forensics, Steganography, Learning

A Segurança Computacional tem um diferencial em relação a outros tópicos em Computação: boa parte dos problemas não é de concepção, mas de execução. Por exemplo, um desenvolvedor pode até usar programação defensiva, mas errar na hora de definir quantos caracteres serão copiados para um *buffer*. Do ponto de vista da explorabilidade da vulnerabilidade, a intenção é irrelevante, e é justamente essa dependência intrínseca da implementação que torna a abordagem prática essencial para um bom aprendizado de Segurança.

Agregar conhecimento prático em disciplinas de Segurança requer o enfrentamento de múltiplos obstáculos. Do ponto de vista cognitivo, as principais dificuldades incluem o pouco espaço dedicado ao tópico na maioria dos cursos de Computação (Weiss et al., 2015) e a necessidade de conhecer como diferentes abstrações computacionais (como arquiteturas em camadas e construções de linguagens de programação) são efetivamente implementadas, de modo a compreender melhor a superfície de ataque de um sistema (Bratus, 2007). Esse conhecimento específico é intrinsecamente complexo, ao passo que os currículos de Computação têm evoluído no sentido de minimizar a complexidade (Bratus, 2007). Isto cria uma barreira para que novos estudantes optem por se especializar na área. Uma subárea da Segurança que se encontra em crescimento, embora ainda não seja adequadamente vista nos currículos, é a Computação Forense – CF, que abrange técnicas para preservação, coleta e análise de evidências em recursos computacionais, relacionadas a crimes digitais. Sendo um tópico relativamente recente, a CF sente de forma mais aguda os desafios supracitados (Palmer et al., 2015).

A falta de um modelo pedagógico consolidado traz ainda a dificuldade no ensino da CF. Recursos e instrumentos precisam ser aplicados adequadamente com vistas ao aprendizado. Neste sentido, atividades práticas são essenciais na formação do discente, em especial em uma área em que evidências precisam ser descobertas, manipuladas e tratadas.

Uma possibilidade de atividade prática vem dos jogos, entre os quais destacam-se os de *videogame*, tabuleiro e desafios (Mirkovic et al., 2015). Estes jogos variam em assuntos abordados, público-alvo, complexidade e etc, sendo importante avaliar estes aspectos antes de aplicá-los no contexto educacional.

Do ponto de vista dos jogadores – no contexto educacional, os discentes –, os jogos do tipo desafio são frequentemente aplicados com dois objetivos: ganhar e aprender. Em um contexto de ensino formal o objetivo é aprender. Competições do tipo desafio, também chamadas de caça ao tesouro (ou *hunt treasure*) resumem-se em problemas que precisam ser resolvidos com processos e ferramentas, tipicamente sem interação com outros jogadores (neste caso, colegas). Estes desafios motivam os jogadores a encontrarem algum(ns) recurso(s) secreto(s). Por exemplo, um desafios forense pode consistir na descoberta de mensagens embutidas em pacotes de dados

capturados na rede. Estes jogos podem ser facilmente reproduzidos, uma vez que não exigem mais que um número limitado de ferramentas que possibilite sua solução, tais como o Wireshark, para análise de pacotes de rede, utilizado para resolver alguns desafios (Northcutt, 2016; Malwarewolf, 2015), editores hexadecimais e ferramentas esteganográficas.

O objetivo deste artigo é descrever a aplicação de um desafio para introduzir a temática de Computação Forense em uma disciplina de Segurança Computacional, apoiando docentes que queiram abordar o tema em suas aulas e visando a atrair talentos para as áreas de Cibersegurança e CF. Os resultados, discutidos na sequência do trabalho, indicam que experiências como o desafio aplicado são atividades lúdicas que permitem que os alunos aprendam sobre Criptografia e ferramentas e conceitos de CF, reduzindo a lacuna existente entre teoria e prática, e podem motivá-los a aprofundarem seus estudos na área.

O restante deste artigo está organizado como segue. A seção 2 discute a Computação Forense na Educação. A seção 3 descreve o desafio proposto, desde a sua criação até a sua aplicação e o retorno dos estudantes. apresenta os resultados de sua aplicação. A seção 4 conclui o artigo.

Computação forense na educação

Diante dos desafios de contribuir com a educação no Brasil, é urgente inserir temas cotidianos em cursos voltados às necessidades da população. Para indivíduos inseridos na Era da Informação, utilizar Tecnologias da Informação e Comunicação (TIC) nos processos de ensino e aprendizagem, ou, ainda, promover cursos desta área, podem ser facilitadores de aprendizagem, bem como propulsores de carreiras e motivadores para o desenvolvimento da criticidade e do protagonismo, considerando a educação como um elemento de transformação (Freire, 2005).

Nos cursos superiores de Tecnologia da Informação é imprescindível o ensino de assuntos relacionados à Segurança Computacional, tanto pelo citado caráter atual do tema quanto pela necessidade de profissionais nesta área. Porém, para atrair profissionais para a área, é importante promover o ensino através de metodologias que ofereçam eficácia pedagógica e incentivo ao discente. Uma forma motivadora para a introdução da Cibersegurança na educação formal é através de jogos e desafios.

Embora ainda não sejam largamente difundidas nos currículos dos cursos de TI, a inserção da Cibersegurança, da CF e das práticas não-tradicionais no ensino destas áreas tem ganhado espaço e aceitação dos discentes. Um dos motivos para isso pode ter relação com a falta de um modelo pedagógico consolidado (Yasinsac et al., 2003), embora já existam propostas para preencher essa lacuna (Palmer et al., 2015). Além disso, para que seja possível trabalhar na área, é necessário utilizar ferramentas

tecnológicas sofisticadas para preservar, extrair e analisar evidências digitais de forma apropriada (Pan et al., 2012). Ainda nesse sentido, há estudos na área envolvendo o uso de ferramentas *open-source* para ensino de Forense Digital (Manson et al., 2007; Fagundes et al., 2011).

Desafios forenses vêm sendo aplicados há alguns anos fora do contexto de sala de aula. Por exemplo, o Departamento de Defesa dos EUA promoveu entre 2006 e 2013 o DC3 Digital Forensics Challenge (Lacey et al., 2009), um desafio aberto a participantes de todo o mundo. Experiências no Brasil incluem a Campus Party[1], desde 2011, e o Workshop de Forense Computacional do SBSeg, em 2015[2]e 2016[3]. O público-alvo desses desafios, porém, não é bem definido ou controlado, incluindo alunos de graduação e pós-graduação e até mesmo profissionais. Além disso, não foram publicadas discussões sobre os efeitos didáticos dos desafios citados para estudantes de graduação. O aprendizado baseado em jogos para a Computação Forense está descrito em (Pan et al., 2012) com o desenvolvimento de um jogo voltado a estudantes de graduação cuja implantação ainda não foi divulgada.

Desafio proposto

O desafio foi idealizado como uma atividade envolvendo Esteganografia, área de estudo de técnicas para escrita oculta, e Criptografia, conjunto de técnicas que tornam um texto claro em ilegível (Petitcolas et al., 1999). Tal atividade visava à reprodução de comunicações em ambientes inseguros tais como as realizadas por terroristas e narcotraficantes na Internet (Terra, 2008; Secundino, 2013). A ideia era encaminhar um arquivo aos estudantes e um documento com o enunciado do desafio, de forma que os estudantes precisariam utilizar as técnicas mencionadas para obter as mensagens ocultas e cifradas.

Método de criação

A primeira decisão necessária para a criação do desafio dizia respeito ao tipo do meio de cobertura, ou seja, o tipo de arquivo que deveria esconder a mensagem secreta. Dada a grande quantidade de ferramentas de Esteganografia em imagens, optou-se por este tipo de arquivo, embora seja possível também esteganografar em áudio (Jayaram et al., 2011), vídeo (Chandel & Jain, 2016), texto (Agarwal, 2013) e em protocolos (Dhobale & Ghorpade, 2013). O passo seguinte consistiu em selecionar as ferramentas esteganográficas. Optou-se pelas ferramentas `f5.jar` e `Outguess`, por ambas

1 http://brasil.campus-party.org/

2 http://sbseg2015.univali.br/workshops/wfc

3 http://sbseg2016.ic.uff.br/

trabalharem com imagens de codificação JPEG e estarem disponíveis para Sistemas Operacionais *Unix-like*, utilizados nos laboratórios da instituição de ensino onde a atividade foi aplicada.

A proposta do desafio era esteganografar duas imagens dentro de uma terceira imagem, todas com formato JPEG. Para tanto, foram selecionadas três imagens de tamanhos diferentes, sendo uma maior (3872 x 2832 *pixels*), uma intermediária (800 x 600 *pixels*) e uma menor (200 x 120 *pixels*). A imagem menor foi esteganografada na imagem intermediária. Posteriormente a imagem intermediária, que já continha a imagem menor embutida, foi esteganografada na imagem maior. As imagens utilizadas no desafio são exibidas na Figura 1.

O tamanho das imagens é um fator importante, bem como a quantidade de cores, já que a porção de informação esteganografável é limitada pela técnica utilizada.

Figura 1. Miniatura das imagens (a) maior, (b) intermediária e (c) menor, utilizadas no desafio.
Fonte: Elaborado pelos autores.

Para que os alunos soubessem que havia mais de um nível de Esteganografia, a proposta não foi esteganografar diretamente uma imagem dentro da outra, mas codificá-la em Base64 (Josefsson, 2006), salvando o resultado em um arquivo de texto. Na sequência, este arquivo foi editado, recebendo também um texto que fornecia instruções ao estudante. O primeiro e o último texto gerado com as instruções estava em formato legível. No entanto, no segundo nível, para tornar a atividade mais desafiadora, o texto ainda estava criptografado com uma cifra de substituição monoalfabética, a Cifra de César (Bishop, 2002).

O processo reverso ao da criação permite resolver o problema, obtendo todos os arquivos escondidos, conforme mostra a Figura 2. A ferramenta necessária para o cumprimento de cada atividade do diagrama está indicada junto à seta de transição de um estágio a outro. Para resolver a atividade, os alunos não dispunham dos métodos de criação, devendo descobrir por conta própria a solução do desafio. Nesta etapa, forneceu-se aos estudantes apenas o estego-objeto final, ou seja, a imagem grande que incorporou as demais informações, e o citado documento[4] com o enunciado do desafio.

4 Disponível em: goo.gl/ke9RlN

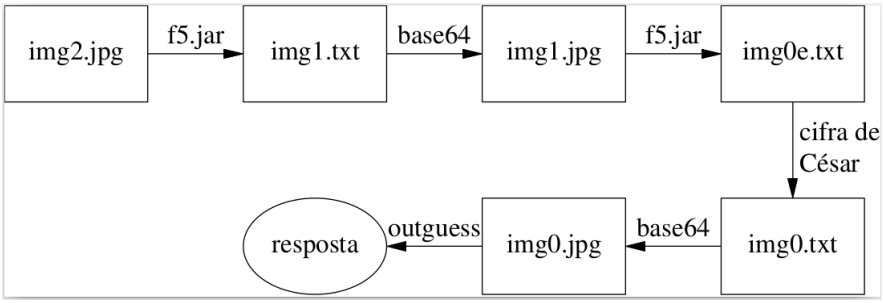

Figura 2. Fluxo para a resolução do desafio.
Fonte: Elaborado pelos autores.

Aplicação e retorno

A atividade foi realizada nos laboratórios do Instituto Federal Catarinense — Campus Blumenau, com duas turmas, nos dois semestres de 2016. A disciplina na qual a atividade foi desenvolvida é ministrada no sexto semestre do curso de Tecnologia em Análise e Desenvolvimento de Sistemas. Os discentes já possuíam, em termos de currículo, conhecimentos em Sistemas Operacionais, Redes de Computadores e Programação. Dentro da disciplina, alguns assuntos abordados antes da atividade proposta envolviam propriedades de Segurança da Informação, conceituação, criação e execução de *scripts* (inclusive maliciosos) e aspectos básicos de Criptografia.

Os estudantes não foram informados com antecedência sobre a atividade, pois a ideia era que tanto ela quanto o aprendizado se desenvolvessem durante a aula. Na primeira turma havia oito alunos, dos quais sete compareceram. Na segunda turma, os onze discentes matriculados compareceram. Cada estudante teve acesso à definição do desafio e teve a seu dispor um computador com Sistema Operacional *Unix-like* com as ferramentas necessárias para resolver a atividade.

Alguns estudantes tentaram encontrar mensagens observando a imagem, aproximando-a (*zoom*) ou alterando sua extensão. Outros abriram a imagem em editores de texto, o que já fornecia indícios do que deveria ser feito, pois a ferramenta `f5.jar` insere uma assinatura no arquivo, informando o nome do seu criador. Com esta informação, uma pesquisa na *web* já podia guiar os estudantes na resolução da primeira etapa. Para concluir as demais etapas, algum conhecimento em comandos de terminal e busca por outras ferramentas esteganográficas seriam necessários.

Alguns estudantes encontraram páginas que ensinavam a usar a ferramenta `f5.jar`, mas tiveram dificuldades em compreender que a ferramenta poderia extrair a mensagem esteganografada sem o uso de senhas. Houve um estudante que resolveu esta etapa inserindo uma senha padrão. Em um segundo momento, decodificar a mensagem em Base64 não foi simples aos discentes, mas alguns obtiveram êxito utilizando duas formas: comando de terminal (`base64`) e serviços online de codificação/decodificação.

A partir da segunda imagem obtida, nenhum estudante conseguiu avançar, embora o conteúdo de Criptografia tivesse sido visto em aulas anteriores. A mensagem cifrada com a Cifra de César não foi descoberta, mas alguns alunos chegaram perto disso tentando desvendá-la em páginas web que decifravam *rot13* (Cifra de César com chave igual a 13). A dificuldade em vencer esta etapa do desafio ilustra a lacuna entre teoria e prática observada no ensino de tópicos de Segurança Computacional, e reforça a importância de atividades que permitam torná-la cada vez menor.

Após realizarem a atividade e observarem a solução final[5], os estudantes foram convidados a responder um simples questionário com duas perguntas:

Com base na atividade realizada, responda:
1) A atividade foi motivadora?
2) Você conseguiu aprender sobre Esteganografia?

Nas duas turmas em que a atividade foi aplicada houve unanimidade nas respostas. A atividade foi considerada motivadora para todos os discentes. Ainda com base nas respostas, a temática Esteganografia foi apreendida por todos. A eficácia no aprendizado dos conceitos foi corroborada por um índice de acertos de 100% nas questões referentes à Esteganografia em provas teóricas aplicadas posteriormente, sustentando as respostas fornecidas no questionário.

Considerações finais

O trabalho relatou uma forma não tradicional de apresentar conceitos e ferramentas relacionados à Criptografia e Computação Forense, por meio de uma atividade de desafio envolvendo a técnica de Esteganografia, no contexto de uma disciplina de Segurança Computacional em um curso superior.

Os relatos dos estudantes envolvidos na atividade e as avaliações posteriores pressupõem que o objetivo foi alcançado. Embora nenhum estudante tenha conseguido resolver sozinho a atividade em sua totalidade, o interesse na resolução da tarefa, o retorno positivo sobre a prática, inclusive nas provas posteriores, e o entendimento sobre as ações realizadas indicam o efetivo valor pedagógico desta.

As propostas de continuidade do trabalho envolvem a aplicação de novos desafios em sala de aula, o aprimoramento do *feedback* dos alunos com a elaboração de um questionário com novas perguntas, o rastreamento do histórico de ações desenvolvidas no computador, balizando uma melhor identificação das dificuldades e o aproveitamento de outras técnicas de Computação Forense na criação de novos desafios. Pretende-se, ainda, desenvolver uma ferramenta de geração automática de

5 Disponível em: goo.gl/EWnQcy

desafios, envolvendo não apenas aspectos específicos de forense, mas enquadrados no contexto da Cibersegurança.

Agradecimentos

Os autores agradecem ao Instituto Federal Catarinense, por meio do Programa Institucional de Qualificação de servidores para o Instituto Federal Catarinense (PIQIFC), e à Universidade do Estado de Santa Catarina, que tornaram possível a realização deste trabalho.

Referências

Agarwal, M. (2013, Jan.) Text Steganographic Approaches: A Comparison. *International Journal of Network Security & Its Applications (IJNSA), 5*(1), 91-106.

Bishop, M. (2002). Computer Security: Art and Science. Addison-Wesley.

Bratus, S. (2007). What Hackers Learn that the Rest of Us Don't: Notes on Hacker Curriculum. *IEEE Security & Privacy, 5*(4), 72-75.

Chandel, B., & Jain, S. (2016). Video Steganography: A Survey. *IOSR Journals (IOSR Journal of Computer Engineering), 18*(1), 11-17.

Dhobale, D. D., & Ghorpade, V. R. (2013, Sept.). An Overview of Advanced Network Protocol Steganography. *International Journal of Advanced Research in Computer and Communication Engineering, 2*(9).

Fagundes, L., Neukamp, P., & Silva, P. (2011). Ensino da Forense Digital Baseado em Ferramentas Open Source. *In International Conference on Forensic Computer Science — ICoFCS 2011*, 5, 100-105.

Freire, P. (2005). Pedagogia do Oprimido. Rio de Janeiro: Paz e Terra, 42.a edição.

Jayaram, P., Ranganatha, H. R., & Anupama, H. S. (2011). Information Hiding Using Audio Steganography — A Survey. *The International Journal of Multimedia & Its Applications (IJMA), 3*, 86-96.

Josefsson, S. (2006). The Base16, Base32, and Base64 Data Encodings. RFC 4648, *Internet Engineering Task Force (IETF).*

Lacey, T. H., Peterson, G. L., & Mills, R. F. (2009). The Enhancement of Graduate Digital Forensics Education via the DC3 Digital Forensics Challenge. In Proc. HICSS'09.

Malwarewolf. Network Forensics – Round 1: Ann's Bad AIM. (2015). Disponível em: <https://malwerewolf.com/2015/03/network-forensics-round-1-anns-bad-aim/>. Acesso em: 26 nov. 2016

Manson, D., Carlin, A., Ramos, S., Gyger, A., Kaufman, M., & Treichelt, J. (2007). Is the Open Way a Better Way? Digital Forensics using Open Source Tools. In *Proc. HICSS'07.*

Mirkovic, J., Dark, M., Du, W., Vigna, G., & Denning, T. (2015, May-June) Evaluating Cybersecurity Education Interventions: Three Case Studies. *IEEE Security & Privacy, 13*(3), 63-69.

Northcutt, S. (2016). What the PCAP contest actually tells us. Disponível em: https://www.linkedin.com/pulse/what-pcap-contest-actually-tells-us-stephen-northcutt. Acesso em: 26 abr. 2016.

Palmer, I., Wood, E., Nagy, S., Garcia, G., Bashir, M., & Campbell, R. (2015). Digital Forensics Education: A Multidisciplinary Curriculum Model. In *International Conference on Digital Forensics and Cyber Crime*, 3-15.

Pan, Y., Mishra, S., Yuan, B., Stackpole, B., & Schwartz, D. (2012). Game-based Forensics Course for First Year Students. In *Proc. 13th Annual Conference on Information Technology Education* (SIGITE '12), 13-18.

Petitcolas, F., Anderson, R.J., & Kuhn, M.G. (1999). Information Hiding - A Survey. *Proceedings of the IEEE, 87*(7), 1062-1078.

Secundino, A. A. (2013). Um estudo sobre abordagens computacionais de esteganografia e esteganálise em imagens. Trabalho de Conclusão de Curso. Universidade Federal de Juiz de Fora, Juiz de Fora. Disponível em: http://monografias.nrc.ice.ufjf.br/tcc-web/exibePdf?id=109. Acesso em 8 set 2016.

Terra. Abadia usava Hello Kitty para enviar ordens. 2008. Disponível em: http://noticias.terra.com.br/brasil/noticias/0,,OI2666590-EI5030,00- Abadia+usava+Hello+Kitty+para+enviar+ordens.html. Acesso em 8 set 2016.

Weiss, R.S., Boesen, S., Sullivan, J.F., Locasto, M.E., Mache, J., & Nilsen, E. (2015). Teaching Cybersecurity Analysis Skills in the Cloud. In *Proc. SIGCSE'15,* 332-337.

Yasinsac, A., Erbacher, R.F., Marks, D.G., Pollitt, M.M., & Sommer, P.M. (2003). Computer Forensics Education. *IEEE Security & Privacy, 1*(4), 15-23.