Uma Análise sob a Ótica de Simulação do Eixo Segurança de Software do Referencial de Formação do Curso de Bacharelado em CiberSegurança

Emanuel F. Coutinho

Programa de Pós-Graduação em Computação (PCOMP)
Universidade Federal do Ceará (UFC) – Quixadá – CE – Brasil

emanuel.coutinho@ufc.br

Abstract. *With the increasing integration of digital resources, devices and physical systems, a need for training and qualification arises. In this context, Bachelor's Degree courses in Cybersecurity emerge. According to the Training References for Bachelor's Degree courses in Cybersecurity, eight training axes were proposed. This article aims to discuss some aspects of how simulation can collaborate and support the Software Security axis of the Training Reference for the Bachelor's Degree Course in Cybersecurity.*

Resumo. *Com a crescente integração de recursos digitais, dispositivos e sistemas físicos, surge uma necessidade de formação e capacitação. Nesse contexto, cursos de Bacharelado em Cibersegurança emergem. Conforme os Referenciais de Formação dos cursos de Bacharelado em Cibersegurança, oito eixos de formação foram propostos. Esse artigo visa discutir alguns aspectos de como a simulação pode colaborar e apoiar o eixo Segurança de Software do Referencial de Formação do Curso de Bacharelado em Cibersegurança.*

1. Introdução

A rápida evolução da tecnologia e a crescente dependência tecnológica de empresas e serviços traz consigo uma preocupação: a cibersegurança [Alawida et al. 2022]. A tendência crescente de integração de recursos digitais (incluindo conectividade de rede e capacidade computacional) com dispositivos e sistemas físicos, tem resultado na ampla disseminação da Internet das Coisas (IoT) e Sistemas Ciber-Físicos (CPS), nas mais diversas áreas de aplicação [Greer et al. 2019]. Isso pode implicar na necessidade de formação e capacitação. Os Referenciais de Formação para os cursos de Bacharelado em CiberSegurança estão em consonância com as Diretrizes Curriculares Nacionais (DCN2016), homologadas em novembro de 2016, por meio da Resolução Nº 05 de 16/11/2016 [MEC 2016]. O Bacharelado em CiberSegurança é considerado um curso da área de Computação [SBC 2023].

A área de CiberSegurança tem a necessidade de profissionais com formação integral, mais ampla e profunda no tema. Em particular, a formação na área deve contemplar os eixos de dados, software, componentes, conexões, sistemas, pessoas, organizações e sociedade, todos elementos essenciais que compõem o ecossistema computacional moderno [SBC 2023]. Os termos "sistemas ciberfísicos", ou "CPS", e "Internet das Coisas", ou "IoT", têm origens distintas, mas definições sobrepostas, sendo que ambos se referem a tendências na integração de capacidades digitais, incluindo conectividade de rede e

capacidade computacional, com dispositivos e sistemas físicos [Greer et al. 2019]. Exemplos variam de veículos inteligentes a sistemas avançados de manufatura, em setores tão diversos como energia, agricultura, cidades inteligentes e muito mais.

A educação na área de CiberSegurança tem crescido consideravelmente nas últimas décadas [SBC 2023]. Porém, a sua necessidade como uma área autônoma é frequentemente desconsiderada ou negligenciada como um fator crítico de sucesso, ao desenvolver um quadro de profissionais necessários na sociedade para proteger seus ativos. Recentemente, entidades internacionais relevantes na área de CiberSegurança passaram a promover iniciativas voltadas à educação específica envolvendo essas habilidades, como o NIST, NSA e ENISA. Existe um consenso que enfrentar os desafios de ensino em CiberSegurança deve ser uma prioridade para a segurança da sociedade.

Profissionais de CiberSegurança devem possuir competências teórica, técnica e metodológica, além de experiência prática para lidar com variadas situações e domínios de aplicação [SBC 2023]. Assim, as simulações podem atuar como aliados na compreensão do comportamento, dos riscos e também dos impactos de ciberataques [Nunes et al. 2024]. Para promover a proficiência na área, o curso requer um conteúdo que inclua conhecimento teórico essencial para desenvolver competências técnicas que apoiam a aplicação deste conhecimento, que para os egressos dos Cursos de Bacharelado em CiberSegurança, foram agrupados em oito eixos de formação: Segurança de Dados, Segurança de Sistemas, Segurança de Conexão, Segurança de Software, Segurança de Componentes, Segurança Organizacional, Fatores Humanos em Segurança e Segurança e Sociedade. A proposta desse artigo visa discutir alguns aspectos de simulação sobre o Referencial de Formação do Curso de Bacharelado em CiberSegurança, em particular o eixo Segurança de Software, buscando a disseminação das áreas envolvidas para a sociedade.

2. Eixo de Formação Segurança de Software

O eixo de Segurança de Software aborda o desenvolvimento e uso de software que preserva confiavelmente as propriedades de segurança da informação e sistemas que a protegem [SBC 2023]. A Segurança do Software depende da aderência dos requisitos às necessidades do software e da qualidade do desenvolvimento, implementação, testes, manutenção e documentação. Possui como conhecimentos essenciais: princípios fundamentais de projeto incluindo o privilégio mínimo, especificação aberta, separação de responsabilidade, validação de entradas; requisitos de segurança e seus papéis no projeto; aspectos de implementação; análise estática e dinâmica de código em testes de software; gerenciamento de configuração e correção de software; ética, especialmente no desenvolvimento, testes e divulgação de vulnerabilidade. O eixo possui como competência empregar técnicas seguras no ciclo de desenvolvimento de software, e é dividido em competências derivadas. A Tabela 1 lista para cada competência derivada do eixo seus conteúdos.

3. Análise das Competências Derivadas com Simulação

3.1. Usar técnicas e princípios fundamentais de software seguro

Fundamentos e teorias relacionadas ao desenvolvimento de software seguro são necessários para um bom desenvolvimento. E compreender os fundamentos auxilia a desenvolver estratégias para simular cenários e projetar ferramentas. O desenvolvimento de

Tabela 1. Competências derivadas e conteúdos [SBC 2023]

Competências Derivadas	Conteúdos
C.4.1. Usar técnicas e princípios fundamentais de software seguro	Princípio do Mínimo Privilégio; Princípio de Falhas-Seguras (fail-safe) por Padrão; Princípio da Mediação Completa (Evitando Contorno de Controle); Princípio de Separação de Deveres; Princípios da Confiança Mínima e Confiança Zero; Princípio da Simplicidade do Software; Vantagens e Desvantagens de Segurança em Projeto Aberto; Desenvolvimento em Camadas, Modular e Componentizado; Segurança por Projeto
C.4.2. Praticar princípios fundamentais de projeto de segurança de software	Integração de Segurança no Ciclo de Desenvolvimento de Software; Linguagens de Programação Projetadas para Segurança
C.4.3. Empregar boas práticas de desenvolvimento seguro	Validação de Entradas e Verificação do que Representam; Uso Correto de API; Uso Correto de Mecanismos de Segurança; Garantia de Estados Consistentes dos Softwares; Manipulação Correta de Erros e Exceções; Programação Defensiva; Encasulamento Adequado de Estruturas e Módulos; Avaliação de os Riscos Externos ao Software em Tempo de Execução
C.4.4. Desenvolver análise e testes de segurança	Análise Estática da Segurança do Código; Análise Dinâmica da Segurança do Código; Teste Unitário de Segurança; Teste de Integração de Segurança; Teste de Segurança de Software
C.4.5. Empregar conceitos de segurança na implantação, manutenção e documentação de software	Configuração de Segurança; Atualização e Ciclo de Vida de Vulnerabilidades; Análise de Compatibilidade do Ambiente e Requisitos de Segurança do Software; Impactos de Segurança na Descontinuidade (Descomissionamento) de Software; Desenvolvimento, Operação e Segurança Integrados (DevSecOps); Documentação de Segurança

software em camadas é comum, e incorporar segurança se torna uma boa prática. Uma ação de simulação pode ser a análise do impacto em camadas e entre camadas, o que pode ser utilizado para estudar conceitos, técnicas e princípios de software seguro.

Simular situações relacionadas a princípios como Separação de Deveres, Confiança Mínima e Confiança Zero são ações de segurança que podem prevenir fraudes e erros por meio da divisão de tarefas e responsabilidades, pelo questionamento da confiança em usuários e sistemas. Tais ações visam proteger recursos com verificações constantes e controles de acesso e provilégios.

3.2. Praticar princípios fundamentais de projeto de segurança de software

Modelos de simulação são frequentemente codificados (ou pelo menos podem ser traduzidos) em linguagens de programação de simulação [França and Neto 2021]. Nesse contexto, é necessário que além dos requisitos funcionais e não funcionais tradicionalmente elicitados e especificados, que se reforce a visão de requisitos de segurança, desde o nível de código, integração, sistema e usuário. Exemplos de requisitos de segurança são: confidencialidade (ex. criptografia de dados), integridade (ex. checksums, assinaturas digitais), e disponibilidade (ex. proteção contra DDoS).

Outro aspecto é a incorporação de segurança em todos o ciclo de desenvolvimento do software, e não apenas na aplicação. Todo o processo deve considerar segurança de dados e código. Processos também devem considerar segurança. Por fim, as linguagens de programação também devem ter mecanismos de segurança, de forma que possam prover aplicações projetadas para segurança. Isso envolve código, APIs, interfaces, etc.

É fundamental haver abordagens que permitam investigar a natureza e o comportamento de ciberataques, desde a sua motivação, vulnerabilidades, estratégias de defesa e também potenciais impactos socioeconômicos [Figueredo Franco et al. 2022].

3.3. Empregar boas práticas de desenvolvimento seguro

Para o desenvolvimento de software de maneira geral, boas práticas são sempre bem vindas. Padrões, exemplos, ferramentas podem colaborar para que o desenvolvimento se torne mais seguro. E nesse contexto, a simulação pode auxiliar bem. O estudo e uso de APIs na busca de falhas de segurança, possíveis falhas de código, detecção de problemas na integridade de dados pode se beneficiar de simulações. A combinação de software e hardware, e a combinação de diversas camadas de segurança desde os níveis mais baixos do desenvolvimento até canadas de usuário também pode ser simulado. UM exemplo é a utilização de mecanismos de manipulação de erros e exceções, e como eles se propagam

no sistema, além de seus impactos em tempo de execução. A correta e segura definição de interfaces também devem ser observadas e possivelmente simuladas para refinamento.

Modelos de simulação e software são abstrações de um sistema pretendido [França and Neto 2021]. Dependendo da escala do modelo de simulação, a manutenibilidade, a reutilização e outros atributos de qualidade tornam-se uma preocupação. Portanto, técnicas e métodos de modularização, separação de interesses, reutilização e composição de modelos também são necessários para modelos de simulação.

3.4. Desenvolver análise e testes de segurança

Esses procedimentos poderiam ser aprimorados com técnicas e critérios de teste de software já estabelecidos na literatura de Engenharia de Software [França and Neto 2021]. Análise de códigos do ponto de vista estático e dinâmico podem ser avaliados, e simuladas situações de falhas ou pontos a serem melhorados. Os testes podem ocorrer desde o nível unitário, integração e sistêmicos, e seus efeitos podem ser avaliados quando perpetuados. Por outro lado, testes de desempenho, robustez e segurança podem se beneficiar de modelos de simulação para gerar cargas de requisições, simulando entradas e ataques maliciosos para auxiliar na verificação de software.

Relatos de ações maliciosas explorando vulnerabilidades não são raros. Por exemplo, os dispositivos médicos com uso intensivo de Internet das Coisas (IoT) possuem sistema operacional embarcado com baixo poder computacional e criptográfico. Assim, são facilmente alvos de *malware* injetáveis [Lelis et al. 2020]. As simulações podem ajudar na avaliação de cenários de ataques, invasões e negações de serviços.

3.5. Empregar conceitos de segurança na implantação, manutenção e documentação de software

Simulações para analisar os efeitos de vulnerabilidades durante o ciclo de vida de desenvolvimento. Como simular vulnerabilidades e suas respectivas documentações Simulação dos efeitos da descontinuidade de software DevSecOps é a integração da segurança em todas as fases do ciclo de vida de desenvolvimento de software, unindo desenvolvimento, segurança e operações.A simulação da integração dessas áreas

Ambientes de teste para estudar novos tipos de ataque, para testar vulnerabilidades em sistemas e protocolos ou para validar recursos de defesa, tipicamente são escassos, limitados em termos de escalabilidade ou complexos no que tange a preparação dos cenários de cibersegurança [Rahouti and Xiong 2019]. Diversos ambientes de simulação, emulação e experimentação têm sido utilizados para realizar experimentos e aplicar práticas de ensino em redes [Gomez et al. 2023].

4. Considerações Finais

A área de Cibersegurança possui diversos aspectos de software e hardware. Ambos se unem para focar na segurança de aplicações e usuários. Neste cenário, profissionais são necessários para atender a esses aspectos. A simulação é uma abordagem que vem para colaborar com a Cibersegurança, podendo trazer diversos benefícios e oportunidades.

De maneira geral, pretende-se com esta pesquisa atender aos seguintes itens: (i) Ampliar a disseminação da área de simulação, especificamente voltada para software,

em um curso emergente; (ii) Formação de profissionais que possam utilizar recursos de simulação em suas atividades visando segurança em software; e (iii) Desenvolvimento de novas tecnologias de simulação mais direcionadas para Cibersegurança.

Neste artigo, apenas se analisou o eixo Segurança de Software, sendo necessário avaliar todos os demais sete eixos, e compreender melhor como simulações podemo colaborar para a melhoria do referencial e da formação de profissionais em Cibersegurança.

Referências

Alawida, M., Omolara, A. E., Abiodun, O. I., and Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, 34(10, Part A):8176–8206.

Figueredo Franco, M., Martins Lacerda, F., and Stiller, B. (2022). Um framework para planejamento e gerenciamento de projetos de cibersegurança em pequenas e médias empresas. *Revista de Gestão e Projetos*, 13(3):10–37.

França, B. and Neto, V. G. (2021). Opportunities for simulation in software engineering. In *Anais do III Workshop em Modelagem e Simulação de Sistemas Intensivos em Software*, pages 50–54, Porto Alegre, RS, Brasil. SBC.

Gomez, J., Kfoury, E. F., Crichigno, J., and Srivastava, G. (2023). A survey on network simulators, emulators, and testbeds used for research and education. *Computer Networks*, 237:110054.

Greer, C., Burns, M., Wollman, D., and Griffor, E. (2019). Cyber-physical systems and internet of things. https://doi.org/10.6028/NIST.SP.1900-202. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD.

Lelis, C., Pereira, L., and Marcondes, C. (2020). Uma abordagem de detecção de atividade maliciosa em ambientes hospitalares. In *Anais do XX Simpósio Brasileiro de Computação Aplicada à Saúde*, pages 380–391, Porto Alegre, RS, Brasil. SBC.

MEC (2016). Diretrizes curriculares nacionais para os cursos de graduação em computação - resolução cne/ces nº 5, de 16 de novembro de 2016. http://portal.mec.gov.br/index.php?option=com_docman&view=download&alias=52101-rces005-16-pdf&category_slug=novembro-2016-pdf&Itemid=30192. Acesso: 06/05/2025.

Nunes, J., Franco, M., Scheid, E., Kozenieski, G., Lindemann, H., Soares, L., Nobre, J., and Granville, L. (2024). Sim-ciber: Uma solução baseada em simulações probabilísticas para quantificação de riscos e impactos de ciberataques utilizando relatórios estatísticos. In *Anais do XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 570–585, Porto Alegre, RS, Brasil. SBC.

Rahouti, M. and Xiong, K. (2019). A customized educational booster for online students in cybersecurity education. In *Proceedings of the 11th International Conference on Computer Supported Education - Volume 2: CSEDU*. INSTICC, SciTePress.

SBC (2023). Referenciais de formação para o curso de bacharelado em cibersegurança. https://doi.org/10.5753/sbc.ref.2023.125. Acesso: 06/05/2025.