Os Desafios de Cibersegurança dos Referenciais do BCS/SBC

Aldri Santos (UFMG)[1], Altair Santin (PUCPR)[1], André Grégio (UFPR)[1], Carlos Raniery (UFSM)[1], Daniel Batista (USP)[1], Dianne Medeiros (UFF)[1], Diego Kreutz (UNIPAMPA)[1], Diogo Mattos (UFF)[1], Edelberto Franco (UFJF)[1], Igor Moraes (UFF)[1], Lourenço Pereira Jr. (ITA)[1], Marcos Simplicio (USP)[1], Michele Nogueira (UFMG)[1], Michelle Wangham (Univali/RNP)[1], Natalia Fernandes (UFF)[1], Rodrigo Miani (UFU)[1]

[1]Comissão Especial de Cibersegurança - Sociedade Brasileira de Computação (CESeg)

Abstract. *This document describes the main research and innovation challenges in the area of cybersecurity. The content builds upon education as a key element: it is organized into eight pillars, comprising the main areas listed in the Cybersecurity Curricular Guideline, published by the Brazilian Computer Society as a guide to inspire the creation of courses to train qualified personnel. The result is a comprehensive set of research topics addressing crucial cybersecurity needs in contemporary computer systems.*

Resumo.
Este documento descreve os principais desafios de pesquisa e inovação na área de cibersegurança. O conteúdo toma por base a educação como elemento-chave: ele se organiza em oito pilares, cobrindo as principais áreas elencadas nos Referenciais de Formação do Curso de Bacharelado em Cibersegurança (RF-CS), documento publicado pela Sociedade Brasileira de Computação como um guia para inspirar a criação de cursos para a formação de pessoal qualificado na área. O resultado é um conjunto abrangente de tópicos de pesquisa que abordam necessidades cruciais de cibersegurança em sistemas computacionais contemporâneos.

1. Introdução

O *déficit* estimado de profissionais de Cibersegurança apenas no Brasil é de 750 mil[1]. Em 2023, a comissão de educação da Comissão Especial de Cibersegurança (CE-Seg) da Sociedade Brasileira de Computação (SBC) publicou os Referenciais de Formação do Curso de Bacharelado em Cibersegurança (RF-CS) [SBC, 2023], que busca guiar a formação de profissionais em Cibersegurança, área crítica na Era da Informação atual, por meio de 8 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. Dado que os eixos do RF-CS cobrem amplamente a área de Cibersegurança, este documento resume como os desafios da área podem ser divididos em temas de pesquisa, a fim de direcionar eventuais ações de colaboração entre academia, indústria e sociedade para lidar com aspectos relevantes de pesquisa em cibersegurança no Brasil e no mundo.

[1]Disponível em `https://www.fortinet.com/content/dam/fortinet/assets/reports/pt_br/2024-cybersecurity-skills-gap-report.pdf`.

2. O Desafio da Cibersegurança

O grande desafio da ciberseguraça no Brasil é detalhado em oito eixos temáticos, conforme definido pelo RF-CS da SBC. Os desafios de cada eixo são detalhados a seguir.

2.1. Segurança de Dados

Mitigar a ameaça da computação quântica é um dos principais desafios no eixo de Segurança de Dados, que trata da proteção de dados armazenados, em processamento e em trânsito. A razão é que computadores quânticos de grande porte podem obter chaves privadas dos principais esquemas criptográficos usados na Internet atualmente. Uma solução para esse problema é a chamada criptografia pós-quântica (*post-quantum cryptography* - PQC). O NIST lançou um processo de padronização de algoritmos criptográficos pós-quânticos. Apesar desse avanço, desafios importantes permanecem tanto para os esquemas já padronizados como para possíveis alternativas, considerando métricas de segurança, desempenho e flexibilidade. Em especial, destacam-se como áreas de pesquisa: (1) análise de segurança dos esquemas, cobrindo aspectos teóricos e de implementação (2) a otimização dos algoritmos, considerando técnicas de projeto e de implementação, para reduzir o uso de recursos a níveis mais próximos dos algoritmos clássicos; (3) a adaptação de soluções existentes para uso de PQC. Uma alternativa consiste no uso de tecnologias de comunicação quântica. Especificamente, aproveitando as propriedades físicas dos meios de comunicação, há a possibilidade de se fazer a distribuição de chaves secretas (*quantum key distribution* – QKD) entre usuários com garantias de que elas não foram capturadas durante a transmissão [Cao et al., 2022]. Nesse caso, embora métricas de segurança, desempenho e flexibilidade também se apliquem, um desafio da QKD em comparação a PQC é a ausência de padrões de QKD bem definidos e amplamente adotados.

2.2. Segurança de Sistemas

O eixo de Segurança de Sistemas é abrangente e inclui a integração entre componentes de hardware, software, infraestrutura de comunicação e sub-sistemas. Os principais desafios atuais são o uso de Inteligência Artificial (IA) e Ciência de Dados para auxiliar neste eixo. O uso de IA para cibersegurança é um tema explorado há tempos na automação de tarefas de monitoramento e detecção de ataques, geração de traços de auditoria, imposição de controles de segurança, análise de vulnerabilidades em software etc. Além disso, técnicas de ciência de dados são úteis para lidar com processamentos complexos envolvendo diversas fontes, volumes e velocidades de dados. Por outro lado, a aplicação de cibersegurança para sistemas de IA é uma área emergente, levando a conceitos como Aprendizado de Máquina em Contexto Adversário e Aprendizado de Máquina Seguro [Vassilev et al., 2024]. Desafios da área incluem: (i) mitigação dos efeitos do uso de IA por parte dos atacantes (por exemplo, para evadir sistemas inteligentes, roubar modelos, envenenar bases de dados públicas usadas na modelagem de IA, e praticar violações éticas, de privacidade de usuários e de direitos autorais); (ii) aplicação correta (eficiente, eficaz, ética e adequada) das técnicas de IA considerando a heterogeneidade dos dados de segurança (*streams*, dados discretos, múltiplos formatos etc.); (iii) consolidar os resultados do processamento inteligente distribuído de grandes massas de dados provenientes de redes de altíssima velocidade, com criptografia e formatos/fontes/protocolos variados para detecção e prevenção de ataques em tempo quase real.

2.3. Segurança de Conexão

Este eixo contempla as interligações lógicas e físicas entre componentes computacionais, cujos desafios de cibersegurança são em grande parte fruto da constante evolução das tecnologias de comunicação.Enquanto a implantação das redes além do 5G (*Beyond* 5G - B5G) prometem melhorias contínuas em métricas como taxas de transmissão e latência, isso também exige a tomadas de decisões de segurança autônomas, capazes de lidar com a conexão de bilhões de dispositivos e aplicações de forma transparente, resiliente e com garantia de desempenho. Este desafio arquitetural pode ser endereçado por meio de abordagens altamente flexíveis, baseadas em virtualização e softwarização de redes, como as redes de acesso via rádio abertas (Open RAN). Contudo, a abertura de interfaces e o uso de *software* de código-fonte de diversas fontes distintas aumenta a superfície de ataque a esses sistemas. Uma linha de pesquisa relevante nesse contexto tem como foco a proteção contra abuso e o acesso indevido a informações em redes B5G, usando princípios de segurança por projeto. Comumente, soluções na camada de controle dessas redes envolvem tecnologias descentralizadas e com elevado grau de transparência, buscando promover o modelo de "arquitetura de confiança zero" (*Zero-Trust Architecture* – ZTA). Logo, é importante medir a dependência das soluções por entidades confiáveis e a existência de pontos críticos de falha, e se são capazes de prover mecanismos eficientes para autenticação de entidades e preservação de privacidade dos dados. Na camada física, o gerenciamento de espectro e de recursos é fundamental para assegurar disponibilidade e permitir a detecção e isolamento eficiente de ameaças [Ramezanpour e Jagannath, 2022].

2.4. Segurança Organizacional, Segurança e Sociedade & Fatores Humanos

O eixo de Segurança Organizacional lida com a proteção de organizações contra ameaças e gestão de riscos de segurança. O eixo de Segurança e Sociedade aborda cibercrimes, privacidade e aspectos legais, éticos e políticos. Finalmente, eixo de Fatores Humanos em Segurança concentra-se na proteção de dados em contexto pessoais e corporativos. O ponto em comum entre esses eixos é o foco na interação de indivíduos com sistemas: as decisões e comportamentos por eles adotados tornam-se um ponto crítico para a cibersegurança e, portanto, compreendê-los é essencial para construir mecanismos de proteção eficientes [Pollini et al., 2022]. Por exemplo, ataques de engenharia social exploram diretamente as emoções e instintos humanos para ludibriá-los, afetando alvos específicos ou toda uma cadeia de suprimentos, como o incidente ocorrido com a biblioteca *XZ Utils* [Buchanan, 2024] em que atacantes se infiltraram como mantenedores do repositório para inserir portas dos fundos em duas versões da biblioteca. Lidar com tais desafios requer uma abordagem holística que combine educação, conscientização e tecnologia. A pesquisa na área envolve o desenvolvimento de ações e programas para melhorar o letramento digital dos usuários e sua postura de segurança. A efetividade de soluções deve ser medida pela sua capacidade de levar usuários a reconhecer e evitar cenários de ameaça, como tentativas de engenharia social, e diferenciar fatos de dados falsos. Para desenvolver esse pensamento crítico, são necessárias estratégias de comunicação eficientes, que, além de mostrar como implementar medidas de segurança, expliquem o racional envolvido, permitindo ao usuário lidar com cenários de ataque cada vez mais complexos.

2.5. Segurança de Software e Segurança de Componentes

O eixo de Segurança de Software se concentra no desenvolvimento e o uso de software de modo a garantir propriedades de segurança na aplicação-alvo, incluindo con-

ceitos de programação segura. O eixo de Segurança de Componentes trata do projeto, aquisição, teste, análise e manutenção de componentes de hardware. Em ambos, um tema desafiador é a proteção contra ataques na cadeia de suprimentos. O pano de fundo desse desafio é o fato de que sistemas computacionais modernos geralmente envolvem componentes de vários fornecedores especializados. No cenário com diferentes fornecedores, a falha em um elo da cadeia pode levar a impactos negativos expressivos. No caso de hardware, a potencial adulteração de componentes por meio de modificação de firmware permite ataques lógicos e físicos de difícil detecção. Esse risco é ilustrado pela explosão remota de dispositivos de comunicação usados pelo grupo Hezbollah, ação que envolveu a inserção de elementos estranhos ao sistema na sua fabricação [BBC News, 2024]. Questões similares aparecem na cadeia de produção de software, como ilustra o já mencionado caso da biblioteca *XZ Utils* [Buchanan, 2024]. Ainda, para evitar falhas não propositais, é necessária a incorporação de segurança no processo contínuo de desenvolvimento, integração e implantação.Para isso, é importante modelar adversários e usar adequadamente arcabouços que ajudam a retratar fidedignamente a realidade de cada aplicação. Para aferir se esse princípio está sendo respeitado, algo especialmente necessário em sistemas de controle industrial e de missão crítica, deve-se considerar o desenvolvimento de técnicas e ferramentas que facilitem verificabilidade e auditabilidade. No contexto de hardware, algumas estratégias incluem a adoção de protocolos de atestação de componentes [Cremers et al., 2023] e do conceito de *open hardware* na construção de sistemas complexos [Emanuilov, 2020]. Para os casos de computação de propósito geral, como em nuvem computacional, componentes de hardware confiáveis podem fazer parte da solução, ao permitir a construção de ambientes de execução confiável (TEE) [Muñoz et al., 2023]. No cenário de software, há a necessidade de soluções que permitam validar atualizações, melhorando a capacidade de detecção de vulnerabilidades para além do que fazem hoje ferramentas de análise estática e dinâmica de código. Métricas para avaliar o quão próximo se está da solução para esse desafio incluem: variedade e grau de adoção de soluções que melhorem a auditabilidade de hardware e software, permitindo a proteção de um amplo conjunto de sistemas; a facilidade de integração de mecanismos de proteção e verificação na cadeia de suprimentos; e a maturidade das tecnologias disponíveis, avaliado pelo número e gravidade das vulnerabilidades descobertas ao longo do tempo.

3. Considerações Finais

Este documento apresentou os grandes desafios da Cibersegurança organizado conforme os eixos de formação definidos no RF-CS da SBC. O eixos têm focos distintos, mas o desafio comum a todos é a Educação em Cibersegurança. É cada vez mais urgente atrair para a área profissionais de diferentes perfis, com formação desde ensino médio e técnico até mestrado e doutorado. A definição do RF-CS e o atual processo de sua transformação em Diretrizes Curriculares Nacionais pelo Conselho Nacional de Educação, que possibilita a abertura de cursos de graduação na área, é uma ação de médio e longo prazo para tratar a carência de profissionais em cibersegurança. Organizar competições temáticas com viés educativo e disponibilizar cursos sobre cibersegurança nos canais da SBC e CESeg podem ser medidas de curto prazo para atrair e capacitar pessoas. Ações de curto prazo, como o programa Hackers do Bem, devem ser uma prioridade e ajudam a desenvolver a área. Porém, políticas de Estado com planejamento de médio e longo prazo, especialmente para a educação em cibersegurança, devem ser um alvo de investimentos do país, incluindo incentivos para parcerias com a indústria. O custo das certificações

profissionais é bastante elevado e o Estado brasileiro poderia estabelecer parceiras sociais e de inclusão para estes casos também. É preciso formar professores em cursos de licenciatura visando a educação dos jovens nas boas práticas de segurança e privacidade no uso da tecnologia. A não priorização de cibersegurança pode causar prejuízos financeiros e à imagem, ameaçando a democracia, o direito à privacidade e as liberdades civis.

Referências

BBC News (2024). Como pagers do Hezbollah explodiram, em ataque atribuído ao Mossad. https://www.bbc.com/portuguese/articles/ce8vxg1xgx3o.

Buchanan, B. (2024). The social engineering of XZ. https://medium.com/asecuritysite-when-bob-met-alice/the-social-engineering-of-xz-f905084438fc.

Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. e Hanzo, L. (2022). The evolution of quantum key distribution networks: On the road to the Qinternet. *IEEE Communications Surveys & Tutorials*, 24(2):839–894.

Cremers, C., Dax, A. e Naska, A. (2023). Formal analysis of SPDM: Security protocol and data model version 1.2. Em *USENIX Security Symposium*, p. 6611–6628.

Emanuilov, I. (2020). Security through transparency and openness in computer design. Em *Int. Conf. on Risks and Security of Internet and Systems*, p. 105–116. Springer.

Muñoz, A., Rios, R., Román, R. e López, J. (2023). A survey on the (in) security of trusted execution environments. *Computers & Security*, 129:103180.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F. e Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, 24(2):371–390.

Ramezanpour, K. e Jagannath, J. (2022). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Computer Networks*, 217:109358.

SBC (2023). Referenciais de formação para o curso de bacharelado em cibersegurança. Relatório técnico, Sociedade Brasileira de Computação (SBC).

Vassilev, A., Oprea, A., Fordyce, A. e Anderson, H. (2024). Adversarial machine learning: A taxonomy and terminology of attacks and mitigations. Relatório técnico, National Institute of Standards and Technology.