Nome: Davi Cândido de Almeida

Matrícula: 857859

Nome: Lucas Carneiro Nassau Malta

Matrícula: 857340

Tema escolhido: Práticas de Segurança aplicadas no desenvolvimento de Software

<u>Conferências:</u>

- ACM ASIA Symposium on Information, Computer and Communications Security (A1): ACM Digital Library

  Título do Artigo: SweetPAKE: Key exchange with decoy passwords

  Autores: Afonso Arriaga, Peter Y. A. Ryan e Marjan Škrobot

  Link ou DOI: https://dl.acm.org/doi/10.1145/3634737.3645009

  Resumo:
  O artigo discute o modelo de segurança SweetPAKE, que assegura a indistinguibilidade de chaves de sessão e dificulta a identificação de senhas reais. Ele explora os protocolos aPAKE, que permitem o armazenamento seguro de senhas como hashes unidirecionais, e apresenta o compilador BeePAKE, que utiliza múltiplos textos cifrados para autenticação e gera chaves de sessão de alta entropia. A segurança é avaliada por meio de modelos baseados em jogos e simulações, focando na resistência a ataques.

- Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg) (A4): SBC

  Título do Artigo: Um Framework Gerador de Tráfego para Detecção de Intrusões em Redes CAN

  Autores: Luiz F. Junior, Paulo Sergio M. Vargas, Paulo Vitor C. Lima, Silvio E. Quincozes

  Link ou DOI: https://sol.sbc.org.br/index.php/sbseg/article/view/30081

  Resumo:

  O seguinte artigo traz como problemática a necessidade do uso massivo de dados durante o uso de IDSs baseados em Machine Learning, tecnologias essas usadas para a automação de testes de segurança em rede. A partir disso, é proposto o desenvolvimento de um gerador de conjunto de dados,

baseado em redes Generativas Adversárias (GANs) e Codificadores Automáticos Variacionais (VAEs), a partir de uma técnica que se divide em um gerador de dados sintéticos e um discriminador responsável em avaliar sua autenticidade. A pesquisa buscou partir do nível de proximidade com os dados reais, ou seja, o menos sintético, comparar dois modelos de geradores e uma combinação entre eles, foram estes modelos o GAN, VAE, GAN-VAE (combinação dos modelos anteriores), resultando, portanto, no modelo GAN-VAE como o de maior fidelidade.

- Conferência sobre aplicações de segurança de computadores (ACSAC) (A2): ACM Digital Library

Título do Artigo: An Empirical Analysis of Enterprise-Wide Mandatory Password Updates

Autores: Ariana Mirian, Stefan Savage, Grant Ho, Geoffrey M. Voelker

Link ou DOI: https://dl.acm.org/doi/10.1145/3627106.3627198

Resumo:

O artigo em questão aborda uma discussão sobre a complexidade que envolvem a implementação de sistemas de atualizações obrigatórias de senhas em um organização, abordando tópicos como o interrompimento/desfoco de prioridades organizacionais para a priorização do mantimento da segurança das senhas, falta de suporte tecnológico ou até mesmo a conscientização dos funcionários sobre tais necessidades, a dificuldade em manter o padrão seguro de senhas constante, bem como o aumento das despesas dos setores de ti, a fim de garantir que tais práticas ocorram com eficiência

Periódicos:

- COMPUTERS & SECURITY (A1): ScienceDirect

Título do Artigo: Security risk assessment in IoT environments: A taxonomy and survey

Autores: Mofareh Waqdan, Habib Louafi, Malek Mouhoub

Link ou DOI:

https://www.sciencedirect.com/science/article/pii/S0167404825001452

Resumo:

O presente artigo apresenta uma pesquisa abrangente sobre os riscos de segurança em ambientes de Internet das coisas (IoT), focando nas crescentes vulnerabilidades e ameaças cibernéticas enfrentadas pelos dispositivos IoT. A pesquisa efetuada utiliza a metodologia PRISMA, a fim de

executar uma revisão sistemática da literatura, indicando os principais riscos e avaliando os mecanismos utilizados para a segurança da IoT, categorizando varia metodologias de avaliação de risco e discute os desafios enfrentados devido à heterogeneidade dos dispositivos, junto da evolução das ameaças cibernéticas. Sendo portanto, o objetivo principal desta pesquisa a orientação de pesquisas futuras em melhorar a resiliência dos dispositivos de IoT contra falhas de segurança.

- Journal of Information Security and Applications (A1): ScienceDirect

  Título do Artigo: SoK: The design paradigm of safe and secure defaults

  Autores: Jukka Ruohonen

  Link ou DOI:

  https://www.sciencedirect.com/science/article/pii/S2214212625000274

  Resumo:

  O presente artigo apresenta uma metodologia de design de padrões de segurança chamado SoK, a partir de um estudo de mapeamento sistemático, ou seja, uma revisão da literatura relevante. O artigo discute sobre os controles de acesso e o princípio de padrões de falhas, apresentando sua importância bem como as lacunas percebidas, adaptando paradigmas teóricos a aplicações práticas de engenharia de segurança, além de constantemente enfatizar a priorização da construção de sistemas seguros em contrapartida à divisão das etapas de teste para a identificação de vulnerabilidades. O artigo também busca estruturar um catálogo sistemático de princípios de segurança, bem como solicitar uma maior exploração das vulnerabilidades em todos os domínios da computação.

- Journal of Computer Security (B1): IOS Press

  Título do Artigo: Data privacy in the Internet of Things based on anonymization: A review

  Autores: Flávio Neves, Rafael Souza, Juliana Sousa, Michel Bonfim e Vinícius Garcia

  Link ou DOI: https://journals.sagepub.com/doi/10.3233/JCS-210089

  Resumo:
  O estudo apresenta uma Revisão Sistemática da Literatura (SLR) sobre segurança e privacidade em IoT, com foco na anonimização de dados. Os autores analisaram 21 estudos, utilizando um formulário de extração de dados para classificar objetivos, métodos de avaliação e aplicações propostas. O trabalho destaca técnicas de anonimização, como obfuscação e k-anonimidade, e discute os desafios enfrentados na implementação dessas

técnicas. Além disso, sugere direções futuras para pesquisa, enfatizando a necessidade de soluções que melhorem a privacidade e segurança dos dados gerados por dispositivos IoT, contribuindo para um ambiente mais seguro.